NetScaler Console 14.1

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Notes de publication 69

Migrer NetScaler Console sur site vers Citrix Cloud 71

- Configurer l'agent NetScaler 72
- Obtenir le fichier CSV client et secret depuis Citrix Cloud 72
- Valider les licences du service NetScaler Console 72
- Migrer à l'aide d'un script 73
- Revenir à NetScaler Console sur site 77
  - Prérequis 77
  - Utiliser le script de restauration 77
- FAQ 79
  - Service NetScaler Console 79
    - L'agent NetScaler est-il facultatif, comme l'agent NetScaler sur site ? 79
    - Pourquoi le service NetScaler Console ? 79
    - Que se passe-t-il après la migration si NetScaler Console sur site est une paire HA ? 79
    - Que se passe-t-il si l'agent tombe en panne pour une raison quelconque ? 79
    - La sauvegarde des instances est-elle également migrée ? 79
    - Les données historiques sont-elles également migrées ? 80
    - Les licences sur site sont-elles également migrées ? 80
    - Qu'est-ce qui n'est pas migré depuis NetScaler Console sur site ? 80
    - NetScaler Console sur site est intégré à Citrix Director. Qu'advient-il de l'intégration ? 80
    - Après la migration, est-il à nouveau nécessaire de licencier l'instance ou d'activer l'analyse ? 80
  - Outil de migration 81
    - Après l'exécution du script de migration, des messages d'erreur s'affichent. Quel peut être le problème ? 81

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les instances NetScaler ont des versions inférieures à la limitation mentionnée pour les licences en pool. Que se passe-t-il si l'option « Y » est sélectionnée pour changer le serveur de licences ? 81

Que se passe-t-il si le script de migration a échoué la configuration des instances NetScaler ? 81

Que se passe-t-il si quelques instances NetScaler ne parviennent pas à être déplacées vers le service NetScaler Console ? La réexécution du script de migration aidera-t-elle ? 81

Existe-t-il un fichier journal pour vérifier l'état de la migration ? 82

Que se passe-t-il si la session est interrompue pendant l'exécution du script de migration ? 82

Que se passe-t-il si le service NetScaler Console dispose de moins de licences que le NetScaler Console sur site et que le script de migration est lancé ? 82

Que se passe-t-il lorsque NetScaler Console sur site est migré vers le compte Express du service NetScaler Console ? 82

Que se passe-t-il si un utilisateur invité de Citrix Cloud (autre que l'utilisateur administrateur qui a créé le compte Citrix Cloud) tente de migrer la configuration NetScaler Console sur site ? 82

Script de restauration 83

Que se passe-t-il si le script de restauration est utilisé dans une paire HA NetScaler Console sur site ? 83

Qu'advient-il du nœud de reprise après sinistre après l'utilisation du script de restauration ? 83

Dépannage 83

Profil manuel ajouté au service NetScaler Console 83

Appareil NetScaler ajouté au service NetScaler Console 83

Importation de modèles personnalisés StyleBook vers le service NetScaler Console 84

Tâches de configuration ajoutées au service NetScaler Console 84

Blocs IP ajoutés au service NetScaler Console 84

Statut d'ajout du rapport du tableau de bord réseau 84

Tous les articles pratiques 85

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion des instances 85
Gestion de la configuration 86
Gestion des certificats 87
StyleBooks 87
Analytique 88
Gestion des événements 88
Authentification 89
Système NetScaler Console 89
Fonctions réseau 90
Vue d'ensemble 91
Fonctionnalités et solutions 91
Analyse et gestion des applications 91
Réseaux 92
Orchestration 93
Architecture 94
Comment NetScaler Console découvre les instances 94
Vue d'ensemble du sondage 96
Comment NetScaler Console sonde les instances et entités gérées 97
Différentes méthodes d'interrogation des instances 103
Interrogation globale des instances 103
Interrogation manuelle des instances 103
Interrogation manuelle des entités 104
Programme de télémétrie NetScaler® 106
Modes de collecte de télémétrie 112
Mode de collecte de télémétrie automatisée 112
Mode de collecte de télémétrie manuel 113
Diagnostics pour le dépannage des problèmes de collecte et de téléchargement de télémétrie 115
Comportement des diagnostics à partir de la version 14.1 build 56.x 115

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fonctionnement 115
Diagnostics au niveau du collecteur (Console) 116
Diagnostics au niveau de l'appareil (NetScaler) 117
Comportement du diagnostic avant la version 14.1 build 56.x 123
Notifications pour les téléchargements de télémétrie 124
Gouvernance des données 126
CONDITIONS D'UTILISATION DES INFORMATIONS IoC 129
Licences NetScaler Console 130
Licences 130
Haute disponibilité 135
Comment les licences sont-elles synchronisées entre les nœuds haute disponibilité de NetScaler Console ? 135
Orchestration 136
Mettre à niveau les licences de serveur virtuel 136
Vérification 137
Gérer les serveurs virtuels 137
Désactiver l'attribution automatique de licences aux serveurs virtuels 137
Sélectionner des serveurs virtuels tiers pour l'attribution de licences 138
Appliquer manuellement les licences de serveurs virtuels 138
Configurer la licence de serveur virtuel basée sur une stratégie 138
Afficher les serveurs virtuels sous licence 139
Configurer la prise en charge automatique des licences pour les serveurs virtuels non adressables 139
Licences 140
Haute disponibilité 142
Exigences système 143
Exigences pour NetScaler Console 143
Exigences pour l'agent NetScaler Console sur site 144

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Version minimale de NetScaler requise pour les fonctionnalités de NetScaler Console 144
Exigences pour l'analyse NetScaler Console 146
Versions minimales de Citrix Virtual Apps and Desktops requises pour les fonctionnalités de NetScaler Console 146
Clients légers pris en charge pour HDX™ insight 146
Licence d'instance NetScaler requise pour HDX insight 146
Hyperviseurs pris en charge 147
Systèmes d'exploitation et versions de Workspace pris en charge 147
Navigateurs pris en charge 148
Ports pris en charge 148
Ports pour le serveur NetScaler Console 149
Ports pour l'agent 152
Ports pour les instances NetScaler 153
Ports pour l'agent intégré NetScaler 154
Ports pour les serveurs externes 155
Limitations 156
Démarrage 158
Étape 1 - Examiner les exigences système 158
Étape 2 - Déployer NetScaler Console 159
Étape 3 - Ajouter des instances à NetScaler Console 159
Étape 4 - Activer l'analyse sur les serveurs virtuels 160
Étape 5 - Configurer le serveur NTP sur NetScaler Console 160
Étape 6 - Configurer les paramètres système pour des performances optimales de NetScaler Console 160
Prochaines étapes 162
Interface utilisateur graphique améliorée 163
Menu Afficher au survol 163
Hiérarchie de menu simplifiée 163

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Libellés de sous-menu mis à jour 164
Infrastructure > Configuration 164
Licences NetScaler > Licences en pool 164
Passerelle > HDX Insight 165
Paramètres 165
Menu réductible 166
Menu développé 166
Menu réduit 166
Basculement de la barre latérale 166
Afficher la barre latérale 166
Masquer la barre latérale 166
Définir comme écran d'accueil 166
Épingler les éléments favoris 167
Migrer vers le service 167
Déployer 168
Conditions préalables à l'installation de NetScaler Console 169
Exigences générales pour NetScaler Console 170
NetScaler® Console léger uniquement pour les licences groupées ou flexibles 170
NetScaler Console sur Citrix Hypervisor 171
Prérequis 171
Configuration système requise pour XenCenter® 172
Installer NetScaler® Application Delivery Management 172
Vérification 173
NetScaler Console sur Microsoft Hyper-V 173
Prérequis 173
Exigences système de Microsoft Hyper-V 174
Installation de NetScaler® Application Delivery Management 174
Vérification 176

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console sur VMware ESXi 176
Prérequis 177
Pour installer NetScaler Console 177
Vérification 180
Automatiser le déploiement de l'agent NetScaler® sur VMware ESXi 180
Configurer l'agent NetScaler 180
Enregistrer l'agent NetScaler et modifier le mot de passe par défaut 181
Prérequis 181
Comment configurer et enregistrer un agent NetScaler 181
Étape 1 : Télécharger et modifier le fichier .OVF 182
Étape 2 : Installer l'appliance virtuelle NetScaler Console sur VMware ESXi 185
Étape 3 : Vérifier 187
NetScaler Console sur cluster Kubernetes 188
Prérequis 188
Cluster Kubernetes 188
Partage NFS 188
Appliance NetScaler 189
Installer NetScaler Console sur un cluster Kubernetes 189
NetScaler Console sur serveur Linux KVM 191
Prérequis 191
Configuration matérielle requise 192
Exigences logicielles 192
Télécharger les fichiers d'installation de NetScaler Console 193
Installer NetScaler Application Delivery Management sur Linux-KVM 193
Configurer le NetScaler Application Delivery Management 196
NetScaler Console sur hyperviseur Nutanix (Acropolis) 198
Configuration matérielle requise 198
Télécharger le fichier d'installation de NetScaler Console 198

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer NetScaler Console sur l'hyperviseur Nutanix 199
Configuration réseau 200
NetScaler Console sur Red Hat OpenShift Virtualization 201
Configuration matérielle requise 201
Prérequis 202
Exigences de la plateforme 202
Architecture de déploiement 202
Installer NetScaler Console sur Red Hat OpenShift Virtualization 202
Étape 1 - Préparer l'environnement 202
Étape 2 - Télécharger le fichier d'installation de NetScaler Console 203
Étape 3 - Télécharger l'image vers le volume amorçable RHOCPV 203
Étape 4 - Créer la machine virtuelle 203
Étape 5. Démarrer la machine virtuelle 204
Étape 6. Accéder à NetScaler Console 204
NetScaler Console sur Azure Cloud 204
Prérequis 204
Configurer NetScaler Console 205
Paire HA NetScaler Console sur Azure Cloud 206
Prérequis 206
Configurer la paire HA NetScaler Console 207
NetScaler Console sur Amazon Web Services (AWS) 209
Prérequis 209
Configurer NetScaler Console 209
Configurer le déploiement haute disponibilité 211
Scénario de déploiement 211
Composants de l'architecture haute disponibilité 213
Outil de surveillance 213
Nœud principal 213

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nœud secondaire 213
Réplication physique en continu 213
Messages de pulsation 214
Adresse IP flottante 214
Points clés à noter 214
Conditions préalables 216
Pour configurer NetScaler Console en mode haute disponibilité 217
Enregistrer le premier serveur (nœud principal) 217
Enregistrer le deuxième serveur (nœud secondaire) 218
Déployer la configuration de haute disponibilité à partir de l'interface graphique du nœud principal 218
Désactiver la haute disponibilité 220
Redéployer la haute disponibilité 220
Scénarios de basculement de haute disponibilité 221
Afficher les messages du journal de synchronisation de la base de données 221
Scénario de split-brain 221
Licences 222
Configurer la haute disponibilité sur différents sous-réseaux de couche 3 (HA sur L3) 222
Architecture de haut niveau 223
Déploiement et configuration 224
Configurer la haute disponibilité dans NetScaler Console 225
Configurer NetScaler en tant qu'équilibreur de charge externe 225
Exemple de script de configuration d'équilibrage de charge NetScaler 226
Avantages 232
Configurer la reprise après sinistre pour la haute disponibilité 232
Activer l'authentification de base 233
Configurer l'authentification de base 233
Flux de travail de reprise après sinistre 234

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration initiale avant le sinistre 234
Prérequis 234
Configuration initiale de la reprise après sinistre 235
Déployer NetScaler Console en mode haute disponibilité 236
Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console à l'aide de la console DR 236
Déployer le nœud de reprise après sinistre à l'aide de l'interface graphique de NetScaler Console 237
Workflow après le sinistre 238
Après la reprise après sinistre 239
Rétablir les configurations sur le site principal d'origine 240
Configurer la reprise après sinistre pour un nœud autonome 241
Flux de travail de reprise après sinistre 242
Conditions préalables 242
Configuration initiale de la reprise après sinistre 243
Flux de travail après le sinistre 246
Après la reprise après sinistre 247
Restaurer les configurations sur le site principal d'origine 248
Configurer les agents sur site pour un déploiement multisite 249
Architecture 250
Activer l'authentification de base 251
Configurer l'authentification de base 251
Pour commencer 251
Installer l'agent dans un centre de données 251
Ports 252
Enregistrer l'agent 254
Attacher un agent à un site 255
Actions de l'agent 255

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter des instances NetScaler 256
Attacher une instance existante à l'agent 256
Accéder à l'interface graphique d'une instance pour valider les événements 256
Basculement de l'agent NetScaler 257
Configurer le seuil d'inaccessibilité de l'agent et la notification 258
Communication sécurisée entre les agents NetScaler® Console et NetScaler Console 258
Installer un agent NetScaler® en tant que microservice sur un cluster Kubernetes 259
Démarrage 260
Installer l'agent NetScaler dans le cluster Kubernetes 260
Installer un opérateur OpenShift d'agent NetScaler Console pour le déploiement sur site de NetScaler Console 261
Prérequis 262
Installer l'opérateur d'agent 262
Supprimer une instance d'agent 263
Désinstaller l'opérateur d'agent 264
Mettre à niveau les agents 264
Processus de mise à niveau 264
Migrer le déploiement de serveur unique NetScaler Console vers un déploiement haute disponibilité 265
Migrer de NetScaler Insight Center vers NetScaler Console 266
Prérequis 266
Exigences matérielles 267
Procédure d'installation 267
Intégrer NetScaler Console avec Citrix Director 268
Prérequis 269
Exigences matérielles pour la migration de HDX Insight vers NetScaler Console 269
Configuration minimale requise 269
Configuration logicielle requise 269

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations 270
Attacher un disque supplémentaire à NetScaler Console 270
Attacher un disque supplémentaire dans une NetScaler Console autonome 271
Lancer l'outil de partitionnement de disque 272
Créer des partitions sur le nouveau disque supplémentaire 273
Redimensionner les partitions du disque supplémentaire existant 274
Supprimer les partitions du disque supplémentaire 275
Redémarrer la machine virtuelle 276
Créer un fichier de sauvegarde des données du disque 276
Commandes supplémentaires 277
Attacher des disques supplémentaires à NetScaler Console déployé en haute disponibilité 279
Chiffrement de disque NetScaler MPX™ via NetScaler Console 282
Conditions préalables 283
Ajouter le numéro de série de l'instance dans le serveur HSM (Thales CipherTrust Manager) 284
Chiffrement du disque d'instance via NetScaler Console 285
Validation après le chiffrement 287
Restaurer l'instance NetScaler MPX après le chiffrement 287
Comportement de la paire HA NetScaler MPX™ après le chiffrement 288
Comportement du cluster NetScaler MPX™ après chiffrement 288
NetScaler Console Cloud Connect 290
Prérequis 291
Configurer Cloud Connect 294
Flux de travail 1 – Nouvel utilisateur (pas de compte Citrix Cloud et pas de locataire de service NetScaler Console) 294
Flux de travail 2 – Un compte Citrix Cloud existe mais le locataire du service NetScaler Console n'existe pas 295
Flux de travail 3 - Le compte Citrix Cloud et le locataire du service NetScaler Console existent 295

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prise en charge de la configuration du proxy pour Cloud Connect 296
État de Cloud Connect et comportement d'actualisation 297
État de Cloud Connect 297
Actualiser l'état de Cloud Connect 298
Diagnostics de Cloud Connect 298
Gestion des erreurs et messagerie 299
Notifications pour l'état de Cloud Connect 299
Fréquence des notifications 300
Canaux de notification 300
Gestion des notifications 300
Données collectées via Cloud Connect 301
Dépannage des problèmes de connectivité Cloud Connect 301
Autres options 301
Comportement des fonctionnalités spécifiques à la version 302
FAQ 303
Configurer 306
Ajouter des instances à NetScaler Console 307
Comment créer un profil NetScaler 307
Ajouter des instances NetScaler à NetScaler Console 310
Ajouter des instances NetScaler CPX à NetScaler Console 311
Ajouter une instance NetScaler BLX autonome dans NetScaler Console 312
Ajouter des instances NetScaler BLX haute disponibilité dans NetScaler Console 313
Accéder à l'interface graphique d'une instance depuis la NetScaler Console 314
Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler Console 314
Configurer les analyses 316
Gérer les licences et activer l'analyse sur les serveurs virtuels 316
Gérer les licences sur les serveurs virtuels 317
Configurer l'analyse globalement 321

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prérequis 322
Activer l'analyse 322
Configurer l'analyse sur les serveurs virtuels 322
Configurer l'analyse sur les serveurs virtuels existants 323
Configurer l'analyse globale 326
Migrer l'analyse 329
Attribuer un profil réseau à l'instance NetScaler gérée 330
Conditions préalables 330
Configurer le serveur NTP 331
Configurer les paramètres système 332
Configurer les alarmes système 332
Configurer les notifications système 332
Configurer les paramètres de sauvegarde du système 333
Configurer les paramètres de sauvegarde des instances 333
Activer l'authentification de base 334
Configurer l'authentification de base 334
Activer ou désactiver les fonctionnalités de NetScaler Console 334
Intégrer NetScaler Console à l'instance ServiceNow 335
Conditions préalables 336
Comment intégrer NetScaler Console à ServiceNow ? 336
Étape 1 - S'abonner au service ITSM Adapter dans Citrix Cloud 336
Étape 2 - Créer un accès de point de terminaison dans l'instance ServiceNow 336
Étape 3 - Ajouter une instance ServiceNow 337
Étape 4 - Tester la génération automatique de tickets ServiceNow dans NetScaler Console 337
Définir les notifications ServiceNow dans NetScaler Console 337
Exporter ou planifier l'exportation de rapports 338
Exporter un rapport 339

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Planifier l'exportation du rapport 339
Afficher et modifier les rapports d'exportation planifiés 340
Mise à niveau 341
Avant la mise à niveau 341
Points importants à noter avant de passer à la version 14.1-xx.xx et ultérieure 342
Mettre à niveau un seul serveur NetScaler Console vers la version 14.1-xx.xx 343
Mettre à niveau une paire haute disponibilité vers la version 14.1 344
Mettre à niveau le déploiement de reprise après sinistre de NetScaler Console 344
Mettre à niveau le nœud de reprise après sinistre de NetScaler Console 345
Mettre à niveau les agents sur site pour un déploiement multisite 345
Mettre à niveau l'agent sur site 345
Ajouter un disque supplémentaire au serveur NetScaler Console 346
Authentification 347
Serveurs d'authentification externes 347
Authentifier les utilisateurs dans NetScaler Console 348
Ajouter un serveur d'authentification LDAP 349
Ajouter un serveur d'authentification RADIUS 351
Ajouter un serveur d'authentification TACACS 352
Utilisateurs dans NetScaler Console 353
Groupes d'utilisateurs dans NetScaler Console 354
Extraire un groupe de serveurs d'authentification 354
Activer les serveurs d'authentification externes et les options de secours 355
Configurer les serveurs externes de secours et en cascade 356
Prise en charge de l'authentification à deux facteurs (2FA) avec LDAP, RADIUS et TACACS 357
Configurer l'authentification à deux facteurs 357
Accès utilisateur à NetScaler® Console avec authentification à deux facteurs 358
Contrôle d'accès 359
Contrôle d'accès basé sur les rôles 359

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations 361
Configurer les stratégies d'accès 361
Accorder des autorisations StyleBook aux utilisateurs 364
Configurer les groupes 364
Créer un groupe d'utilisateurs 365
Comment l'accès utilisateur change en fonction de la portée de l'autorisation 373
Mappage du RBAC lors de la mise à niveau de NetScaler Console de la version 12.0 vers les versions ultérieures 373
Configurer les rôles 374
Configurer les utilisateurs 375
Tâches exploitables et recommandations 377
Tâches 378
Recommandations 381
Comment utiliser le flux de travail Guide me et compléter la recommandation ? 384
Configurer les notifications 385
FAQ 385
Un tableau de bord unifié pour afficher les détails des métriques clés de l'instance 387
Applications 387
Infrastructure NetScaler 388
Sécurité des applications 388
Passerelle 389
Personnaliser le tableau de bord 389
Afficher les détails de l'agent 390
Créer et appliquer des filtres 390
Modifier les filtres 391
Créer des tableaux de bord personnalisés pour afficher les détails des métriques clés d'instance 391
Plus d'options dans le tableau de bord 392

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Partager le tableau de bord avec d'autres utilisateurs 393
Applications 394
Prérequis 394
Présentation des applications 394
Applications discrètes 395
Applications personnalisées 395
Points à noter 395
Applications de microservices 395
Gestion des applications et tableau de bord des applications 396
Gérer les applications 396
Tableau de bord des applications 396
Mises à jour du nouveau comportement du tableau de bord par rapport à l'ancien tableau de bord 396
Gérer les applications 397
Afficher les détails de l'application 397
Ajouter une application 398
Créer une application à l'aide du StyleBook 400
Modifier ou supprimer une application 401
Exporter les rapports du tableau de bord des applications et du tableau de bord de sécurité 401
Afficher les applications 402
Configurer et associer une application à plusieurs applications personnalisées 403
Vue d'ensemble du tableau de bord des applications 405
Rechercher et filtrer les résultats à l'aide de la barre de recherche 407
Créer et appliquer des balises aux applications 407
Détails de l'application 408
Sélectionner les composants de l'App Score et définir des seuils 411
Détails de l'application pour les applications de microservices 413
Analyse intelligente des applications 416

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer l'analyse intelligente des applications 417
Indicateurs de performance pour l'analyse des applications 419
Temps de réponse 420
Services actifs 420
Utilisation moyenne du CPU 420
Utilisation de la mémoire 421
Basculement de services 421
Serveur instable 422
Accumulation de sessions 423
Faible réutilisation de session 424
Accumulation de la file d'attente de surtension 425
Paquets HTTP inhabituellement volumineux 425
Type de persistance incorrect 426
Dépassements de la limite de la file d'attente de réassemblage TCP 427
Trafic SSL en temps réel 427
Dépanner le tableau de bord des applications 428
Scénario de dépannage 429
L'application est sous licence 429
Le collecteur de métriques est activé 429
Instance NetScaler® versions antérieures 430
Versions ultérieures de l'instance NetScaler 430
Utilisation et anomalies des applications 433
Analyse de l'utilisation de pointe et creuse 434
Évaluer les limites de mise à l'échelle de l'application 434
Identifier les 5 principales fenêtres de maintenance d'application 434
Analyse de l'utilisation des applications 436
Afficher les détails des métriques au format graphique 442
Dépanner les problèmes de Web Insight 445

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyse de la notation SSL A+ 446
Mettre à niveau vers la note SSL A+ 447
Rétablir la note SSL 447
Déterminer l'impact de l'évaluation SSL sur le trafic de l'application 448
Tableau de bord Web Insight 449
Requêtes de cache intégré 451
Dépanner les problèmes de Web Insight 451
Afficher la cause première de la latence des applications 452
Exploration des applications 452
Temps de réponse 453
Graphe de services 455
Graphe de services pour les applications sur toutes les instances NetScaler 455
Graphique de service pour les applications Kubernetes 456
Graphique de service pour les applications Web à 3 niveaux 457
Graphe de services pour les applications Kubernetes 458
Configuration du graphique de service 459
Exigences logicielles 459
Avant de commencer 460
Topologie d'entrée à niveau unique ou unifiée 460
Topologie à deux niveaux ou Service Mesh Lite 460
Topologie du maillage de services 461
Afficher les détails dans le graphique de service 463
Tableau de bord du graphique de service 463
Afficher les tendances des métriques clés à l'aide de la vue tabulaire 465
Afficher les métriques client 466
Afficher les métriques TCP et SSL 468
Afficher les détails du service 469
Appliquer des filtres 469

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utilisation de l'option de paramètres 469
Analyser les erreurs 470
Afficher les détails de la transaction HTTP 470
Configurer les seuils dans le graphique de service 471
Seuil unique 472
Double seuil 472
Afficher les détails du service 473
Détails des métriques 473
Afficher les détails du pod de back-end 474
Afficher les détails d'entrée pour le dépannage des problèmes 475
Traçage distribué 478
Prérequis 479
Afficher les détails de la trace de service 483
Afficher les détails de la transaction 483
Afficher les détails de diagnostic pour les données partielles ou manquantes dans le graphe de service 485
Diagnostics pour l'absence de données 485
Diagnostics pour les données partielles 486
Dépannage 486
Graphe de service pour les applications 486
Vue d'application 487
Vue des fonctions réseau 487
Vue du graphique de service pour les transactions inactives 487
Analyser les métriques 488
Mesures client 488
Mesures de fonction réseau 488
Mesures de service 488
Métriques NetScaler (uniquement pour les applications GSLB) 489

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vue d'ensemble de toutes les applications dans le graphique de service 489
Afficher les métriques client 490
Afficher les détails de NetScaler 490
Afficher les applications discrètes 490
Afficher les applications de microservices 492
Barre de recherche pour filtrer les résultats 493
StyleBooks 494
Catégories de StyleBook 496
StyleBooks par défaut et personnalisés 496
StyleBooks publics et privés 497
Exemple de StyleBook marqué comme privé 497
Afficher les StyleBooks 497
Télécharger des StyleBooks personnalisés 498
Mettre à jour un StyleBook personnalisé 499
Supprimer les StyleBooks personnalisés 499
Afficher les dépendances de StyleBook 500
Pour afficher les dépendances de StyleBook 500
Dépendances en amont 500
Dépendances en aval 501
Auditer la configuration NetScaler par rapport au pack de configuration 501
Télécharger le bundle de support d'un pack de configuration 501
Créer une balise pour le StyleBook 502
Pour configurer un StyleBook à l'aide de commandes CLI 503
Cloner un StyleBook 503
Importer et synchroniser des StyleBooks à partir d'un référentiel externe 504
Ajouter un référentiel et importer des StyleBooks depuis un référentiel externe 505
Étapes pour importer des StyleBooks et des packs de configuration depuis GitHub/GitLab 507
Utiliser les StyleBooks par défaut 507

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour créer une configuration à partir d'un StyleBook par défaut 507
StyleBook de pare-feu d'application Web 509
Déploiement des configurations de pare-feu d'application 509
Masquer tous les StyleBooks par défaut 512
StyleBook d'analyse Prometheus 513
Prérequis 513
Migrer la configuration d'application NetScaler® à l'aide du générateur de configuration StyleBooks 514
Partage d'entités de configuration entre les configurations migrées 515
Fonctionnalités NetScaler prises en charge 516
Créer un StyleBook pour migrer la configuration d'application NetScaler 517
Limitations 520
StyleBooks d'applications métier 520
StyleBook SSO Google Apps 521
Pour déployer le StyleBook SSO Google apps 522
StyleBook SSO Office 365 526
Pour déployer le StyleBook SSO Microsoft Office 365 527
StyleBook Microsoft Skype Entreprise 531
Composants principaux 531
Configuration des instances NetScaler dans une entreprise 533
StyleBook Microsoft Exchange 540
Fonctionnalités NetScaler configurées à l'aide du StyleBook Microsoft Exchange 540
Prérequis 540
Configuration d'un StyleBook Microsoft Exchange 541
StyleBook Microsoft SharePoint 543
Prérequis 543
Fonctionnalités NetScaler configurées par le StyleBook Microsoft SharePoint 2016 543
Déploiement des configurations StyleBook SharePoint 545

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Affichage des objets définis sur l'instance NetScaler 548
StyleBook de proxy Microsoft ADFS 548
Avantages de l'utilisation de NetScaler comme proxy ADFS 548
StyleBook Oracle E-Business 553
Pour créer une configuration pour Oracle E-Business Suite 12.2 553
Citrix StoreFront™ StyleBooks 554
Créer une configuration pour les applications Citrix StoreFront 555
Créer et utiliser des StyleBooks personnalisés 556
Avant de commencer 556
Anatomie d'un StyleBook 557
StyleBook pour créer un serveur virtuel d'équilibrage de charge 558
En-tête 558
Composants 564
Créez votre StyleBook 565
StyleBook pour créer une configuration de répartition de charge de base 568
En-tête 568
Composants 571
Sorties 576
Créez votre StyleBook 577
Créer un StyleBook composite 581
Créez votre StyleBook 582
Utiliser les attributs d'interface graphique dans un StyleBook personnalisé 586
Importer des StyleBooks personnalisés 587
Pour importer votre StyleBook 588
Rechercher des StyleBooks personnalisés 592
Créer et modifier un pack de configuration 592
Créer un pack de configuration 592

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Réutiliser les configurations créées en dehors des StyleBooks et partager les configurations entre les ConfigPacks 593

Modifier le StyleBook d'un pack de configuration 594

Exporter ou importer des packs de configuration 596

Enregistrer un pack de configuration en tant que brouillon 598

Créer un calendrier pour un pack de configuration 599

Détacher une instance cible d'un pack de configuration 600

Créez vos StyleBooks 600

Créer un StyleBook pour télécharger des fichiers vers NetScaler Console 604

Configuration StyleBook 605

Créez votre StyleBook -1 605

Créez votre StyleBook - 2 607

Création de configurations pour télécharger des fichiers 608

Créer un StyleBook pour télécharger des fichiers de certificat SSL et de clé de certificat vers NetScaler Console 610

Configuration StyleBook 610

Création de configurations pour télécharger des fichiers SSL 613

Créez votre StyleBook 614

Gérer les certificats SSL depuis le magasin de certificats à l'aide de StyleBooks 618

Paramètres 618

Composants 619

Créez votre StyleBook 620

Activer l'analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook 624

Rôles d'instance 627

Section « target-roles » 628

Rôle « default » 629

Composants avec des rôles 629

Créez votre StyleBook 632

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utilisation des API 635
Créer un StyleBook pour effectuer des opérations non-CRUD 637
Prise en charge des opérations non-CRUD 638
Migrer les packs de configuration d'un StyleBook vers un autre StyleBook 639
Migrer les packs de configuration 640
Créez vos StyleBooks 641
Gérer les sources de données 645
Utiliser une instance NetScaler comme source de données 647
Utilisation de la source de données intégrée sans collection 647
Utilisation de la source de données intégrée avec collection 650
Utiliser les instances NetScaler cibles comme sources de données 657
Exemple de StyleBook pour utiliser l'instance NetScaler cible comme source de données 658
Utiliser des sources de données personnalisées 659
Ajouter un type de source de données 660
Ajouter un schéma de collection sous le type de source de données 660
Ajouter une source de données 661
Ajouter des données de collection 661
Utiliser une source de données personnalisée sans collection 661
Utiliser des sources de données personnalisées avec une collection 664
Utiliser les API pour créer des configurations à partir de StyleBooks 667
Exemple 1 667
Exemple 2 671
Exemple 3 673
Exemple 4 675
Mise à jour d'une configuration 678
Suppression d'une configuration 679
Utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificat et de clé 680

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser l'API pour créer des configurations afin de télécharger n'importe quel type de fichier 682
Utiliser l'API pour importer des StyleBooks personnalisés 684
Utiliser l'API pour télécharger des StyleBooks personnalisés 686
Utiliser l'API pour supprimer des StyleBooks personnalisés 687
Grammaire des StyleBooks 688
En-tête 690
Importer des StyleBooks 692
Paramètres 693
'nom' 694
'libellé' 694
'Description' 694
« type » 694
'réseau' 697
'dynamic-allocation' 698
'clé' 698
'obligatoire' 699
'allowed-values' 699
'par défaut' 701
'motif' 702
'min-value' 703
'max-value' 703
'min-length' 704
'max-length' 704
'min-items' 704
'max-items' 705
'interface graphique' 705
'colonnes' 706
'modifiable' 706

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'collapse_pane' 706
'mise en page' 712
'dependent-parameters' 713
Mécanisme parameters-default-sources 715
Construction source de paramètres 719
Conditions de paramètre 720
'augment-allowed-values' 722
'show' ou 'hide' 722
'set-default' 723
'set-required' 724
'set-allowed-values' 724
'set-label' 725
'set-description' 725
'collapse-pane' ou 'expand-pane' 726
'set-pattern' 726
Conditions de paramètre imbriquées 727
Substitutions 728
Mappage de substitution 736
Itérer à travers les listes de substitution 737
Composants 740
Composants d'aide 742
Propriétés facultatives 744
Le construct properties-default-sources 747
Calcul des propriétés du composant 749
Composants imbriqués 749
Construction de condition 751
Structure de répétition 753
Construction de condition de répétition 757

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Répétitions imbriquées 758
Sorties 760
Référence des paramètres 762
Référence parent 763
Référence des composants 765
Référence des substitutions 767
Référence de variable 767
Opérations 769
Analyse 773
Serveurs virtuels cibles et types d'informations 777
Alarmes 778
Expressions 782
Expressions arithmétiques 782
Expressions de chaîne 783
Expressions de liste 783
Expressions relationnelles 783
Expressions logiques - booléennes 784
Expressions de chaîne littérales 784
Expressions cibles 785
Validation du type d'expression 786
Interpolations sur place 789
Types autorisés dans les interpolations 790
Interpolations simples 791
Conversions de type automatiques 791
Interpolations séquentielles 791
Interpolations imbriquées 791
Interpolations avec quotewrap 792
Fonctions intégrées 792

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fonction str() 793

entier() 793

booléen() 793

Fonction len() 794

Fonction min() 794

maximum() 795

binaire() 795

octal() 795

hexadécimal() 796

minuscule() 796

majuscule() 796

somme() 796

Fonction pow() 797

ip() 797

base64.encode() 797

base64.decode() 798

existe() 798

Filtrer() 798

if-then-else() 799

joindre() 799

diviser() 800

Mapper() 800

mettre_entre_guillemets() 801

remplacer() 802

rogner() 803

tronquer() 803

unique() 803

url.encode() 804

© 1997–2026 Citrix Systems, Inc. All rights reserved.

url.decode() 804

is-ipv4() 804

is-ipv6() 804

Commence par() 804

Se termine par() 805

contient() 805

sous-chaîne() 805

multiples() 806

inverser() 807

Détection des dépendances 807

Dépendances cycliques 809

Sécurité 812

Tableau de bord de sécurité des applications 812

Détails de l'indice de menace 813

Détails de l'indice de sécurité 814

Tableau de bord de sécurité unifié 814

Applications sécurisées 815

Configurer les protections pour les applications non sécurisées 815

Afficher les détails des violations de sécurité des applications 821

Prérequis 822

Sécurité des API 822

Afficher les analyses d'API 822

Distribution des points de terminaison d'API 823

Instances d'API 823

Points de terminaison d'API 823

Échecs d'authentification 824

Afficher différentes informations d'API 824

Découvrir les points de terminaison d'API 826

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les points de terminaison d'API 827
Passerelle 828
Gateway Insight 828
Points à noter 829
Limitations 829
Activer Gateway Insight 830
Pour NetScaler Console version **13.0 Build 41.x ou ultérieure** 831
Activer la journalisation du nom d'utilisateur pour l'authentification, l'autorisation et l'audit AppFlow sur une appliance NetScaler Gateway à l'aide de l'interface graphique 831
Affichage des rapports Gateway Insight 831
Pour afficher les échecs EPA, SSO, d'authentification, d'autorisation et de lancement d'application 832
Pour afficher un résumé des modes de session, des clients et du nombre d'utilisateurs 832
Affichage des rapports Gateway Insight pour les utilisateurs 832
Pour afficher les détails de l'utilisateur 833
Affichage des rapports Gateway Insight pour les applications 834
Pour afficher les détails de l'application 834
Affichage des rapports Gateway Insight pour les passerelles 835
Pour afficher les détails de la passerelle 835
Exportation des rapports 835
Pour exporter un rapport 836
Cas d'utilisation de Gateway Insight 836
Un utilisateur ne peut pas se connecter à l'appliance NetScaler Gateway ou aux serveurs web internes 837
Échecs d'authentification 837
Échecs EPA 838
Échecs SSO 839
Après s'être connecté avec succès à NetScaler Gateway, un utilisateur ne peut pas lancer d'application virtuelle 840

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir lancé une nouvelle application avec succès, un utilisateur souhaite afficher le nombre total d'octets et la bande passante consommés par cette application 841

Un utilisateur s'est connecté à NetScaler Gateway avec succès, mais ne peut pas accéder à certaines ressources réseau dans le réseau interne 841

Différents utilisateurs peuvent utiliser différents déploiements de NetScaler Gateway ou se connecter à NetScaler Gateway via différents modes d'accès. L'administrateur doit pouvoir afficher les détails sur les types de déploiement et les modes d'accès 842

Dépanner les problèmes de Gateway Insight 842

Liste de contrôle de la configuration de Gateway Insight 842

Liste de contrôle de la connectivité entre NetScaler et NetScaler Console 843

Liste de contrôle de la génération d'enregistrements dans NetScaler 843

Validation des enregistrements dans NetScaler Console 844

Validation des journaux Logstream dans NetScaler Console 844

Compteurs Gateway Insight 844

Enregistrements AppFlow dans le journal NetScaler 845

Contacter le support technique de Citrix 847

Problèmes connus 847

HDX™ Insight 847

Identification de la cause première des problèmes de performances lentes 848

Scénario 1 848

Scénario 2 849

Cartes géographiques pour HDX Insight 850

Cas d'utilisation 851

Limitations 851

Activation de la collecte de données HDX™ Insight 852

Activation de la collecte de données pour la surveillance des NetScaler déployés en mode utilisateur LAN 852

Activation de la collecte de données pour les appliances NetScaler Gateway déployées en mode saut unique 855

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activation de la collecte de données pour les appliances NetScaler Gateway déployées en mode double saut 857

Configurer HDX Insight sur les serveurs virtuels utilisés pour Optimal Gateway 858

Activer la collecte de données pour la surveillance des NetScaler déployés en mode transparent 864

Activer la collecte de données pour les appliances NetScaler Gateway déployées en mode saut unique 867

Activer la collecte de données pour surveiller les NetScaler déployés en mode transparent 868

Activer la collecte de données pour les appliances NetScaler Gateway déployées en mode double-saut 871

Activer la collecte de données pour surveiller les NetScaler déployés en mode utilisateur LAN 876

Créer des seuils et configurer des alertes pour HDX™ Insight 879

Exemples de cas d'utilisation 881

Affichage des rapports et métriques HDX™ Insight 883

Rapports et métriques de la vue utilisateur 884

Rapports et métriques de la vue Application 896

Rapports et métriques de la vue Bureau 903

Rapports et métriques de la vue d'instance 916

Rapports et métriques de la vue des licences 920

Rapports et métriques de la vue Application 921

Rapports et métriques de la vue Bureau 928

Rapports et métriques de la vue Utilisateur 941

Rapports et métriques de la vue d'instance 953

Rapports et métriques de la vue des licences 957

Résoudre les problèmes de HDX™ Insight 957

Liste de contrôle de la configuration de HDX Insight 958

Liste de contrôle de la connectivité entre NetScaler et NetScaler Console 958

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Liste de contrôle de la génération d'enregistrements pour le trafic HDX/ICA dans NetScaler 959
Compteurs d'erreurs 968
Validation nstrace 973
Liste de contrôle du remplissage des enregistrements dans NetScaler Console 973
Avant de contacter le support technique Citrix 973
Problèmes connus 973
Infrastructure 974
Analyse de l'infrastructure 974
Analyse de l'infrastructure 975
Score d'instance 975
Indicateurs de santé 975
Afficher les problèmes de capacité NetScaler 978
Valeur des indicateurs de santé 979
Tableau de bord d'analyse de l'infrastructure 979
Vue Circle Pack 980
Cercles d'instances 980
Cercles d'instances groupés 981
Cercles d'instances en cluster 981
Comment utiliser Circle Pack 982
Vue tabulaire 982
Comment utiliser le panneau de résumé 983
Informations sur l'instance 985
Profil de trafic 985
Comment utiliser le panneau de paramètres 985
Vue 986
Seuils de score 986
Comment visualiser les données sur le tableau de bord 986

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les détails de l'instance dans Infrastructure Analytics 987
Afficher les problèmes de capacité dans une instance NetScaler 992
Afficher les actions recommandées pour résoudre les problèmes de capacité 993
Analyse d'infrastructure améliorée avec de nouveaux indicateurs 994
Vue tabulaire 996
Afficher les détails d'une anomalie 996
Gestion des instances 996
Ajouter une instance 997
Comment utiliser le tableau de bord des instances 997
Surveiller les sites répartis mondialement 998
Cas d'utilisation 999
Configuration des géocartes 1000
Comment créer des balises et les attribuer aux instances 1002
Comment rechercher des instances en utilisant les valeurs des balises et des propriétés 1003
Pour rechercher des instances NetScaler VPX 1004
Mises à jour centralisées de la base de données GeoIP via NetScaler® Console 1005
Limitations 1006
Configuration des mises à jour centralisées de la base de données GeoIP via NetScaler Console 1006
Gérer les partitions d'administration des instances NetScaler 1008
Créer une paire haute disponibilité NetScaler 1011
Sauvegarder et restaurer les instances NetScaler 1012
Configurer les paramètres de sauvegarde des instances 1013
Restaurer une instance NetScaler à l'aide de NetScaler Console 1016
Forcer un basculement vers l'instance NetScaler secondaire 1018
Forcer une instance NetScaler secondaire à rester secondaire 1019
Créer des groupes d'instances 1020
Pour créer un groupe d'instances à l'aide de NetScaler Console 1020

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour identifier et ajouter des instances non mappées à un groupe 1021
Provisionner des instances NetScaler VPX sur SDX à l'aide de NetScaler Console 1021
Étape 1 - Ajouter une instance VPX 1022
Étape 2 - Allouer des licences 1022
Étape 3 - Allouer des ressources 1023
Étape 4 - Ajouter l'administration de l'instance 1026
Étape 5 - Spécifier les paramètres réseau 1027
Étape 6 - Spécifier les paramètres VLAN de gestion 1028
Afficher l'instance VPX provisionnée 1029
Provisionner des instances NetScaler VPX sur VMware ESX 1029
Prérequis 1029
Convertir les fichiers NetScaler VPX en modèles 1030
Créer des autorisations pour que NetScaler Console accède à VMware vCenter 1030
Créer un site dans NetScaler Console 1031
Provisionner une instance sur VMware ESX 1032
Redécouvrir plusieurs instances NetScaler VPX 1033
Dégérer une instance 1034
Tracer l'itinéraire vers une instance 1034
Afficher les adresses IP appartenant à NetScaler 1035
Exporter les adresses IP appartenant à NetScaler 1035
Planifier l'exportation des adresses IP détenues par NetScaler 1036
Répliquer les configurations d'une instance NetScaler à une autre 1037
Pour répliquer les configurations d'une instance vers d'autres instances NetScaler 1038
Gestion des certificats SSL 1038
Paramètres de la politique SSL d'entreprise 1039
Fonctionnement du certificat NetScaler Console 1040
Cas d'utilisation de la gestion des certificats SSL 1040
Installer des certificats SSL 1040

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Paramètres de notification pour l'expiration des certificats 1041
Renouvellement des certificats 1041
Lier et dissocier les certificats SSL 1042
Journaux d'audit 1042
Renouvellement automatique des certificats à l'aide du protocole ACME 1043
Prise en charge d'ACME dans NetScaler® Console 1043
Étapes de configuration pour l'intégration d'ACME 1045
Émission et renouvellements 1053
Émettre un certificat 1055
Intégration tierce 1056
Limitations 1058
Dépanner les problèmes liés au renouvellement automatique des certificats 1058
Gestion des certificats zéro-touche 1059
Télécharger les certificats 1060
Activer la gestion des certificats zéro-touch 1061
Prise en charge du mode de filtrage SSL 1061
Configurer les paramètres du mode de filtrage 1063
Utiliser le tableau de bord SSL 1063
Pour surveiller les certificats SSL 1064
Pour afficher les pistes d'audit des certificats SSL 1065
Pour supprimer le certificat SSL sur le tableau de bord SSL 1066
Pour exclure les certificats NetScaler par défaut sur le tableau de bord SSL 1067
Afficher, télécharger et téléverser des fichiers SSL 1067
Afficher la chaîne de certificats SSL 1068
Configurer les notifications d'expiration des certificats SSL 1068
Mettre à jour un certificat installé 1069
Installer des certificats SSL sur une instance NetScaler 1070
Créer une demande de signature de certificat (CSR) 1072

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lier et délier des certificats SSL 1074
Configurer une politique d'entreprise 1075
Interroger les certificats SSL des instances NetScaler 1076
Utiliser le magasin de certificats NetScaler Console pour gérer les certificats SSL 1077
Ajouter des certificats SSL au magasin de certificats 1077
Mettre à jour les certificats SSL dans le magasin de certificats 1077
Supprimer les certificats SSL du magasin de certificats 1078
Installer les certificats SSL sur les instances NetScaler® 1078
Importer des certificats depuis les instances NetScaler 1079
Mettre à jour les certificats de serveur sans téléchargements intermédiaires 1079
Gérer les certificats et chiffrements personnalisés de base de données dans un déploiement haute disponibilité 1081
Installer vos certificats de base de données sur NetScaler Console 1081
Gérer vos certificats de base de données installés 1082
Configurer les suites de chiffrement de la base de données 1082
Événements 1082
Utiliser le tableau de bord des événements 1083
Définir l'âge de l'événement pour les événements 1084
Planifier un filtre d'événements 1085
Définir des notifications par e-mail répétées pour les événements 1086
Supprimer les événements 1087
Créer des règles d'événement 1087
Étape 1 - Définir une règle d'événement 1089
Étape 2 - Choisir la gravité de l'événement 1090
Étape 3 - Spécifier la catégorie d'événement 1090
Étape 4 - Spécifier les instances NetScaler 1091
Étape 5 - Sélectionner les objets de défaillance 1091
Étape 6 - Spécifier les filtres avancés 1091

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 7 - Ajouter des actions de règle d'événement 1092
Modifier la gravité signalée des événements qui se produisent sur les instances NetScaler 1100
Afficher le résumé des événements 1100
Afficher les messages d'événement 1101
Afficher les niveaux de gravité des événements et les détails des traps SNMP 1102
Afficher et exporter les messages syslog NetScaler 1104
Configurer NetScaler Console comme serveur syslog 1104
Afficher et rechercher les messages syslog 1104
Exporter et planifier les messages syslog 1105
Supprimer les messages syslog 1105
Suppression des messages syslog en créant des filtres 1106
Désactivation du filtre 1107
Configurer les paramètres de purge pour les événements d'instance 1107
Fonctions réseau 1108
Générer des rapports pour les entités d'équilibrage de charge 1108
Générer un rapport d'équilibrage de charge combiné 1109
Générer un rapport d'entité d'équilibrage de charge individuel 1110
Exporter ou planifier l'exportation des rapports de fonctions réseau 1111
Rapports réseau 1113
Tableau de bord des rapports réseau 1113
Exportation des rapports réseau 1115
Afficher les données de rapport réseau en appliquant des agrégations 1117
Comment gérer les seuils pour les rapports réseau sur NetScaler Console 1118
Définir l'intervalle d'interrogation des performances pour les rapports réseau 1121
Configuration des paramètres d'élagage des rapports réseau 1121
Tâches de configuration 1121
Modèle de configuration 1122
Instance 1123

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fichier 1123

Enregistrer et lire 1123

Articles connexes 1123

Créer une tâche de configuration 1124

Utiliser l'enregistrement et la lecture pour créer des tâches de configuration 1127

Utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances 1130

Utiliser des variables dans les tâches de configuration 1131

Créer des tâches de configuration à partir de commandes correctives 1135

Répliquer la configuration en cours d'exécution et enregistrée d'une instance NetScaler à une autre 1137

Réutiliser les tâches de configuration exécutées 1138

Utiliser la commande SCP (put) dans les tâches de configuration 1139

Utiliser des modèles de configuration 1142

Utiliser le modèle de configuration maître 1142

Planifier des tâches créées à l'aide de modèles intégrés 1148

Planifier une tâche pour configurer l'exportation de métriques de NetScaler vers Prometheus 1149

Utiliser des modèles de configuration pour créer des modèles d'audit 1152

Reprogrammer les jobs configurés à l'aide de modèles intégrés 1153

Réutiliser les modèles d'audit de configuration dans les tâches de configuration 1154

Importer et exporter des modèles de configuration 1157

Audit de configuration 1158

Afficher les rapports d'audit 1158

Auditer les modifications de configuration sur les instances 1162

Obtenir des conseils de configuration sur la configuration réseau 1166

Interroger l'audit de configuration des instances NetScaler® 1167

Générer un diff d'audit de configuration pour les traps SNMP ConfigChange 1168

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tâches de mise à niveau 1169
Validation avant la mise à niveau 1171
Vérifications avant la mise à niveau effectuées par NetScaler Console 1171
Vérifications avant la mise à niveau effectuées par NetScaler 1172
Planifier la mise à niveau des instances NetScaler 1172
Planifier la mise à niveau des instances NetScaler SDX 1176
Planifier la mise à niveau des instances NetScaler BLX 1177
Planifier la mise à niveau du groupe Autoscale™ 1180
Planifier la configuration d'une paire HA d'instances NetScaler 1180
Planifier la conversion d'une paire d'instances HA en cluster 1182
Utiliser les tâches pour mettre à niveau les instances NetScaler® 1183
Vérifications de pré-validation 1183
Paire haute disponibilité NetScaler 1184
Clusters NetScaler 1184
Créer une tâche de maintenance de mise à niveau pour mettre à niveau les instances NetScaler 1184
Suspendre ou reprendre une tâche de mise à niveau planifiée 1191
Relancer les tâches de mise à niveau ayant échoué 1191
Nettoyer l'espace disque NetScaler 1192
Planification des tâches de mise à niveau pour une paire haute disponibilité NetScaler 1193
Télécharger un rapport de différences combiné d'une tâche de mise à niveau NetScaler 1194
Avis de sécurité 1195
Page d'accueil des avis de sécurité 1195
Recommandations de configuration sécurisée 1197
Détection des CVE 1197
Surveillance de l'intégrité des fichiers 1197
Analyser maintenant 1197
Historique des analyses 1198

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler impactés 1198
Paramètres 1198
Recommandations de configuration sécurisée 1199
Priorisation basée sur la gravité 1200
Avantages d'une vue détaillée au niveau de l'instance 1200
Corriger les recommandations de configuration 1201
Détection des CVE 1204
Vue de l'instance 1205
Vue CVE 1207
Référentiel CVE 1208
Points à noter 1208
Surveillance de l'intégrité des fichiers 1210
Détecté par la console 1211
Rapporté par l'appareil 1212
Détection des indicateurs de compromission dans NetScaler Console 1213
Prérequis 1213
Avantages 1213
CVE pris en charge via l'avis de sécurité 1214
Derniers CVE pris en charge 1214
CVE prises en charge 1216
Identifier et corriger les vulnérabilités pour CVE-2026-88771 1219
Corriger CVE-2026-88771 1220
Identifier et corriger les vulnérabilités pour CVE-2026-88772 1220
Corriger CVE-2026-88772 1221
Identifier et corriger les vulnérabilités pour CVE-2026-88773 1221
Corriger CVE-2026-88773 1221
Identifier et corriger les vulnérabilités pour CVE-2026-88774 1222
Corriger CVE-2026-88774 1222

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identifier et corriger les vulnérabilités pour CVE-2026-88775 1223
Corriger CVE-2026-88775 1223
Identifier et corriger les vulnérabilités pour CVE-2026-88776 1223
Corriger CVE-2026-88776 1224
Identifier et corriger les vulnérabilités pour CVE-2026-88777 1224
Corriger CVE-2026-88777 1225
Corriger les vulnérabilités pour CVE-2026-88778 1225
Corriger CVE-2026-88778 1225
Identifier et corriger les vulnérabilités pour CVE-2026-19490 1227
Corriger CVE-2026-19490 1227
Identifier et corriger les vulnérabilités pour CVE-2026-19489 1228
Corriger CVE-2026-19489 1228
Corriger les vulnérabilités pour CVE-2026-13474 1228
Corriger CVE-2026-13474 1229
Identifier et corriger les vulnérabilités pour CVE-2026-10817 1231
Corriger CVE-2026-10817 1231
Identifier et corriger les vulnérabilités pour CVE-2026-10816 1232
Corriger CVE-2026-10816 1232
Identifier et corriger les vulnérabilités pour CVE-2026-8655 1232
Corriger CVE-2026-8655 1233
Identifier et corriger les vulnérabilités pour CVE-2026-8452 1233
Corriger CVE-2026-8452 1234
Identifier et corriger les vulnérabilités pour CVE-2026-8451 1234
Corriger CVE-2026-8451 1234
Identifier et corriger les vulnérabilités pour CVE-2026-4368 1235
Corriger CVE-2026-4368 1235
Identifier et corriger les vulnérabilités pour CVE-2026-3055 1236
Corriger CVE-2026-3055 1236

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identifier et corriger les vulnérabilités pour CVE-2025-12101 1236
Corriger CVE-2025-12101 1237
Identifier et corriger les vulnérabilités pour CVE-2025-8424 1237
Corriger CVE-2025-8424 1238
Identifier et corriger les vulnérabilités pour CVE-2025-7776 1239
Corriger CVE-2025-7776 1239
Identifier et corriger les vulnérabilités pour CVE-2025-7775 1240
Corriger CVE-2025-7775 1241
Identifier et corriger les vulnérabilités pour CVE-2025-6543 1241
Corriger CVE-2025-6543 1242
Identifier et corriger les vulnérabilités pour CVE-2025-5349 1243
Corriger CVE-2025-5349 1244
Corriger les vulnérabilités pour CVE-2025-5777 1244
Corriger CVE-2025-5777 1245
Corriger les vulnérabilités pour CVE-2024-8535 1247
Corriger CVE-2024-8535 1248
Corriger les vulnérabilités pour CVE-2020-8300 1250
Corriger CVE-2020-8300 1251
Scénario 1256
Corriger les vulnérabilités pour CVE-2021-22927 et CVE-2021-22920 1258
Corriger CVE-2021-22927 et CVE-2021-22920 1258
Scénario 1263
Identifier et corriger les vulnérabilités pour CVE-2021-22956 1264
Identifier les instances affectées par CVE-2021-22956 1264
Corriger CVE-2021-22956 1265
Identifier et corriger les vulnérabilités pour CVE-2022-27509 1268
Identifier les instances impactées par CVE-2022-27509 1269
Corriger CVE-2022-27509 1269

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE non prises en charge dans l'avis de sécurité 1270
Avis de mise à niveau 1271
Afficher l'avis de mise à niveau 1272
Définir les versions préférées 1272
Mettre à niveau les instances NetScaler 1273
Orchestration 1275
VMware NSX Manager 1276
OpenStack : Intégration des instances NetScaler 1277
Pilote NetScaler pour OpenStack Neutron LBaaS 1277
Enregistrement mutuel de NetScaler Console et OpenStack 1277
Locataires dans OpenStack 1278
Stratégies de placement 1278
Packages de services 1278
Fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2 1278
Scénario de cas d'utilisation 1279
Flux de travail d'intégration de NetScaler Console avec OpenStack 1280
OpenStack : Intégration des instances NetScaler 1281
Prérequis 1284
Tâches de pré-configuration dans NetScaler Console et OpenStack 1285
Configurer LBaaS V1 à l'aide de Horizon 1294
Configurer LBaaS V2 à l'aide de la ligne de commande 1295
Configurer la commutation de contenu de couche 7 1299
Provisionnement manuel d'une instance NetScaler VPX sur OpenStack 1307
Provisionnement d'une instance NetScaler VPX sur OpenStack à l'aide de StyleBook 1309
Prise en charge des licences VPX d'enregistrement et de retrait et des licences en pool pour l'environnement OpenStack 1311
Prise en charge du VLAN partagé pour les partitions d'administration 1312
Flux de travail de la licence d'essai 1314

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Intégrer avec les services OpenStack Heat 1314
Stratégies d'isolation des packages de services 1319
Allocation flexible de périphériques basée sur des politiques 1320
NSX Manager : provisionnement manuel des instances NetScaler 1324
Prérequis 1324
Exigences matérielles de VMware ESXi 1324
Configuration de VMware NSX 1325
Ajout d'une instance NetScaler VPX dans NetScaler Console 1326
Enregistrement de VMware NSX Manager auprès de NetScaler Console 1326
Création d'un package de service dans NetScaler Console 1327
Exécution de l'insertion de service d'équilibrage de charge pour Edge 1328
Affichage de la passerelle L2 sur NSX Manager 1330
Affichage du NetScaler alloué 1330
Configuration de l'instance NetScaler VPX à l'aide de StyleBook 1330
Affichage de la configuration de l'équilibreur de charge 1331
Suppression du service d'équilibrage de charge 1331
NSX Manager : approvisionnement automatique des instances NetScaler 1332
Présentation 1332
Prérequis 1332
Déploiement en haute disponibilité de NetScaler Console et des instances NetScaler 1333
Configuration des détails du point de terminaison HA de NetScaler Console 1333
Enregistrement de VMware NSX Manager auprès de NetScaler Console 1333
Chargement des licences dans NetScaler Console 1334
Téléchargement des images NetScaler VPX dans NetScaler Console 1335
Création de packages de services dans NetScaler Console 1335
Effectuer l'insertion de service d'équilibrage de charge pour Edge 1337
Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de VMware NSX Manager 1338

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de NetScaler Console 1340
Vérification de la création de serveurs virtuels et de groupes de services dans les instances NetScaler VPX 1340
Suppression des services d'équilibrage de charge 1341
Gérer la configuration Ingress de Kubernetes dans NetScaler Console 1341
Avant de commencer 1342
Configurer NetScaler Console avec un jeton secret pour gérer un cluster Kubernetes 1343
Ajouter le cluster Kubernetes dans NetScaler Console 1343
Paramètres 1345
Configurer la gestion des adresses IP (IPAM) 1345
Ajouter un fournisseur d'adresses IP externe 1346
Infoblox DDI en tant que fournisseur externe 1347
Ajouter un réseau 1348
Afficher les adresses IP allouées 1349
Configurer une politique d'action pour recevoir des notifications d'événements d'application 1349
Configurer une stratégie d'action 1351
Utiliser la barre de recherche 1363
Utiliser l'option des journaux d'audit 1363
Intégration de l'observabilité 1363
Intégration avec Splunk 1363
Configurer Splunk pour recevoir des données de NetScaler Console sur site 1364
Configurer NetScaler Console sur site pour exporter des données vers Splunk 1368
Afficher les tableaux de bord dans Splunk 1369
Intégration avec New Relic 1371
Prérequis 1371
Tableau de bord New Relic 1373
Intégration avec Microsoft Sentinel 1373

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer l'espace de travail Log Analytics 1374
Créer une application Microsoft Entra 1375
Configurer le point de terminaison de collecte de données 1376
Créer des tables pour exporter des données 1376
Créer un abonnement dans NetScaler Console 1390
Afficher les journaux dans Microsoft Azure 1391
Configurer les instances NetScaler® pour l'exportation d'informations vers Prometheus à l'aide du schéma par défaut 1392
Afficher les journaux des configurations échouées 1393
Configurer l'exportation des métriques et des journaux d'audit NetScaler® vers Splunk 1393
Afficher les journaux des configurations ayant échoué 1394
Listes de contrôle d'accès 1394
Directives d'utilisation 1394
Comment configurer une ACL 1395
Activer la fonctionnalité ACL 1395
Créer une règle ACL 1395
Activer une règle ACL 1396
Autres actions pour les règles ACL 1397
Désactiver une règle ACL 1397
Modifier une règle ACL 1397
Supprimer une règle ACL 1398
Renuméroter les priorités des règles ACL 1398
Dépannage 1399
Utiliser les journaux d'audit de NetScaler Console pour gérer et surveiller votre infrastructure 1399
Journaux d'audit liés à l'instance NetScaler 1399
Configurer le service NetScaler Console comme serveur syslog 1400
Journaux d'audit liés à NetScaler Console 1400
Configuration d'un serveur syslog pour surveiller les journaux d'audit et de shell 1400

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Journaux d'audit liés aux applications 1401
Licences NetScaler 1402
Service d'activation de licence 1402
Compatibilité des versions de NetScaler pour LAS 1404
Transition vers le LAS 1405
Activer le LAS avec Cloud Connect 1405
Licencier ou migrer des instances NetScaler vers LAS 1407
Comportement du blob d'activation de licence 1411
Alerte de période de grâce de la licence 1411
Comportement mis à jour de NetScaler lorsque la connectivité est interrompue entre la console sur site et le service de console 1411
Informations envoyées à LAS pendant le flux de travail de licence LAS 1413
Bonnes pratiques pour la surveillance de votre environnement NetScaler Console sur site connecté au cloud ayant migré vers LAS 1414
Prérequis 1414
Surveiller l'expiration du blob d'activation LAS de Console sur site 1415
Surveiller la dernière date de renouvellement à l'aide de l'interface graphique 1415
Surveiller l'expiration du blob d'activation LAS des instances NetScaler (NetScaler sous licence via Console sur site connectée au cloud) 1417
Afficher l'état de l'instance NetScaler à l'aide de la CLI 1417
Notifications 1417
Surveiller l'expiration des droits de licence 1419
Notifications 1419
Notifications par e-mail 1419
Gestion des licences 1420
Licence basée sur LAS 1421
Ports du serveur de licences 1421
Informations sur l'expiration des licences 1422

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Paramètres de notifications 1423

Prise en charge RBAC pour LAS 1425

Droits gérés manuellement (licences basées sur des fichiers) 1426

Fichiers de licence 1426

Points importants à noter 1427

Paramètres de port du serveur de licences 1429

Informations sur l'expiration de la licence 1429

Paramètres de notification 1430

Capacité minimale et maximale pour les licences Flexed et Pooled 1433

Tableau 1. Capacité Flexed prise en charge pour MPX 1435

Tableau 2A. Capacité Flexed prise en charge pour NetScaler SDX version antérieure à la build 13.0-47.x 1436

Tableau 2B. Capacité Flexed prise en charge pour NetScaler SDX version 13 (build 13.0-47.x et versions ultérieures), version 13.1 (build antérieure à 51.x) et version 14.1 (build antérieure à 12.x) 1437

Tableau 2C. Capacité Flexed prise en charge pour NetScaler SDX version 13.1 (build 51.x et ultérieure) et version 14.1 (build 12.x et ultérieure) 1438

Tableau 3. Bande passante minimale/maximale et instances minimales/maximales prises en charge pour les instances NetScaler CPX 1440

Tableau 4. Bande passante minimale/maximale et instances minimales/maximales prises en charge pour les instances NetScaler VPX sur les hyperviseurs et les services cloud 1440

Tableau 5. Bande passante minimale/maximale prise en charge et instances minimales/maximales pour les instances NetScaler BLX 1441

Tableau 6. Exigence de licence de capacité zéro pour différents facteurs de forme 1441

Licence de capacité Flexed 1442

Matériel à capacité nulle 1443

Gérer et installer les licences Z-cap 1444

Instances NetScaler VPX autonomes 1444

Instances autonomes NetScaler CPX 1445

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instances autonomes NetScaler BLX 1446
Pool de bande passante 1446
Pool d'instances 1446
Configurer la licence 1447
Licences basées sur LAS 1449
Étape 1 : Activer LAS et récupérer les droits 1449
Étape 2 : Ajouter des instances NetScaler à NetScaler Console On-prem 1449
Étape 3 : Licencier ou migrer des instances NetScaler 1449
Étape 4 : Modifier la capacité de débit flexible 1449
Licences spéciales pour les appliances MPX sans licence 1450
Comportement du blob d'activation de licence 1451
Alerte de période de grâce de la licence 1451
Droit géré manuellement (licences basées sur des fichiers) 1451
Avant de commencer 1451
Étape 1 - Appliquer les licences dans NetScaler Console 1452
Étape 2 - Enregistrer NetScaler Console en tant que serveur de licences et allouer des licences 1452
Étape 3 - Modifier la capacité de débit flexible pour les instances NetScaler 1454
NetScaler MPX-Z 1455
NetScaler SDX-Z 1455
Exigences de licence pour la paire haute disponibilité NetScaler (commun aux licences LAS et basées sur des fichiers) 1456
États de licence Flexed NetScaler (commun aux licences LAS et basées sur des fichiers) 1456
Tableau de bord des licences Flexed 1457
Modifier la capacité de débit allouée sur une instance NetScaler 1459
Libérer des licences sur une instance NetScaler 1460
Rapports de licences Flexed 1460
Transition vers les licences Flexed 1464

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licences basées sur LAS 1465
Droits gérés manuellement (licences basées sur des fichiers) 1466
Licence de bande passante en pool vers licence Flexed 1466
vCPU en pool vers la capacité de bande passante Flexed 1467
Abonnement fixe ou licence perpétuelle vers licence Flexed 1467
CICO vers la capacité de bande passante Flexed 1468
Scénarios pour l'expiration des licences Flexed ou Pooled et le comportement en cas de problèmes de connectivité 1469
Licences basées sur le LAS 1470
Avant l'expiration du terme 1470
Après l'expiration du terme 1470
Scénarios de comportement en cas de problèmes de connectivité 1470
Licence gérée manuellement (licence basée sur un fichier) 1471
Types de licences Flexed 1471
Scénario : Facteur de forme MPX 1471
Scénario : Facteur de forme SDX 1472
Scénario : Facteur de forme VPX/BLX/CPX 1472
Scénarios de comportement en cas de problèmes de connectivité 1473
Configurer le serveur NetScaler Console en tant que serveur de licences Flexed ou Pooled 1473
Comment configurer le serveur NetScaler Console uniquement comme serveur de licences Flexed ou Pooled 1475
Licences héritées 1476
Capacité mutualisée NetScaler 1477
Fonctionnement de la licence de capacité mutualisée NetScaler 1478
Matériel à capacité nulle 1479
Instances NetScaler VPX autonomes 1479
Instances NetScaler CPX autonomes 1480
Instances NetScaler BLX autonomes 1481

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pool de bande passante 1481

Pool d'instances 1481

Serveur de licences NetScaler Console 1481

Configurer la capacité groupée NetScaler 1487

Versions matérielles et logicielles prises en charge 1488

États de la capacité en pool NetScaler 1488

Étape 1 - Appliquer les licences dans NetScaler Console 1489

Étape 2 - Enregistrer NetScaler Console en tant que serveur de licences 1490

Étape 3 - Allouer des licences groupées aux instances NetScaler 1493

Configurer la capacité en pool sur les instances NetScaler 1494

Mettre à niveau une licence perpétuelle dans NetScaler VPX vers la capacité groupée NetScaler 1496

Prérequis 1497

Mettre à niveau la licence perpétuelle dans une paire haute disponibilité NetScaler VPX vers la capacité groupée NetScaler 1498

Mise à niveau d'une licence perpétuelle dans NetScaler MPX vers la capacité groupée NetScaler 1500

Mise à niveau de la licence perpétuelle dans une paire haute disponibilité NetScaler MPX vers la capacité groupée NetScaler 1503

Mettre à niveau une licence perpétuelle dans un NetScaler SDX vers la capacité groupée NetScaler 1506

Capacité groupée NetScaler sur les instances NetScaler en mode cluster 1509

Allouer la capacité groupée NetScaler à un cluster NetScaler 1510

Allouer la capacité groupée NetScaler à un cluster NetScaler à l'aide de l'interface de ligne de commande 1512

Archiver et extraire les licences NetScaler VPX et NetScaler BLX 1513

Prérequis 1514

Installation des licences dans NetScaler Console 1514

Vérification 1515

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface graphique de NetScaler 1515

Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface de ligne de commande NetScaler 1516

Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'API 1517

Mettre à jour l'adresse IP d'un serveur de licences 1518

Configurer les vérifications d'expiration pour les licences d'enregistrement et de retrait NetScaler VPX et NetScaler BLX 1519

Licences de processeur virtuel NetScaler 1520

Licences de CPU virtuel pour NetScaler VPX 1521

Configuration d'un serveur de licences dans la licence NetScaler VPX à l'aide de l'interface de ligne de commande 1523

Gestion des licences de CPU virtuelles sur NetScaler Console 1523

Licences de CPU virtuelles pour NetScaler CPX 1524

Comportements attendus en cas de problèmes 1526

Le serveur de licences ne répond plus 1527

L'instance NetScaler en pool cesse de répondre 1528

Le serveur de licences et l'instance NetScaler en pool cessent de répondre 1528

L'instance NetScaler en pool s'arrête correctement 1528

Problèmes de connectivité réseau 1529

Période de grâce 1529

Gérer les paramètres système 1530

Configurations réseau 1530

Configurations système 1531

Maintenance du système 1533

Élagage des données 1533

Sauvegarde 1534

Notifications d'événements 1535

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Paramètres SSL 1535
Configurer les fonctionnalités 1536
Configurer les paramètres de sauvegarde du système 1536
Configurer les paramètres du serveur proxy 1537
Points à noter 1537
Configuration du serveur proxy 1537
Gérer le certificat CA 1539
Prise en charge de la configuration proxy 1539
Pas de proxy (Accès Internet direct) 1540
Proxy explicite de transfert (Non interceptant) 1540
Proxy SSL-interceptant explicite 1540
Proxy SSL-interceptant transparent 1540
Configurer un serveur NTP 1541
Mettre à niveau NetScaler Console 1542
Vérifications avant la mise à niveau 1543
Déblocage de la mise à niveau de NetScaler Console lorsque la vérification préalable à la mise à niveau LAS échoue 1545
Comment réinitialiser le mot de passe de NetScaler Console 1546
Configurer une carte réseau secondaire pour accéder à NetScaler Console 1550
Prérequis 1551
Configurer une deuxième carte réseau dans NetScaler Console 1551
Configurer une carte réseau secondaire pour accéder à l'agent NetScaler® 1552
Modifier les adresses réseau des cartes réseau IPV4 à l'aide de la CLI 1552
Configurer l'intervalle de purge du syslog 1553
Configurer les paramètres de purge du système et des événements 1554
Configurer les paramètres de purge des événements à l'aide de NetScaler Console 1555
Activer l'accès shell pour les utilisateurs non par défaut 1556
Récupérer les serveurs NetScaler Console inaccessibles 1557

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment utiliser le script de récupération de base de données NetScaler Console pour un déploiement autonome de NetScaler Console 1557

Comment utiliser le script de récupération de la base de données NetScaler Console pour un déploiement NetScaler Console à haute disponibilité 1559

Attribuer un nom d'hôte à un serveur NetScaler Console 1559

Sauvegarder et restaurer votre serveur NetScaler Console 1560

Sauvegarder la configuration de NetScaler Console 1561

Transférer un fichier de sauvegarde NetScaler Console vers un système externe 1562

Restaurer la configuration de NetScaler Console à partir d'un fichier de sauvegarde 1563

Instantanés de VM de NetScaler Console dans un déploiement haute disponibilité 1564

Prendre un instantané des serveurs NetScaler Console 1564

Restaurer un instantané des serveurs NetScaler Console 1565

Afficher les informations d'audit 1565

Configurer les paramètres SSL 1566

Surveiller l'utilisation du CPU, de la mémoire et du disque 1567

Configurer les paramètres de notification 1567

Créer une liste de distribution d'e-mails 1568

Créer une liste de distribution SMS 1569

Créer un profil Slack 1569

Créer un profil PagerDuty 1570

Afficher le profil ServiceNow 1571

Générer un fichier de support technique 1571

Configurer un groupe de chiffrements 1573

Créer une destination de trap SNMP, une communauté de gestionnaires et des utilisateurs 1574

Configurer et afficher les alarmes système 1575

Ajouter des limites de seuil aux alarmes d'utilisation du disque 1577

Créer des gestionnaires et des utilisateurs SNMP pour l'agent NetScaler 1577

Ajouter un gestionnaire SNMP v2 1578

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter un gestionnaire SNMP v3 1578
Ajouter un utilisateur SNMP 1579
Gestion des vues SNMP 1580
Configurer les paramètres de l'agent 1580
Définir l'intervalle de maintien en vie de l'agent 1580
Modifier le mot de passe de l'agent sans le mot de passe actuel 1581
Utiliser le tableau de bord de gestion du stockage des données 1581
Comprendre votre stockage de données 1582
État de votre activité d'ingestion de données 1583
Consommation totale de stockage 1583
Tendances de consommation du stockage 1584
Consommation de stockage par fonctionnalités 1586
Gérer votre espace de stockage 1587
Effectuer l'élagage des données 1587
Examiner la politique de rétention des données 1588
Notifier en cas de dépassement de la limite de stockage 1588
Politique de rétention des données 1589
Configurer les paramètres de purge du système 1589
Configurer les paramètres de purge des événements d'instance 1590
Configurer les paramètres de purge des journaux système d'instance 1590
Configurer les paramètres de purge des rapports réseau 1591
NetScaler Console en tant que serveur proxy d'API 1592
Comment NetScaler Console fonctionne en tant que serveur proxy d'API 1592
Comment utiliser NetScaler Console comme serveur proxy API 1594
Exemple 1 : Récupérer les statistiques du serveur virtuel d'équilibrage de charge 1597
Exemple 2 : Créer un serveur virtuel d'équilibrage de charge 1598
Exemple 3 : Modifier un serveur virtuel d'équilibrage de charge 1598
Exemple 4 : Supprimer un serveur virtuel d'équilibrage de charge 1599

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple 5 : Télécharger la configuration CLI en cours d'exécution sur le NetScaler 1599

FAQ 1601

Analytique 1601

Est-il nécessaire d'activer le canal virtuel EUEM sur les instances NetScaler Gateway déployées en mode à saut unique ? 1601

Comment activer NetScaler Console pour surveiller le trafic des applications web et des bureaux virtuels ? 1601

Après avoir ajouté les instances NetScaler, NetScaler Console commence-t-il automatiquement à collecter des informations analytiques ? 1602

Est-il nécessaire d’accéder à l’appliance NetScaler individuelle pour activer l’analyse ? 1602

Quels sont les types de serveurs virtuels qui peuvent être répertoriés sur une instance NetScaler pour activer l’analyse ? 1602

Comment attacher un disque supplémentaire à NetScaler Console ? 1603

Que signifie « les collecteurs ne sont pas configurés sur les instances NetScaler » ? 1603

À quoi sert l'activation des mesures côté client ? 1603

Authentification 1604

Qu'est-ce que l'équilibrage de charge des requêtes d'authentification ? 1604

Pourquoi devons-nous cascader les serveurs d'authentification externes ? 1604

Combien de serveurs d'authentification externes puis-je cascader ? 1604

Ai-je une alternative lorsque l'authentification externe échoue ? 1604

Qu'est-ce que l'authentification locale de secours ? 1604

Qu'est-ce qu'une extraction de groupes d'utilisateurs externes ? 1605

Pourquoi devons-nous attribuer des autorisations de groupe ? 1605

Gestion de la configuration 1606

Puis-je effectuer une configuration sur plusieurs instances NetScaler simultanément à l'aide de NetScaler Console ? 1606

Que sont les tâches de configuration sur NetScaler Console ? 1606

Puis-je planifier des tâches à l'aide de modèles intégrés dans NetScaler Console ? 1606

Gestion des certificats 1606

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La suppression des certificats SSL de NetScaler Console entraîne-t-elle la suppression des certificats des instances NetScaler ? 1606

Déploiement 1607

Quel est le nom d'utilisateur et le mot de passe par défaut ? 1607

Comment changer le mot de passe par défaut ? 1607

Comment réinitialiser le mot de passe ? 1608

Dans une paire HA, si le mot de passe est modifié sur le nœud principal et si l'option « Rompre la paire HA » est sélectionnée ultérieurement, quel est le comportement ? 1608

Si deux serveurs autonomes ont des mots de passe différents, quel est l'impact lors du déploiement de ces deux serveurs en paire HA ? 1608

La configuration HA est terminée, mais l'interface graphique du nœud principal n'est pas accessible. Quelle peut en être la raison ? 1608

La configuration HA est terminée, mais l'interface graphique de l'adresse IP flottante n'est pas accessible. Quelle peut en être la raison ? 1608

Quelle base de données est prise en charge dans NetScaler Console autonome et NetScaler Console HA ? 1608

Quelle est la perte de données potentielle pour le nœud secondaire ? 1608

Que se passe-t-il si le nœud principal est hors service ? 1609

Comment réinstaller le nœud défaillant ? 1609

NetScaler Console prend-il en charge le stockage SAN ? 1609

NetScaler Console prend-il en charge un disque supplémentaire ? 1609

Après avoir désactivé la paire HA, qu'advient-il de l'adresse IP flottante configurée ? 1610

Puis-je attribuer une adresse IP flottante différente lors du redéploiement ? 1610

Pourquoi l'interface graphique du nœud secondaire n'est-elle pas accessible ? 1610

Si le nœud principal est en panne pendant une longue période, les configurations peuvent-elles toujours être effectuées à l'aide de l'interface graphique de l'adresse IP flottante ? 1610

S'il est nécessaire de modifier l'adresse IP du nœud principal, l'adresse IP du nœud secondaire ou l'adresse IP flottante à l'avenir (par exemple, en la remplaçant par IPv6), quelles sont les solutions recommandées à suivre ? 1610

NetScaler Console prend-il en charge les processeurs AMD ? 1611

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Déploiement (reprise après sinistre) 1611

À quelle fréquence la réplication a-t-elle lieu entre le site principal et le site de reprise après sinistre ? 1611

Après avoir initié le script de sauvegarde sur le site de reprise après sinistre, le site de reprise après sinistre devient-il le site principal temporaire, jusqu'à ce que le site principal soit récupéré et entièrement opérationnel ? 1611

Si l'option Rompre la paire HA est sélectionnée, les deux nœuds fonctionnent comme un serveur autonome. Étant donné que la prise en charge de la reprise après sinistre n'est pas applicable pour un serveur autonome, qu'advient-il du site de reprise après sinistre si l'option Rompre la paire HA est sélectionnée ? 1612

Gestion des événements 1612

Comment puis-je suivre tous les événements générés sur mes instances NetScaler gérées à l'aide de NetScaler Console ? 1612

Que sont les règles d'événement ? 1612

Gestion des instances 1613

Que se passe-t-il si une instance NetScaler ne peut pas se connecter à NetScaler Console après l'allocation de bande passante lorsque vous utilisez la licence de capacité groupée NetScaler ? 1613

Que sont les centres de données dans NetScaler Console ? 1613

Quels sont les différents dispositifs NetScaler pris en charge par NetScaler Console ? 1613

Qu'est-ce qu'un profil d'instance ? 1614

Puis-je redécouvrir plusieurs instances NetScaler VPX dans NetScaler Console ? 1614

NetScaler Console peut-il être installé sur NetScaler SDX ? 1614

Puis-je ajouter une instance NetScaler au logiciel NetScaler Console en utilisant une adresse IP publique ? 1614

Comment enregistrer un nœud de reprise après sinistre si les informations d'identification du nœud DR sont modifiées ? 1615

StyleBooks 1615

Les StyleBooks peuvent-ils être utilisés pour configurer différentes instances NetScaler exécutant différentes versions du logiciel NetScaler ? 1615

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsqu'un StyleBook est utilisé pour configurer plusieurs instances NetScaler simultanément, et que la configuration d'une instance NetScaler échoue, que se passe-t-il ? 1615

Les sauvegardes NetScaler effectuées via NetScaler incluent-elles les configurations appliquées via les StyleBooks ? 1615

Gestion du système 1616

Puis-je attribuer un nom d'hôte à mon serveur NetScaler Console ? 1616

Puis-je sauvegarder et restaurer ma configuration NetScaler Console ? 1616

Que sont les seuils et les alertes sur NetScaler Console ? 1616

Puis-je générer un fichier de support technique pour NetScaler Console ? 1616

Qu'est-ce que la purge de syslog ? 1617

Puis-je configurer un serveur NTP sur NetScaler Console ? 1617

À partir de quelle version le déploiement HA actif-passif de NetScaler Console est-il pris en charge ? 1617

J'avais une configuration HA actif-actif de NetScaler Console et j'avais configuré une appliance NetScaler avec un serveur virtuel d'équilibrage de charge dessus pour un accès GUI unifié. Comment mettre à jour cette configuration ? 1618

Puis-je configurer l'équilibrage de charge de la paire HA NetScaler Console sur une instance NetScaler en utilisant le port 443 ? 1618

Un fichier de sauvegarde de serveur NetScaler Console peut-il être utilisé pour restaurer la configuration d'un autre serveur NetScaler Console ? 1618

Après que NetScaler Console a sauvegardé une instance NetScaler, ce fichier de sauvegarde peut-il être utilisé pour restaurer la configuration d'une autre instance NetScaler via NetScaler Console ? 1618

Pouvons-nous forcer NetScaler Console à utiliser une adresse SNIP pour communiquer avec les instances NetScaler, au lieu d'utiliser l'adresse NSIP du serveur NetScaler Console ? 1619

Lorsque je sauvegarde des instances NetScaler dans NetScaler Console, le résultat est-il une sauvegarde complète ou une sauvegarde de base ? 1619

Existe-t-il un guide de dépannage pour NetScaler Console ? 1619

Comment les instances NetScaler sont-elles gérées lorsqu'un basculement HA de NetScaler Console se produit ? 1619

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Que se passe-t-il lorsque le nœud HA de NetScaler Console qui est tombé en panne redémarre ? 1620

Comment les instances NetScaler sont-elles distribuées entre les nœuds HA de NetScaler Console ? 1620

Comment les licences de serveur virtuel sont-elles gérées en cas de basculement HA de NetScaler Console ? 1620

Un équilibreur de charge est-il obligatoire pour une configuration HA de NetScaler Console ? 1620

NetScaler Console prend-il en charge une base de données externe ? 1620

Une instance NetScaler gérée par NetScaler Console peut-elle être utilisée comme équilibreur de charge pour NetScaler Console HA ? 1620

Quelles données sont synchronisées entre les nœuds HA de NetScaler Console ? 1621

index 1622

Configurer les seuils adaptatifs 1623

Pour créer un seuil adaptatif à l'aide de NetScaler Console 1623

Configurer la synthèse de base de données 1623

Pour configurer la synthèse de base de données 1624

Configurer la gestion des SLA 1624

Pour configurer la violation de SLA pour une instance NetScaler 1624

Créer des seuils et des alertes 1625

Pour créer un seuil et une alerte à l'aide de NetScaler Console 1625

Désactiver la collecte de données d'URL 1626

Pour désactiver la collecte de données d'URL depuis NetScaler Console 1626

Présentation de Logstream 1626

Activer Logstream comme mode de transport 1627

Tableaux de bord 1628

Tableau de bord du trafic sortant 1629

Afficher le trafic sortant du réseau 1629

Tableau de bord utilisateur 1630

Investigateur d'activité utilisateur 1630

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Transactions utilisateur 1631
Score de risque 1632
Toutes les violations 1633
Catégories de violations 1633
Tableau de bord des violations de sécurité 1635
Détails de la violation 1635
Vue d'ensemble de l'application 1636
Catégories de violations 1636
Afficher les détails de la violation WAF 1638
Afficher les détails de la violation de bot 1639
Afficher l'historique des événements 1640
Détails de la violation réseau 1640
HTTP Slow Loris 1640
DNS Slow Loris 1641
HTTP Slow Post 1641
Attaque par inondation NXDOMAIN 1642
Attaque de désynchronisation HTTP 1643
Attaque Bleichenbacher 1644
Attaque Segment Smack 1644
Attaque par inondation SYN 1645
Attaque par petite fenêtre 1646
SSL Insight 1646
Prérequis 1647
Configurer SSL Insight 1648
Activer la fonctionnalité AppFlow 1648
Activer les paramètres SSL Insight 1650
Afficher les métriques SSL Insight 1650
Cas d'utilisation : Obtenir un aperçu des transactions SSL 1651

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cas d'utilisation : Métriques SSL pour les clients 1651
Résoudre les problèmes de Web Insight 1652
Diagnostics en cas d'absence de données 1652
Problèmes liés aux rapports du tableau de bord Web Insight 1652
Problème de configuration 1652
Problème de connectivité entre NetScaler et NetScaler Console 1653
Données AppFlow non reçues de NetScaler® 1653
Problème de licence 1654
Problème d'ID de point d'observation 1654
Problème de paramètres AppFlow manquants 1655
Dépanner à l'aide de compteurs 1655
Afficher les analyses pour les transactions web 1656
Transactions web détaillées 1656
Afficher les événements 1657
Ajouter des colonnes dans la liste des événements 1659
Recherche avancée 1659
Enregistrer la recherche 1661
Exporter les données 1661
Procédures détaillées pour configurer une topologie à deux niveaux ou de maillage de services léger 1662
Exigences logicielles 1662
Avant de commencer 1662
Exigences logicielles 1663
Avant de commencer 1663
Configurer les routes statiques dans NetScaler Console 1664
Télécharger les fichiers de déploiement d'exemple depuis GitHub 1665
Ajouter des paramètres dans le fichier YAML CPX 1665
Ajouter une instance VPX, SDX, MPX ou BLX dans NetScaler Console 1667

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter un cluster Kubernetes dans NetScaler Console 1667
Déployer un exemple d'application de microservice 1669
Déployer CPX et enregistrer CPX dans NetScaler Console 1669
Activer la sélection automatique des serveurs virtuels pour la gestion des licences 1669
Activer les paramètres de transaction Web et de transaction TCP 1670
Envoyer du trafic vers les microservices 1670
Procédures détaillées pour configurer la topologie de maillage de services 1671
Configurer les routes statiques dans NetScaler Console 1671
Configurez les paramètres requis 1672
Déployer une application exemple 1674
Ajouter un cluster Kubernetes dans NetScaler Console 1676
Activer la sélection automatique des serveurs virtuels pour la licence 1677
Activer les paramètres de transaction Web et de transaction TCP 1678
Envoyer du trafic aux microservices 1678
Gouvernance des données (pour NetScaler Console entre les versions 14.1-8.x et 14.1-21.x) 1679
Catégories de données 1679
Gouvernance des données (pour NetScaler ADM 14.1-4.42 ou versions antérieures) 1680
Configurer l'identité client 1681
Flux de travail 1 - Si vous êtes un nouvel utilisateur 1681
Flux de travail 2 - si vous êtes un utilisateur existant effectuant une mise à niveau vers la dernière version d'ADM 1681
Diagnostics et collecte de données 1682
Pourquoi les données sont-elles collectées ? 1683
Qui peut utiliser ces données ? 1683
Combien de temps conservons-nous vos données ? 1683
Optimisation de la base de données à l'aide de scripts de maintenance 1684
Programme d'amélioration de l'expérience utilisateur client 1684
Quelles données d'utilisation sont collectées via CUXIP ? 1684

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment CUXIP vous aide-t-il ? 1685
Comment fonctionne CUXIP ? 1685
Comment désactiver CUXIP sur mon ADM ? 1685
Modifications de notre politique de confidentialité 1685
Références 1685
Données de télémétrie facultatives pour Cloud Connect 1686
Données de télémétrie facultatives pour le programme de télémétrie NetScaler® 1691
Utilisation des fonctionnalités de NetScaler Console 1691
Données de télémétrie requises pour Cloud Connect 1698
Données de télémétrie requises pour le programme de télémétrie NetScaler® 1704
Licences 1704
Haute disponibilité 1709
Comment les licences sont-elles synchronisées entre les nœuds haute disponibilité de NetScaler Console ? 1710
Orchestration 1710
Mettre à niveau les licences de serveur virtuel 1711
Vérification 1711
Gérer les serveurs virtuels 1711
Désactiver l'attribution automatique de licences aux serveurs virtuels 1712
Sélectionner des serveurs virtuels tiers pour l'attribution de licences 1712
Appliquer manuellement les licences de serveurs virtuels 1712
Configurer la licence de serveur virtuel basée sur une stratégie 1713
Afficher les serveurs virtuels sous licence 1713
Configurer la prise en charge automatique des licences pour les serveurs virtuels non adressables 1714
Sauvegarder et restaurer une configuration NetScaler Console dans une paire HA 1714
Configurer les paramètres de notification système 1715
Configurer les sites pour les géocartes 1718

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fix	1720

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Notes de publication

Les notes de publication de NetScaler Console 14.1 décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes et les problèmes connus dans une version. Le document des notes de publication pour la version 14.1 comprend les sections suivantes :

- **Nouveautés** : Les nouvelles fonctionnalités et les améliorations apportées aux fonctionnalités existantes publiées dans une version.
- **Problèmes connus** : Les problèmes existants dans une version et leurs solutions de contournement, le cas échéant.
- **Problèmes résolus** : Les problèmes résolus dans une version.

REMARQUE :

Ces notes de publication ne documentent pas les correctifs liés à la sécurité. Pour une liste des correctifs et avis de sécurité, consultez le bulletin de sécurité. Le NetScaler Console Security Advisory prend en charge l'identification et la correction des CVE. Pour plus d'informations sur les CVE prises en charge les plus récentes et existantes, consultez CVE prises en charge via l'avis de sécurité.

Pour consulter le document des notes de publication d'une version spécifique de la version 14.1, cliquez sur le lien correspondant dans le tableau suivant. Lorsque les notes de publication sont mises à jour pour une version, la date de publication est également mise à jour. La date de publication des notes de publication peut ne pas être la même que la date de disponibilité générale de la version.

NOTES DE PUBLICATION POUR LE LOGICIEL NETSCALER CONSOLE SUR SITE VERSION 14.1	DATE DE PUBLICATION
Build 14.1-73.36	Sep 01, 2026
Build 14.1-72.57	May 27, 2026
Build 14.1-66.72	Apr 24, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOTES DE PUBLICATION POUR LE LOGICIEL NETSCALER CONSOLE SUR SITE VERSION 14.1	DATE DE PUBLICATION
Build 14.1-60.57	Jan 20, 2026
Build 14.1-56.71	Dec 05, 2025
Build 14.1-51.83	Dec 05, 2025
Build 14.1-47.46	Jul 02, 2025
Build 14.1-43.50	Feb 27, 2025
Build 14.1-38.53	Dec 18, 2024
Build 14.1-34.43	Oct 28, 2024
Build 14.1-29.63	Aug 19, 2024
Build 14.1-25.56	Jul 09, 2024
Build 14.1-21.60	Apr 28, 2024
Build 14.1-17.38	Mar 18, 2024
Build 14.1-12.34	Dec 19, 2023
Build 14.1-8.50	Oct 10, 2023
Build 14.1-4.42	Aug 07, 2023

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrer NetScaler Console sur site vers Citrix Cloud

Vous pouvez migrer **NetScaler ADM 13.0 64.35 ou une version ultérieure** vers Citrix Cloud. Si votre NetScaler ADM est en version 12.1 ou antérieure, vous devez d'abord effectuer une mise à niveau vers la version **13.0 64.35 ou ultérieure**, puis migrer vers Citrix Cloud. Pour plus d'informations, consultez la section Mise à niveau.

REMARQUE :

Le service NetScaler® ADM est désormais renommé service NetScaler Console. L'interface utilisateur et la documentation de notre produit sont actuellement en cours de mise à jour pour refléter ces changements. Pendant cette période, il est possible que les anciens et les nouveaux noms soient utilisés de manière interchangeable. Nous vous remercions de votre compréhension pendant cette transition.

Le service NetScaler Console via Citrix Cloud™ vous permet d'obtenir :

- Des versions plus rapides, environ toutes les deux semaines avec les dernières mises à jour de fonctionnalités.
- Des analyses basées sur l'apprentissage automatique pour la sécurité des applications et des bots, les performances et l'utilisation.
- Diverses autres fonctionnalités qui ne sont actuellement prises en charge que dans le service NetScaler Console, telles que l'analyse des périodes de pointe et creuses, l'analyse basée sur l'apprentissage automatique pour la sécurité des applications et des bots, l'analyse du CPU des applications, et bien d'autres.

Pour une migration réussie, vous devez :

- Assurez-vous que NetScaler Console sur site dispose d'une connexion Internet pour l'accessibilité à Citrix Cloud.
- Configurer l'agent NetScaler.
- Obtenir le fichier CSV client et secret depuis Citrix Cloud.
- Valider la licence NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Migrer à l'aide d'un script.

Après avoir migré de NetScaler Console sur site vers le service NetScaler Console, si vous souhaitez revenir à NetScaler Console sur site, vous pouvez utiliser le script de restauration. Pour plus d'informations, consultez Revenir à NetScaler Console sur site.

Configurer l'agent NetScaler

Pour permettre les communications entre les instances NetScaler et le service NetScaler Console, vous devez configurer un agent. Les agents NetScaler sont, par défaut, automatiquement mis à niveau vers la dernière version. Vous pouvez également sélectionner une heure spécifique pour la mise à niveau de l'agent. Pour plus d'informations, consultez Configuration des paramètres de mise à niveau de l'agent.

- Si votre NetScaler Console sur site existant (autonome ou paire HA) n'a pas d'agents configurés, vous devez configurer au moins un agent pour le service NetScaler Console.
- Si votre NetScaler Console sur site existant (autonome ou paire HA) est configuré avec des agents sur site pour des déploiements multisites, vous devez configurer le même nombre d'agents pour le service NetScaler Console.

Pour plus d'informations sur la configuration d'un agent, consultez la section Mise en route.

Obtenir le fichier CSV client et secret depuis Citrix Cloud

Après avoir configuré l'agent, obtenez le fichier CSV client et secret depuis la page Citrix Cloud :

1. Connectez-vous à citrix.cloud.com
2. Cliquez sur l'icône **Accueil** et sélectionnez **Gestion des identités et des accès**
3. Dans l'onglet **Accès API**, saisissez un nom de client sécurisé et cliquez sur **Créer un client**.
4. L'ID et le secret sont générés. Cliquez sur **Télécharger** et enregistrez le fichier CSV dans NetScaler Console sur site.

   Par exemple, enregistrez le fichier CSV dans le répertoire /var.

Valider les licences du service NetScaler Console

Vous devez obtenir des licences pour le service NetScaler.

- Les licences VIP du service NetScaler Console doivent être supérieures ou égales aux licences VIP sur site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si les licences VIP sont inférieures, les serveurs virtuels sont sélectionnés aléatoirement et la configuration au niveau VIP pour le service NetScaler Console échoue.

- Si vous utilisez le déploiement NetScaler Console sur site comme serveur de licences, réallouez vos licences au service NetScaler Console avant la migration. Pour plus d'informations, consultez Comment réallouer un fichier de licence.
- Si vous utilisez les licences en pool dans NetScaler Console sur site, vous devez obtenir les licences en pool pour le service NetScaler Console, puis allouer des licences aux instances NetScaler. Pour plus d'informations, consultez Configurer les licences en pool. Les versions NetScaler prises en charge suivantes vous permettent de modifier l'allocation de licences depuis NetScaler Console :
  - NetScaler SDX : 13.0 74.11 ou versions ultérieures.
  - NetScaler VPX et MPX : 13.0 47.24 ou versions ultérieures, 12.1 58.14 ou versions ultérieures, et 11.1 65.10 ou versions ultérieures.

Migrer à l'aide d'un script

- À l'aide de la version 82.x de NetScaler Console, vous pouvez sélectionner la fonctionnalité, puis migrer.
- Pour les versions 76.x ou ultérieures de NetScaler Console, les scripts de migration (`servicemigrationtool.py` et `config_collect_onprem.py`) sont disponibles dans la version, à l'adresse `cd /mps/scripts`.
- Pour les versions de NetScaler Console antérieures à 76.x, vous devez télécharger les scripts de migration et copier les scripts dans NetScaler Console sur site.

  Remarque

  Assurez-vous que NetScaler Console sur site dispose d'une connectivité Internet pendant la migration.

1. À l'aide d'un client SSH, connectez-vous à NetScaler Console sur site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque

> Pour une paire HA NetScaler Console, connectez-vous au nœud principal.

2. Tapez **shell** et appuyez sur **Entrée** pour passer en mode bash.
3. Copiez le fichier CSV de l'ID client et du secret. Par exemple, copiez le fichier dans le répertoire /var.

   Après avoir copié le fichier CSV, vous pouvez vérifier s'il est présent.

   Remarque

   > Pour une paire HA NetScaler Console, copiez le fichier CSV dans le nœud principal.

4. Pour la **version 13.0 82.xx** de NetScaler Console sur site, exécutez les commandes suivantes pour terminer la migration :

   a. `cd /mps/scripts`

   b. `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler Console VM>`

   Par exemple, `python servicemigrationtool.py /var/secureclient.csv`

   Après avoir exécuté le script de migration, l'outil affiche les options suivantes :

   Selon le choix que vous fournissez, seule cette fonctionnalité est migrée vers le service NetScaler Console.

   Dans l'exemple, l'option 1 est sélectionnée. L'outil termine la migration de la gestion et de la surveillance (M&M) et affiche le message suivant :

   La fonctionnalité **Gestion et surveillance (M&M)** comprend :

   - Instances NetScaler, balises, groupes d'instances, profils, applications personnalisées, tâches de configuration, SNMP, configurations syslog.
   - Sites, blocs d'adresses IP, rapports réseau, seuils d'analyse, paramètres de notification, paramètres d'élagage des données.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Modèles d'audit de configuration, intervalles d'interrogation, règles et paramètres d'événement.
- Groupes, rôles et stratégies RBAC

La fonctionnalité **Analyse** comprend :

- Configuration Appflow par vserver à partir des instances NetScaler.
- Configuration Appflow® par périphérique SDWAN.

Remarque :

- La fonctionnalité Gestion et surveillance (M&M) est automatiquement migrée, même si vous sélectionnez une autre fonctionnalité (2, 3 ou 4).
- Vous ne pouvez spécifier qu'une seule fonctionnalité à la fois.
- Une fois la migration d'une fonctionnalité terminée, si vous souhaitez migrer une autre fonctionnalité ultérieurement, la fonctionnalité déjà migrée n'apparaît pas dans la liste. Par exemple, si vous terminez d'abord la migration de la fonctionnalité **Analyse**, la prochaine fois que vous exécuterez le script de migration, vous ne verrez que les options **StyleBooks**, **Licences en pool** et **Tout**.
- Lorsque vous migrez les licences en pool, tous les types, y compris les vservers, sont migrés.

5. Pour NetScaler Console sur site **version 13.0 76.xx**, exécutez les commandes suivantes pour terminer la migration :

   a. `cd /mps/scripts`

   b. `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler Console VM>`

   Par exemple, `python servicemigrationtool.py /var/secureclient.csv`

6. Pour NetScaler Console sur site antérieure à la version 13.0 76.xx :

   a. Téléchargez le script de migration à partir de l'emplacement suivant : `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le fichier téléchargé comprend deux scripts de bundle, `servicemigrationtool_27.py` et `config_collect_onprem_27.py`.

b. Enregistrez les deux scripts dans NetScaler Console sur site. Par exemple, enregistrez-les dans le répertoire /var

c. Exécutez les commandes suivantes pour migrer :

i. `cd /var`

ii. `servicemigrationtool_27.py <path of ClientID/Secret File in NetScaler Console on-prem VM>`

Par exemple, `python servicemigrationtool_27.py /var/secureclient.csv`

Après avoir exécuté le script, il vérifie les prérequis, puis procède à la migration. Le script vérifie d'abord la disponibilité de la licence. Le message suivant s'affiche uniquement si vous disposez d'une licence de service NetScaler Console inférieure à la licence sur site.



Si vous sélectionnez **Y**, la migration se poursuit en attribuant une licence au VIP de manière aléatoire. Si vous sélectionnez **N**, le script arrête la migration.

Si vous disposez d'une version d'instance NetScaler non prise en charge pour le serveur de licences en pool, le message suivant s'affiche :



Si vous sélectionnez **Y**, le processus de migration se poursuit en modifiant le serveur de licences. Si vous sélectionnez **N**, le script vous demande si vous souhaitez poursuivre le reste de la migration. Le script arrête la migration si vous sélectionnez **N**.

Selon la configuration sur site, le temps approximatif nécessaire à la migration est compris entre quelques minutes et quelques heures. Une fois la migration terminée, le message suivant s'affiche :



La migration est réussie une fois que toutes les instances NetScaler et leurs configurations respectives ont été déplacées avec succès vers le service NetScaler Console. Après une migration réussie, NetScaler Console sur site cesse de traiter les événements d'instance suivants :

- Certificats SSL
- Messages Syslog
- Sauvegarde

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cluster d'agents
- Rapports de performances
- Audit de configuration
- Planificateur `Emon`

Revenir à NetScaler Console sur site

Si vous souhaitez revenir à NetScaler Console sur site, assurez-vous que les prérequis sont remplis.

Prérequis

Si votre NetScaler Console sur site (avant la migration vers le service NetScaler Console) est :

- Utilisé comme serveur de licences en pool, assurez-vous de disposer des licences en pool requises dans NetScaler Console sur site.
- Configuré avec des agents NetScaler, assurez-vous que les agents sont disponibles avec le statut « UP ».

Utiliser le script de restauration

Remarque

> Après la restauration, les mêmes configurations (avant la migration) dans Analytics, SNMP, et les licences en pool sont à nouveau disponibles dans NetScaler Console sur site. Si vous avez apporté des modifications à ces configurations après la migration, ces modifications ne sont pas reflétées dans NetScaler Console sur site.

- Pour les versions de **NetScaler Console 82.xx ou ultérieures**, le script de restauration est disponible dans la version et accessible à l'adresse `/mps/scripts`.
- Pour les versions de **NetScaler Console antérieures à 79.xx**, vous pouvez soit effectuer une mise à niveau vers la version 82.x et utiliser le script de restauration, soit télécharger le script de restauration et le copier dans NetScaler Console sur site.

1. À l'aide d'un client SSH, connectez-vous à NetScaler Console sur site.
2. Tapez shell et appuyez sur Entrée pour passer en mode bash.
3. Pour la version **13.0 82.xx** de NetScaler Console, exécutez les commandes suivantes pour effectuer la restauration :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. cd /mps/scripts

b. Python rollback_to_onprem.py `<path of ClientID/Secret File in NetScaler Console on-prem VM>`

   Par exemple, `python rollback_to_onprem.py /var/ secureclient.csv.csv`

   L'outil lance l'opération de restauration et une invite vous demande si vous souhaitez continuer. Tapez **Y** pour continuer.

   Vous pouvez voir le message suivant une fois que la restauration est terminée.

4. Pour NetScaler Console antérieur à la version 82.xx :

   a. Téléchargez le script de restauration à partir de l'emplacement suivant :

      `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

   b. Pour les versions 79.xx et 76.xx de NetScaler Console, enregistrez le script dans `/mps/scripts` et exécutez les commandes suivantes pour restaurer :

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in NetScaler Console on-prem>`

      Par exemple, `python rollback_to_onprem.py /var/ secureclient.csv`

   c. Pour NetScaler Console antérieur aux versions 76.xx, enregistrez le script dans NetScaler Console sur site. Par exemple, enregistrez-le à l'emplacement `/var` et exécutez les commandes suivantes pour restaurer :

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in NetScaler Console on-prem>`

      Par exemple, `python rollback_to_onprem_27.py /var/secureclient.csv`

   L'outil lance l'opération de restauration et une invite vous demande si vous souhaitez continuer. Tapez **Y** pour continuer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQ

Service NetScaler Console

L'agent NetScaler est-il facultatif, comme l'agent NetScaler sur site ?

Non. L'agent est obligatoire pour le service NetScaler Console et toutes les communications entre les instances et le service NetScaler Console passent par l'agent. Dans NetScaler Console sur site, l'agent est facultatif ; cependant, vous pouvez configurer un agent uniquement pour économiser la consommation de bande passante.

Pourquoi le service NetScaler Console ?

Le service NetScaler Console via Citrix Cloud offre les avantages suivants, sans nécessiter de nouvelles versions périodiques :

- Offre SaaS basée sur le cloud avec une intégration plus facile et un coût total de possession inférieur à celui de NetScaler Console sur site.
- Des versions plus rapides, environ toutes les deux semaines avec les dernières mises à jour de fonctionnalités.
- Analyses basées sur l'apprentissage automatique pour la sécurité des applications, les performances et l'utilisation.
- Diverses autres fonctionnalités qui ne sont actuellement prises en charge que dans le service NetScaler Console, telles que l'analyse des périodes de pointe et creuses, l'analyse de la sécurité des applications basée sur l'apprentissage automatique pour WAF et les bots, l'analyse du CPU des applications, et bien d'autres.

Que se passe-t-il après la migration si NetScaler Console sur site est une paire HA ?

Toutes les configurations sont déplacées vers Citrix Cloud. La configuration d'un nœud de reprise après sinistre n'est pas requise.

Que se passe-t-il si l'agent tombe en panne pour une raison quelconque ?

Vous pouvez vous attendre à une perte de données potentielle tant que l'agent n'est pas opérationnel. Cependant, vous pouvez également configurer des agents NetScaler pour des déploiements multisites afin d'assurer la continuité en cas de basculement d'agent. Pour plus d'informations, consultez Configurer les agents pour un déploiement multisite.

La sauvegarde des instances est-elle également migrée ?

La sauvegarde n'est pas incluse dans la migration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les données historiques sont-elles également migrées ?

Les données historiques ne sont pas migrées. Vous pouvez exporter les données depuis NetScaler Console sur site.

Les licences sur site sont-elles également migrées ?

Non. Le fichier de licence sur site ne peut pas être utilisé pour le service NetScaler Console. Vous devez obtenir des licences pour le service NetScaler Console. Pour plus d'informations, consultez Licences. Si vous utilisez des licences en pool dans NetScaler Console sur site, vous devez obtenir des licences en pool pour le service NetScaler Console, puis allouer des licences aux instances.

Qu'est-ce qui n'est pas migré depuis NetScaler Console sur site ?

Les fonctionnalités suivantes ne peuvent pas être migrées vers le service NetScaler Console :

- **RBAC** – Dans le service NetScaler Console, l'accès utilisateur est basé sur l'invitation de l'administrateur. Les utilisateurs du service NetScaler Console doivent avoir un compte dans Citrix Cloud. Par conséquent, les utilisateurs de NetScaler Console sur site ne sont pas migrés.
- **Planifications d'exportation** – Les planifications d'exportation incluent des détails tels que l'exploration et les planifications de diverses pages. Toutes ces planifications d'exportation détaillées ne sont pas migrées.
- **Certificats/Clés/CSR SSL** – Le service NetScaler Console ne peut afficher que les certificats/clés/CSR SSL NetScaler. Par conséquent, les certificats/clés SSL téléchargés vers NetScaler Console sur site ne seront pas migrés vers le service NetScaler Console.

NetScaler Console sur site est intégré à Citrix Director. Qu'advient-il de l'intégration ?

L'intégration de Director avec NetScaler Console n'est actuellement prise en charge que dans NetScaler Console sur site.

Après la migration, est-il à nouveau nécessaire de licencier l'instance ou d'activer l'analyse ?

Vous devez vous assurer que les licences du service NetScaler Console sont supérieures ou égales aux licences VIP sur site. Si les licences sont déjà supérieures au VIP NetScaler Console sur site, les serveurs virtuels sont automatiquement licenciés. Sinon, les licences sont attribuées de manière aléatoire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Outil de migration

Après l'exécution du script de migration, des messages d'erreur s'affichent. Quel peut être le problème ?

Un fichier journal avec les raisons des échecs s'affiche. Vous pouvez prendre les mesures correctives appropriées et exécuter à nouveau le script de migration. En général, avant d'exécuter le script de migration, assurez-vous de :

- Configurer l'agent NetScaler®
- Obtenir les licences du service NetScaler Console
- Copier le chemin correct où vous avez stocké le fichier CSV client et sécurisé

Les instances NetScaler ont des versions inférieures à la limitation mentionnée pour les licences en pool. Que se passe-t-il si l'option « Y » est sélectionnée pour changer le serveur de licences ?

Le changement de serveur de licences n'a lieu que pour les versions prises en charge de NetScaler MPX, VPX et SDX.

Que se passe-t-il si le script de migration a échoué la configuration des instances NetScaler ?

Les instances NetScaler continuent de fonctionner sur la configuration locale de NetScaler Console. Vous pouvez prendre les mesures nécessaires à partir de la raison d'échec suggérée et exécuter à nouveau le script de migration.

Que se passe-t-il si quelques instances NetScaler ne parviennent pas à être déplacées vers le service NetScaler Console ? La réexécution du script de migration aidera-t-elle ?

Oui. Après avoir réexécuté le script, seules les instances ayant échoué sont migrées. Supposons que deux instances sur cinq n'aient pas pu être déplacées. Après avoir pris des mesures correctives et réexécuté le script de migration, les trois instances qui avaient été déplacées avec succès auparavant affichent le message « L'appareil existe déjà ». Et les deux autres instances qui avaient échoué auparavant sont migrées avec succès.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Existe-t-il un fichier journal pour vérifier l'état de la migration ?

Oui, un fichier journal est généré dans le répertoire `/var/mps/log/`. NetScaler Console avec python3.7 a le fichier journal comme `servicemigrationtool.py.log` et NetScaler Console avec python 2.7 a le fichier journal comme `servicemigrationtool_27.py.log`.

Que se passe-t-il si la session est interrompue pendant l'exécution du script de migration ?

Vous pouvez réexécuter le script de migration. Dans la nouvelle session, les instances déjà ajoutées de la session précédente s'affichent comme « L'appareil existe déjà », et la migration se poursuit.

Que se passe-t-il si le service NetScaler Console dispose de moins de licences que le NetScaler Console sur site et que le script de migration est lancé ?

Après l'exécution du script de migration, une suggestion apparaît, indiquant que les licences sont moins nombreuses et vous invitant à continuer ou à arrêter. Si vous souhaitez continuer avec moins de licences, les serveurs virtuels sont licenciés aléatoirement parmi les licences disponibles.

Que se passe-t-il lorsque NetScaler Console sur site est migré vers le compte Express du service NetScaler Console ?

Le compte Express du service NetScaler Console ne dispose que de deux licences de serveur virtuel, de deux packs de configuration StyleBook et de deux tâches de configuration. Si votre NetScaler Console sur site a plus de configurations que celles-ci et que vous lancez la migration avec un compte Express, le script ne peut migrer que les configurations mentionnées applicables au compte Express (deux licences de serveur virtuel, deux packs de configuration StyleBook et deux tâches de configuration).

Que se passe-t-il si un utilisateur invité de Citrix Cloud (autre que l'utilisateur administrateur qui a créé le compte Citrix Cloud) tente de migrer la configuration NetScaler Console sur site ?

Il est recommandé que l'administrateur exécute le script de migration. Un utilisateur invité n'a pas les privilèges d'administrateur (adminExceptSystem_group). Par conséquent, la migration des groupes, des rôles et des stratégies échoue et le message « L'utilisateur n'a pas la permission » s'affiche.

En guise de solution, l'administrateur (qui a créé le compte Citrix Cloud) peut modifier le groupe associé à l'utilisateur invité en « admin_group ».

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Script de restauration

Que se passe-t-il si le script de restauration est utilisé dans une paire HA NetScaler Console sur site ?

La paire HA NetScaler Console sur site est restaurée avec toutes les configurations qui étaient disponibles avant la migration.

Qu'advient-il du nœud de reprise après sinistre après l'utilisation du script de restauration ?

Le nœud de reprise après sinistre est également restauré avec toutes les configurations d'avant la migration.

Dépannage

Lorsque vous exécutez le script de migration pour la première fois, il vérifie les prérequis et procède à la migration. Si tous les prérequis sont remplis, la migration se termine sans erreur. Si un prérequis échoue, le script affiche des messages d'erreur avec les raisons. Après avoir corrigé les erreurs, vous devez exécuter à nouveau le script.

Remarque

Si vous voyez un message d'erreur affichant « existe déjà », cela signifie que :

- Vous avez peut-être exécuté le script de migration plus d'une fois et certaines configurations sont déjà migrées vers le service NetScaler Console.
- Vous avez peut-être créé manuellement la même configuration dans le service NetScaler Console, avant d'exécuter le script de migration.

Reportez-vous à certains des messages d'erreur suivants :

Profil manuel ajouté au service NetScaler Console

Solution de contournement : Si vous avez créé des profils d'administrateur dans le service NetScaler Console avant d'exécuter le script de migration, assurez-vous de supprimer ces profils et de réexécuter le script de migration.

Appareil NetScaler ajouté au service NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solution de contournement : Dans NetScaler Console, vérifiez l'état de l'instance et assurez-vous que vous pouvez y accéder sans problème. Si un problème persiste, corrigez-le et réexécutez le script de migration.

Importation de modèles personnalisés StyleBook vers le service NetScaler Console



Solution de contournement : Ce message d'erreur est un exemple pour le StyleBook déjà migré. Vous pouvez également voir cette erreur si vous avez créé manuellement un StyleBook avec le même nom, la même version et le même espace de noms, dans le service NetScaler Console avant d'exécuter le script de migration.

Tâches de configuration ajoutées au service NetScaler Console



Solution de contournement : Cette erreur se produit si vous avez souscrit à un compte Express et que vous avez plus de deux tâches de configuration. Vous devez obtenir un abonnement valide pour que toutes vos tâches de configuration soient migrées.

Blocs IP ajoutés au service NetScaler Console



Solution de contournement : Supprimez le bloc IP créé manuellement dans le service NetScaler Console et réexécutez le script de migration.

Statut d'ajout du rapport du tableau de bord réseau



Solution de contournement : Supprimez le tableau de bord créé manuellement dans le service NetScaler Console et réexécutez le script de migration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tous les articles pratiques

Les « articles pratiques » de NetScaler Application Delivery Management (NetScaler Console) sont des articles simples, pertinents et faciles à mettre en œuvre sur les fonctionnalités de NetScaler Console. Ces articles contiennent des informations sur certaines des fonctionnalités populaires de NetScaler Console, telles que la gestion des instances, la gestion des applications, les StyleBooks, la gestion des certificats et Analytics.

Cliquez sur le nom d'une fonctionnalité dans le tableau ci-dessous pour afficher la liste des articles pratiques pour cette fonctionnalité.

RUBRIQUES				
Gestion des instances	Gestion des événements	StyleBooks	Gestion des certificats	Système NetScaler Console
	Gestion de la configuration	Authentification	Analytics	Fonctions réseau

Gestion des instances

Comment surveiller les sites distribués globalement

Comment gérer les partitions d'administration des instances NetScaler

Comment ajouter des instances à NetScaler Console

Comment créer des groupes d'instances sur NetScaler Console

Comment configurer des sites pour les Geomaps dans NetScaler Console

Comment forcer un basculement vers l'instance NetScaler secondaire à l'aide de NetScaler Console

Comment forcer une instance NetScaler secondaire à rester secondaire à l'aide de NetScaler Console

Comment sauvegarder et restaurer une instance à l'aide de NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment redécouvrir plusieurs instances NetScaler VPX

Comment interroger les instances et entités NetScaler dans NetScaler Console

Comment désadministrer une instance sur NetScaler Console

Comment tracer l'itinéraire vers une instance depuis NetScaler Console

Gestion de la configuration

Comment créer une tâche de configuration sur NetScaler Console

Comment utiliser la commande SCP (put) dans les tâches de configuration

Comment planifier des tâches créées à l'aide de modèles intégrés dans NetScaler Console

Comment replanifier les tâches configurées à l'aide de modèles intégrés dans NetScaler Console

Comment réutiliser les tâches de configuration exécutées

Comment mettre à niveau les instances NetScaler à l'aide de NetScaler Console

Comment utiliser des variables dans les tâches de configuration sur NetScaler Console

Comment utiliser des modèles de configuration pour créer des modèles d'audit sur NetScaler Console

Comment créer des tâches de configuration à partir de commandes correctives sur NetScaler Console

Comment répliquer les commandes de configuration en cours d'exécution et enregistrées d'une instance NetScaler à une autre sur NetScaler Console

Comment utiliser l'enregistrement et la lecture pour créer des tâches de configuration

Comment utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances

Comment utiliser le modèle de configuration maître sur NetScaler Console

Comment interroger l'audit de configuration des instances NetScaler

Comment réutiliser les modèles d'audit de configuration dans les tâches de configuration

Comment importer et exporter des modèles de configuration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment générer la différence d'audit de configuration pour les traps SNMP ConfigChange

Gestion des certificats

Comment configurer une stratégie d'entreprise sur NetScaler Console

Comment installer des certificats SSL sur une instance NetScaler à partir de NetScaler Console

Comment mettre à jour un certificat installé à partir de NetScaler Console

Comment lier et dissocier des certificats SSL à l'aide de NetScaler Console

Comment créer une demande de signature de certificat (CSR) à l'aide de NetScaler Console

Comment configurer des notifications d'expiration de certificat SSL à partir de NetScaler Console

Comment utiliser le tableau de bord SSL sur NetScaler Console

Comment interroger les certificats SSL à partir des instances NetScaler

StyleBooks

Comment afficher les différents groupes de StyleBooks

Comment créer vos propres StyleBooks

Comment utiliser les StyleBooks définis par l'utilisateur dans NetScaler Console

Comment utiliser l'API pour créer des configurations à partir de StyleBooks

Comment activer l'analyse et configurer des alarmes sur un serveur virtuel défini dans un StyleBook

Comment créer un StyleBook pour télécharger des fichiers vers NetScaler Console

Comment utiliser l'API pour créer des configurations afin de télécharger n'importe quel type de fichier

Comment créer un StyleBook pour télécharger des fichiers de certificat SSL et de clé de certificat vers NetScaler Console

Comment utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificat et de clé

Comment utiliser le StyleBook Microsoft Skype for Business dans les entreprises

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment utiliser le StyleBook Microsoft Exchange dans les entreprises

Comment utiliser le StyleBook Microsoft SharePoint dans les entreprises

Analytique

Comment activer l'analytique sur les instances

Comment configurer les seuils adaptatifs

Comment configurer la gestion des SLA

Comment configurer la synthèse de base de données pour l'analytique

Comment créer des seuils et des alertes à l'aide de NetScaler Console

Comment désactiver la collecte de données URL pour l'analytique depuis NetScaler Console

Gestion des événements

Comment définir l'âge des événements pour les événements sur NetScaler Console

Comment planifier un filtre d'événements à l'aide de NetScaler Console

Comment configurer des notifications par e-mail répétées pour les événements depuis NetScaler Console

Comment supprimer des événements à l'aide de NetScaler Console

Comment utiliser le tableau de bord des événements pour surveiller les événements

Comment créer des règles d'événement sur NetScaler Console

Comment modifier la gravité signalée des événements qui se produisent sur les instances NetScaler

Comment afficher le résumé des événements dans NetScaler Console

Comment afficher les gravités et les décalages des événements des traps SNMP sur NetScaler Console

Comment exporter des messages syslog à l'aide de NetScaler Console

Comment supprimer les messages syslog dans NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment configurer les paramètres d'élagage pour les événements d'instance

Authentification

Comment activer les serveurs d'authentification externes de secours et en cascade

Comment ajouter des serveurs d'authentification RADIUS

Comment ajouter des serveurs d'authentification LDAP

Comment ajouter des serveurs d'authentification TACACS

Comment extraire un groupe de serveurs d'authentification dans NetScaler Console

Comment activer l'authentification locale de secours

Système NetScaler Console

Comment mettre à niveau NetScaler Console

Comment réinitialiser le mot de passe de NetScaler Console

Comment générer un fichier de support technique pour NetScaler Console

Comment sauvegarder et restaurer votre serveur NetScaler Console dans un déploiement à serveur unique

Comment sauvegarder et restaurer une configuration NetScaler Console dans une paire HA

Comment activer l'accès shell pour les utilisateurs non par défaut dans NetScaler Console

Comment configurer le serveur NTP sur NetScaler Console

Comment configurer les paramètres SSL pour NetScaler Console

Comment configurer l'intervalle de purge syslog pour NetScaler Console

Comment afficher les informations d'audit de NetScaler Console

Comment configurer les paramètres de notification système de NetScaler Console

Comment surveiller l'utilisation du CPU, de la mémoire et du disque de NetScaler Console

Comment configurer un groupe de chiffrement pour NetScaler Console

Comment créer des traps, des gestionnaires et des utilisateurs SNMP sur NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment attribuer un nom d'hôte à un serveur NetScaler Console

Comment configurer les paramètres d'élagage du système pour NetScaler Console

Comment configurer les paramètres de sauvegarde du système à l'aide de NetScaler Console

Comment configurer et afficher les alarmes système sur NetScaler Console

Fonctions réseau

Comment générer des rapports pour les entités d'équilibrage de charge

Comment exporter ou planifier l'exportation de rapports de fonctions réseau

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vue d'ensemble

REMARQUE :

À partir de la version 14.1-17.x, NetScaler ADM est renommé NetScaler Console. Pour les versions antérieures, le nom du produit est NetScaler ADM.

NetScaler Console est une solution de gestion centralisée qui simplifie les opérations en offrant aux administrateurs une visibilité à l'échelle de l'entreprise et en automatisant les tâches de gestion qui doivent être exécutées sur plusieurs instances. Vous pouvez gérer et surveiller les produits NetScaler, notamment NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX et NetScaler Gateway. Vous pouvez utiliser NetScaler Console pour gérer, surveiller et dépanner l'ensemble de l'infrastructure globale de livraison d'applications à partir d'une console unique et unifiée.

NetScaler Console est une appliance virtuelle qui s'exécute sur Citrix Hypervisor, VMware ESXi et Linux KVM. NetScaler Console relève le défi de la visibilité des applications en collectant les informations détaillées suivantes sur le trafic des applications web et des bureaux virtuels :

- informations au niveau de la session utilisateur
- Données de performance des pages web
- informations de base de données transitant par les instances NetScaler de votre site et fournit des rapports exploitables.

NetScaler Console permet aux administrateurs informatiques de dépanner et de surveiller de manière proactive les problèmes des clients en quelques minutes.

Fonctionnalités et solutions

NetScaler Console offre les fonctionnalités suivantes :

Analyse et gestion des applications

Analyse des performances des applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App Score est le résultat d'un système de notation qui définit les performances d'une application. Il indique si l'application fonctionne bien en termes de réactivité, n'est pas vulnérable aux menaces et si tous les systèmes sont opérationnels.

Analyse de la sécurité des applications

Le tableau de bord de sécurité des applications offre une vue d'ensemble de l'état de sécurité de vos applications. Par exemple, il affiche des métriques de sécurité clés telles que les violations de sécurité, les violations de signature, les indices de menace. Le tableau de bord de sécurité des applications affiche également des informations relatives aux attaques telles que les attaques SYN, les attaques par petite fenêtre et les attaques par inondation DNS pour les instances NetScaler découvertes.

Réseaux

Instances

Permet de gérer les instances NetScaler et NetScaler Gateway.

Groupes d'instances

Permet de regrouper vos instances comme suit :

- Groupe statique : vous permet de définir un groupe d'appareils que vous pouvez utiliser dans différentes tâches telles que les tâches de configuration, etc.
- Bloc d'adresses IP privées : vous permet de regrouper vos instances en fonction de leur emplacement géographique.

Gestion des événements

Lorsque l'adresse IP d'une instance NetScaler est ajoutée à NetScaler Console, un appel NITRO est envoyé par NetScaler Console et s'ajoute implicitement comme destination de trap pour l'instance afin de recevoir ses traps ou événements.

Les événements représentent des occurrences d'événements ou d'erreurs sur une instance NetScaler gérée.

Gestion des certificats

NetScaler Console simplifie désormais tous les aspects de la gestion des certificats pour vous. Grâce à une console unique, vous pouvez établir des politiques automatisées pour garantir le bon émetteur, la force de clé et les algorithmes corrects, tout en gardant un œil attentif sur les certificats inutilisés ou bientôt expirés. Pour commencer à utiliser le tableau de bord SSL de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console et ses fonctionnalités, vous devez comprendre ce qu'est un certificat SSL et comment vous pouvez utiliser NetScaler Console pour suivre vos certificats SSL.

Gestion de la configuration

NetScaler Console vous permet de créer des tâches de configuration qui vous aident à effectuer des tâches de configuration, telles que la création d'entités, la configuration de fonctionnalités, la réplication des modifications de configuration, les mises à niveau du système et d'autres activités de maintenance en toute simplicité sur plusieurs instances. Les tâches et modèles de configuration simplifient les tâches administratives les plus répétitives en une seule tâche sur NetScaler Console.

Audit de configuration

Vous permet de surveiller et d'identifier les anomalies dans les configurations de vos instances.

- Conseils de configuration : Vous permet d'identifier les anomalies de configuration.
- Modèle d'audit : Vous permet de surveiller les modifications d'une configuration spécifique.

Rapports réseau

Vous pouvez optimiser l'utilisation des ressources en surveillant vos rapports réseau sur NetScaler Console.

Orchestration

Orchestration cloud

Permet l'intégration des produits NetScaler avec l'orchestration cloud OpenStack. NetScaler Console et OpenStack implémentent les API l'un de l'autre, permettant l'intégration de la fonctionnalité d'équilibrage de charge (LBaaS) de l'instance NetScaler avec l'orchestration cloud OpenStack.

Orchestration

NetScaler Console prend en charge le SDN dans le réseau d'entreprise en s'intégrant aux contrôleurs SDN de différents fournisseurs. NetScaler Console prend en charge à la fois VMware NSX Manager et Cisco Application Policy Infrastructure Controller (APIC).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Architecture

La base de données NetScaler Console est intégrée au serveur, et le serveur gère tous les processus clés, tels que la collecte de données, les appels NITRO. Dans son magasin de données, le serveur stocke un inventaire des détails de l'instance, tels que le nom d'hôte, la version du logiciel, la configuration en cours d'exécution et enregistrée, les détails du certificat, les entités configurées sur l'instance. Un déploiement de serveur unique convient si vous souhaitez traiter de petites quantités de trafic ou stocker des données pendant une durée limitée.

Actuellement, NetScaler Console prend en charge deux types de déploiements logiciels : serveur unique et haute disponibilité.

L'image suivante montre les différents sous-systèmes au sein de NetScaler Console et comment la communication s'établit entre le serveur NetScaler Console et les instances gérées.



Le sous-système de service de NetScaler Console agit comme un serveur web qui gère les requêtes et réponses HTTP envoyées aux sous-systèmes de NetScaler Console depuis l'interface graphique ou l'API, en utilisant les ports 80 et 443. Ces requêtes sont envoyées aux sous-systèmes via le bus de messages (système de traitement des messages) en utilisant le mécanisme IPC (communication inter-processus). Une requête est envoyée au sous-système de contrôle, qui traite l'information ou l'envoie au sous-système approprié. Chacun des autres sous-systèmes — Inventaire, StyleBooks, Collecteur de données, Configuration, Décodeur AppFlow, Analyse AppFlow, Performances, Événements, Entités, Gestionnaire SLA, Provisionneur et Journal — a un rôle spécifique.

Les plug-ins d'instance sont des bibliothèques partagées qui sont uniques à chaque type d'instance pris en charge par NetScaler Console. Les informations sont transférées entre NetScaler Console et les instances gérées à l'aide d'appels NITRO, ou via les protocoles SNMP, Secure Shell (SSH) ou Secure Copy (SCP). Ces informations sont ensuite traitées et stockées dans la base de données interne (magasin de données).

Comment NetScaler Console découvre les instances

Les instances sont des appliances NetScaler ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller depuis NetScaler Console. Pour gérer et surveiller ces instances, vous devez les ajouter au serveur NetScaler Console. Vous pouvez ajouter les appliances NetScaler et les appliances virtuelles suivantes à NetScaler Console :

- Instances NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX

- Instances NetScaler Gateway

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler Console ou ultérieurement.

REMARQUE

NetScaler Console utilise l'adresse IP NetScaler (NSIP) des instances NetScaler pour la communication. NetScaler Console peut également découvrir les instances NetScaler avec une adresse IP de sous-réseau (SNIP) sur laquelle l'accès de gestion est activé. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances NetScaler et NetScaler Console, consultez Ports.

Si vous souhaitez ajouter une paire HA NetScaler à l'aide de SNIP, assurez-vous d'activer le mode INC (Independent Network Configuration) sur la paire HA NetScaler. Pour plus d'informations sur l'ajout d'instances, consultez Ajouter des instances.
Lorsque vous ajoutez une instance à NetScaler Console, le serveur s'ajoute implicitement comme destination de trap pour l'instance et collecte l'inventaire de l'instance.

Le diagramme suivant décrit comment NetScaler Console découvre et ajoute implicitement des instances.



Comme indiqué dans le diagramme, les étapes suivantes sont effectuées implicitement par NetScaler Console.

1. NetScaler Console utilise les détails du profil d'instance pour se connecter à l'instance. À l'aide d'un appel NetScaler NITRO, NetScaler Console récupère les informations de licence de l'instance. En fonction des informations de licence, il détermine si l'instance est une instance NetScaler et le type de plate-forme NetScaler (par exemple, NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX ou NetScaler Gateway). En cas de détection réussie de l'instance, celle-ci est ajoutée à la base de données NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cette étape peut échouer si le profil d'instance n'inclut pas les informations d'identification correctes. Pour les instances NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX et NetScaler Gateway, cette étape peut également échouer si les licences ne sont pas appliquées à l'instance.

REMARQUE

En utilisant HTTP, vous pouvez ajouter toutes les instances à NetScaler Console même si les licences ne sont pas configurées sur les instances.

2. NetScaler Console ajoute son adresse IP à la liste des destinations de trap sur l'instance. Cela permet à NetScaler Console de recevoir les traps générés sur l'instance NetScaler.

   Cette étape peut échouer si le nombre de destinations de trap sur l'instance dépasse la limite maximale de destinations de trap. La limite maximale sur les instances est de 20.

3. NetScaler Console collecte l'inventaire de l'instance en envoyant une requête NITRO. Il collecte les détails de l'instance tels que le nom d'hôte, la version du logiciel, la configuration en cours d'exécution et enregistrée, les détails du certificat, les entités configurées sur l'instance.

   Cette étape peut échouer en raison de problèmes de réseau ou de pare-feu.

   Pour savoir comment ajouter des instances à NetScaler Console, consultez Ajouter des instances.

Vue d'ensemble du sondage

Le sondage est un processus par lequel NetScaler Console collecte certaines informations auprès des instances NetScaler. Vous avez peut-être configuré plusieurs instances NetScaler pour votre organisation, partout dans le monde. Pour surveiller vos instances via NetScaler Console, NetScaler Console doit collecter certaines informations telles que l'utilisation du CPU, l'utilisation de la mémoire, les certificats SSL, les fonctionnalités sous licence, les types de licences, etc., de toutes les instances NetScaler gérées. Voici les différents types de sondage qui ont lieu entre NetScaler Console et les instances gérées :

- Sondage d'instance
- Sondage d'inventaire
- Collecte de données de performance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sondage de sauvegarde d'instance
- Sondage d'audit de configuration
- Sondage de certificat SSL
- Sondage d'entité

NetScaler Console utilise des protocoles tels que l'appel NITRO, Secure Shell (SSH) et Secure Copy (SCP) pour sonder les informations des instances NetScaler.

Comment NetScaler Console sonde les instances et entités gérées

NetScaler Console effectue automatiquement des sondages à intervalles réguliers par défaut. NetScaler Console vous permet également de configurer des intervalles de sondage pour certains types de sondage et vous permet de sonder manuellement si nécessaire.

Le tableau suivant décrit les détails des types de sondage, de l'intervalle de sondage, du protocole utilisé, etc. :

TYPE DE SONDAGE	INTERVALLE DE SONDAGE	INFORMATIONS INTERROGÉES	PROTOCOLE UTILISÉ	CONFIGURATION DE L'INTERVALLE D'INTERROGATION
Interrogation d'instance	Toutes les 1 minute (par défaut)	Informations statistiques telles que l'état, les requêtes HTTP par seconde, l'utilisation du CPU, l'utilisation de la mémoire et le débit.	Appel NITRO.	Non
Interrogation d'inventaire	Toutes les 60 minutes (par défaut)	Détails de l'inventaire tels que la version de build, les informations système, les fonctionnalités	Appels NITRO et SSH	Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE DE SONDAGE	INTERVALLE DE SONDAGE	INFORMATIONS INTERROGÉES	PROTOCOLE UTILISÉ	CONFIGURATION DE L'INTERVALLE D'INTERROGATION
		sous licence et les modes.		
Collecte de données de performance	Toutes les 5 minutes (par défaut)	Informations de reporting réseau	Appel NITRO	Non
Interrogation de la sauvegarde d'instance	Toutes les 12 heures (par défaut)	Fichier de sauvegarde de l'état actuel des instances NetScaler gérées	Appels NITRO, SSH et SCP.	Oui. Accédez à **Infrastructure > Instances > NetScaler**. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, cliquez sur **Sauvegarder/ Restaurer**.
Interrogation de l'audit de configuration	Toutes les 10 heures (par défaut)	Modifications de configuration qui se produisent sur les instances NetScaler (par exemple, configuration en cours d'exécution par rapport à la configuration enregistrée)	SSH, SCP et appel NITRO	Oui. Accédez à **Infrastructure > Audit de configuration**. Sur la page Audit de configuration, cliquez sur **Paramètres** et configurez l'intervalle d'interrogation pour l'audit de configuration.
				Vous pouvez interroger manuellement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE DE SONDAGE	INTERVALLE DE SONDAGE	INFORMATIONS INTERROGÉES	PROTOCOLE UTILISÉ	CONFIGURATION DE L'INTERVALLE D'INTERROGATION
				les audits de configuration et ajouter immédiatement tous les audits de configuration des instances à NetScaler Console. Pour ce faire, accédez à **Infrastructure > Audit de configuration** et cliquez sur **Interroger maintenant**. La page **Interroger maintenant** vous permet d'interroger toutes les instances ou des instances sélectionnées dans le réseau.
Interrogation des certificats SSL	Toutes les 24 heures (par défaut)	Certificats SSL installés sur les instances NetScaler.	Appels NITRO et SCP	Oui. Accédez à **Infrastructure > Tableau de bord SSL**. Sur la page Tableau de bord SSL, cliquez sur **Paramètres** pour configurer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE DE SONDAGE	INTERVALLE DE SONDAGE	INFORMATIONS INTERROGÉES	PROTOCOLE UTILISÉ	CONFIGURATION DE L'INTERVALLE D'INTERROGATION
				l'intervalle d'interrogation.
				Vous pouvez interroger manuellement les certificats SSL et ajouter immédiatement tous les certificats des instances à NetScaler Console. Pour ce faire, accédez à **Infrastructure > Tableau de bord SSL** et cliquez sur **Interroger maintenant**. La page **Interroger maintenant** vous permet d'interroger toutes les instances ou des instances sélectionnées dans le réseau.
Interrogation d'entités				

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE DE SONDAGE	INTERVALLE DE SONDAGE	INFORMATIONS INTERROGÉES	PROTOCOLE UTILISÉ	CONFIGURATION DE L'INTERVALLE D'INTERROGATION
Toutes les instances	Toutes les 720 minutes (par défaut)	Toutes les entités configurées sur les instances. Une entité est une stratégie, un serveur virtuel, un service ou une action attaché à une instance NetScaler. Pour activer l'interrogation d'entités, consultez Activer ou désactiver les fonctionnalités de NetScaler Console.	Appel NITRO	Oui. Il peut être défini entre 30 minutes et 1440 minutes. Pour configurer, accédez à **Infrastructure > Fonctions réseau**. Sur la page Fonctions réseau, cliquez sur **Paramètres** pour configurer l'intervalle d'interrogation.
				Vous pouvez interroger manuellement les entités et ajouter immédiatement toutes les entités des instances à NetScaler Console. Pour ce faire, accédez à **Infrastructure > Fonctions**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE DE SONDAGE	INTERVALLE DE SONDAGE	INFORMATIONS INTERROGÉES	PROTOCOLE UTILISÉ	CONFIGURATION DE L'INTERVALLE D'INTERROGATION
				réseau et cliquez sur **Interroger maintenant**. La page **Interroger maintenant** vous permet d'interroger toutes les instances ou des instances sélectionnées dans le réseau.
Instances NetScaler sélectionnées	Toutes les 15 minutes (par défaut)	Interrogez uniquement les instances NetScaler où des modifications ont été apportées avant le déclenchement du cycle d'interrogation par défaut.	Appel NITRO	Oui. Il peut être défini entre 5 minutes et 60 minutes. Accédez à **Infrastructure > Fonctions réseau**, cliquez sur **Paramètres**, et spécifiez l'heure dans la zone de texte **Délai pour les fonctions réseau**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

En plus de l'interrogation, les événements générés par les instances NetScaler gérées sont reçus par NetScaler Console via des traps SNMP envoyés aux instances. Par exemple, un événement est généré en cas de défaillance du système ou de modification de la configuration.

Lors de la sauvegarde de l'instance, les fichiers SSL, les fichiers de certificat CA, les modèles NetScaler, les informations de base de données, etc., sont téléchargés vers NetScaler Console. Lors d'un audit de configuration, les fichiers ns.conf sont téléchargés et stockés dans le système de fichiers. Toutes les informations collectées à partir des instances NetScaler gérées sont stockées en interne dans la base de données.

Différentes méthodes d'interrogation des instances

Voici les différentes méthodes d'interrogation que NetScaler Console effectue sur les instances gérées :

- Interrogation globale des instances
- Interrogation manuelle des instances
- Interrogation manuelle des entités

Interrogation globale des instances

NetScaler Console interroge automatiquement toutes les instances gérées du réseau en fonction de l'intervalle que vous avez configuré. Bien que l'intervalle d'interrogation par défaut soit de 30 minutes, vous pouvez définir l'intervalle en fonction de vos besoins en accédant à **Infrastructure > Fonctions réseau** > **Paramètres**.

Interrogation manuelle des instances

Lorsque NetScaler Console gère de nombreuses entités, le cycle d'interrogation prend plus de temps pour générer le rapport, ce qui peut entraîner un écran vide ou le système peut toujours afficher des données antérieures.

Dans NetScaler Console, il existe une période d'intervalle d'interrogation minimale pendant laquelle l'interrogation automatique ne se produit pas. Si vous ajoutez une nouvelle instance NetScaler, ou si une entité est mise à jour, NetScaler Console ne reconnaît pas la nouvelle instance ou les mises à jour apportées à une entité avant la prochaine interrogation. Et, il n'y a aucun moyen d'obtenir immédiatement une liste d'adresses IP virtuelles pour d'autres opérations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous devez attendre que la période d'intervalle d'interrogation minimale s'écoule. Bien que vous puissiez effectuer une interrogation manuelle pour découvrir les instances nouvellement ajoutées, cela entraîne l'interrogation de l'ensemble du réseau NetScaler, ce qui crée une charge importante sur le réseau. Au lieu d'interroger l'ensemble du réseau, NetScaler Console vous permet désormais d'interroger uniquement les instances et entités sélectionnées à tout moment.

NetScaler Console interroge automatiquement les instances gérées pour collecter des informations à des heures définies dans la journée. L'interrogation sélective réduit le temps d'actualisation dont NetScaler Console a besoin pour afficher l'état le plus récent des entités liées à ces instances sélectionnées.

Pour interroger des instances spécifiques dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Fonctions réseau**.
2. Sur la page **Fonctions réseau**, dans le coin supérieur droit, cliquez sur **Interroger maintenant**.
3. La page contextuelle **Interroger maintenant** vous offre la possibilité d'interroger toutes les instances NetScaler du réseau ou d'interroger les instances sélectionnées.
    a. Onglet **Toutes les instances** - cliquez sur **Démarrer l'interrogation** pour interroger toutes les instances.
    b. Onglet **Sélectionner les instances** - sélectionnez les instances dans la liste
4. Cliquez sur **Démarrer l'interrogation**.

NetScaler Console lance l'interrogation manuelle et ajoute toutes les entités.

Interrogation manuelle des entités

NetScaler Console vous permet également d'interroger uniquement quelques entités sélectionnées qui sont liées à une instance particulière. Par exemple, vous pouvez utiliser cette option pour connaître l'état le plus récent d'une entité particulière dans une instance. Dans un tel cas, vous n'avez pas besoin d'interroger l'instance dans son ensemble pour connaître l'état d'une entité mise à jour. Lorsque vous sélectionnez et interrogez une entité, NetScaler Console interroge uniquement cette entité et met à jour l'état dans l'interface graphique de NetScaler Console.

Prenons l'exemple d'un serveur virtuel en état HORS SERVICE. L'état de ce serveur virtuel peut être passé à EN SERVICE avant la prochaine interrogation automatique. Pour afficher l'état

© 1997–2026 Citrix Systems, Inc. All rights reserved.

modifié du serveur virtuel, vous pouvez n'interroger que ce serveur virtuel afin que l'état correct soit affiché immédiatement sur l'interface graphique.

Vous pouvez désormais interroger les entités suivantes pour toute mise à jour de leur état : services, groupes de services, serveurs virtuels d'équilibrage de charge, serveurs virtuels de réduction de cache, serveurs virtuels de commutation de contenu, serveurs virtuels d'authentification, serveurs virtuels VPN, serveurs virtuels GSLB et serveurs d'applications.

REMARQUE

Si vous interrogez un serveur virtuel, seul ce serveur virtuel est interrogé. Les entités associées telles que les services, les groupes de services et les serveurs ne sont pas interrogées. Si vous devez interroger toutes les entités associées, vous devez interroger manuellement les entités ou interroger l'instance.

Pour interroger des entités spécifiques dans NetScaler Console :

À titre d'exemple, cette tâche vous aide à interroger les serveurs virtuels d'équilibrage de charge. De même, vous pouvez également interroger d'autres entités de fonction réseau.

1. Dans NetScaler Console, accédez à **Infrasturcture > Network Functions > Load Balancing > Virtual Servers**.
2. Sélectionnez le serveur virtuel dont l'état est HORS SERVICE, puis cliquez sur **Interroger maintenant**. L'état du serveur virtuel passe maintenant à EN SERVICE.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Programme de télémétrie NetScaler®

Citrix collecte des données de télémétrie de licence de base ainsi que des données de télémétrie d'utilisation des fonctionnalités et de déploiement de NetScaler pour ses intérêts légitimes, y compris la conformité des licences. Vous pouvez télécharger automatiquement ou manuellement les données d'utilisation des licences et des fonctionnalités requises pour rester conforme au programme de télémétrie NetScaler décrit ici. Les données de configuration et d'utilisation des fonctionnalités de NetScaler Console sont également collectées pour gérer, mesurer et améliorer les produits et services Citrix. Si vous êtes un client NetScaler Console existant, vous devez vous assurer d'être conforme au programme de télémétrie NetScaler. Nous vous recommandons vivement d'ajouter des instances NetScaler à NetScaler Console pour améliorer et simplifier globalement vos opérations NetScaler et soutenir l'amélioration de nos produits et services en envoyant des données d'utilisation des fonctionnalités NetScaler. En savoir plus.

Vous pouvez télécharger les données de télémétrie requises de l'une des manières suivantes :

- **Mode de collecte automatisé** - Ce mode est activé par défaut après la mise à niveau vers la version **14.1-25.56 ou ultérieure** / **13.1-53.22 ou ultérieure**. Le mode automatisé crée une connexion sortante pour utiliser le canal activé automatiquement (URL de point de terminaison) et télécharge automatiquement les données de télémétrie. Vous devez seulement vous assurer que les URL de point de terminaison sont accessibles. Étant donné que le téléchargement se produit automatiquement, aucune action n'est requise de votre part, sauf si les prérequis échouent. Pour plus d'informations, consultez Mode de collecte automatisé.
- **Mode de collecte manuel** - Ce mode est activé uniquement si le mode automatisé est désactivé. Vous devez télécharger les données de télémétrie requises depuis la page d'accueil de télémétrie NetScaler dans NetScaler Console sur site et effectuer le premier téléchargement vers le service NetScaler Console dans les 30 jours. Les téléchargements ultérieurs doivent être effectués tous les 90 jours pour rester conforme. Pour plus d'informations, consultez Mode de collecte manuel.

Il est recommandé d'utiliser le mode de télémétrie automatisé et de télécharger les données requises automatiquement, mais vous pouvez également choisir de désactiver le mode automatisé et de les télécharger manuellement. Dans les modes automatisé et manuel, le téléchargement des données est requis pour rester conforme au programme de télémétrie NetScaler. Vous pouvez choisir de désactiver l'inclusion des données de télémétrie facultatives dans le téléchargement,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

mais les données de télémétrie requises pour la conformité des licences et l'utilisation des fonctionnalités doivent être fournies dans les deux modes, automatisé et manuel.

Pour rester conforme, le nombre de jours écoulés depuis le dernier téléchargement réussi ne doit pas dépasser 90 jours.

Dans le cadre du programme de télémétrie NetScaler, les configurations suivantes ont été transmises aux instances NetScaler gérées :

- Configuration AppFlow : `enable ns feature AppFlow`
- Configuration du profil de métriques de télémétrie : `add analytics profile telemetry_metrics_profile -type timeseries -outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300`

REMARQUE :

Pour une collecte de télémétrie optimale, nous vous recommandons de mettre à niveau vers la dernière version de NetScaler Console.

- À partir de la version **14.1-43.x** / **13.1-57.x**, NetScaler Console supprime la configuration du profil de métriques de télémétrie si elle est présente dans vos instances NetScaler. La suppression de la configuration du profil de métriques de télémétrie n'a aucun impact sur les fonctionnalités existantes de vos instances NetScaler.
- Si vous n'utilisez pas les fonctionnalités d'analyse de NetScaler ou de NetScaler Console, vous pouvez utiliser la commande suivante pour supprimer la configuration AppFlow :

  `disable ns feature AppFlow`

Le tableau suivant fournit des détails sur les configurations de profil de métriques AppFlow® et de télémétrie dans la dernière version et les versions antérieures :

VERSION	CONFIGURATIONS DÉPLOYÉES DANS LE CADRE DU PROGRAMME DE TÉLÉMÉTRIE	MODE DE TÉLÉMÉTRIE	ACTION REQUISE
14.1-43.x / 13.1-57.x	Non	Automatisé et manuel	Les configurations ne sont pas poussées vers les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERSION	CONFIGURATIONS DÉPLOYÉES DANS LE CADRE DU PROGRAMME DE TÉLÉMÉTRIE	MODE DE TÉLÉMÉTRIE	ACTION REQUISE
			instances NetScaler et la configuration du profil de métriques de télémétrie est supprimée des instances NetScaler si elle est présente. Si vous n'utilisez pas les fonctionnalités d'analyse de NetScaler ou NetScaler Console, vous pouvez utiliser `disable ns feature AppFlow` pour supprimer la configuration AppFlow.
14.1-29.x / 13.1-55.x	Non	Automatisé et manuel	Les configurations ne sont pas poussées dans le cadre du programme de télémétrie NetScaler. Si ces configurations sont présentes dans vos instances NetScaler et que vous souhaitez les supprimer, exécutez la commande `rm analytics profile telemetry_metrics _profile` sur NetScaler pour supprimer la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERSION	CONFIGURATIONS DÉPLOYÉES DANS LE CADRE DU PROGRAMME DE TÉLÉMÉTRIE	MODE DE TÉLÉMÉTRIE	ACTION REQUISE
			configuration du profil de métriques de télémétrie et utilisez `disable ns feature AppFlow` pour supprimer la configuration AppFlow.
14.1-25.56 / 13.1-53.22	Oui. Les configurations de profil de métriques AppFlow et de télémétrie	Automatisé (avec toutes les conditions préalables remplies)	Les configurations sont poussées dans le cadre du programme de télémétrie NetScaler, mais ne sont pas vérifiées toutes les 24 heures. Pour supprimer ces configurations, exécutez la commande `rm analytics profile telemetry_metrics _profile` sur NetScaler pour supprimer la configuration du profil de métriques de télémétrie et utilisez `disable ns feature AppFlow` pour supprimer la configuration AppFlow.
		Automatisé (avec des conditions	NetScaler Console continue de vérifier

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERSION	CONFIGURATIONS DÉPLOYÉES DANS LE CADRE DU PROGRAMME DE TÉLÉMÉTRIE	MODE DE TÉLÉMÉTRIE	ACTION REQUISE
		préalables non remplies) ou manuel	ces configurations toutes les 24 heures et de les pousser vers les instances NetScaler, si ces configurations sont manquantes. Si vous ne souhaitez pas que les configurations soient poussées, vous devez être en mode automatisé (avec toutes les conditions préalables remplies) ou effectuer une mise à niveau vers la dernière version.

REMARQUES :

- Le fichier `/nsconfig/.telemetry.conf` est mis à jour avec la commande suivante pour la télémétrie Gateway. NetScaler Console vérifie cette commande toutes les heures et l'ajoute si elle est manquante :

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Certains paramètres de télémétrie sont collectés via des scripts qui sont poussés de NetScaler Console vers les instances NetScaler. Ces scripts sont en lecture seule et ne modifient rien dans NetScaler.
- Les informations collectées via la télémétrie, telles que les adresses e-mail, les noms d'utilisateur et les adresses IP, sont pseudonymisées de manière sécurisée en hachant les informations à la source à l'aide d'algorithmes de hachage unidirectionnels. Par conséquent,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix ne peut pas accéder à ces valeurs ni les lire. Ces données de télémétrie sont utilisées uniquement à des fins de correspondance logique des actifs.

Le tableau suivant fournit les détails des paramètres collectés dans le cadre du programme de télémétrie NetScaler :

CATÉGORIES	DESCRIPTION	À QUOI SERT-IL ?	OBLIGATOIRE/ FACULTATIF
Licence, et télémétrie de déploiement et d'utilisation de NetScaler	Informations sur les droits de licence, l'allocation, l'utilisation, les données de déploiement NetScaler de haut niveau et l'utilisation des fonctionnalités NetScaler.	Conformité des licences et pour gérer, mesurer et améliorer le service.	Requis
Télémétrie de déploiement et d'utilisation des fonctionnalités de NetScaler Console	Informations sur le déploiement de la console et l'utilisation des fonctionnalités.	Pour gérer, mesurer et améliorer le service.	Facultatif

Pour plus d'informations sur la liste des paramètres de télémétrie facultatifs et requis, consultez Gouvernance des données.

Citrix exige que vous passiez à la version la plus récente de NetScaler Console (14.1-25.56 ou ultérieure / 13.1–53.22 ou ultérieure) dans les 3 mois à compter du **18 juin 2024**. Après la mise à niveau vers NetScaler Console 14.1-25.56 ou ultérieure / 13.1–53.22 ou ultérieure, l'un des modes de télémétrie (automatique ou manuel) doit être activement fonctionnel. Sauf si vous avez opté pour le rapport manuel, vous acceptez d'ajuster vos pare-feu si nécessaire pour permettre le rapport de télémétrie automatique.

Points à noter :

- Le module de télémétrie exécute plusieurs commandes SSH sur NetScaler et lit la sortie dans la réponse en utilisant l'utilitaire SSH de la console NetScaler. L'utilitaire SSH ne fonctionne pas correctement et la télémétrie échoue si l'une des conditions suivantes est remplie :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le nom d'hôte du système d'exploitation NetScaler contient un caractère '#'.
- Le motd (message du jour) de NetScaler contient un caractère '#'.
- L'invite PS1 de NetScaler contient un caractère '#'.

- Vous devez vous assurer de passer à la dernière version (14.1–25.56 et ultérieure / 13.1–53.22 et ultérieure) d'ici le **18 septembre 2024**.
- Si vous optez pour le mode de télémétrie manuelle, le premier téléchargement doit être effectué dans les 30 jours suivant votre passage à la version ci-dessus, mais au plus tard le 18 octobre 2024. Par la suite, le téléchargement manuel de la télémétrie doit être effectué tous les 90 jours pour que votre NetScaler Console sur site soit conforme au programme de télémétrie NetScaler.

Citrix peut suspendre ou résilier votre support Citrix en cas de non-respect de ces exigences sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas dans la mesure où elles sont interdites par la loi ou la réglementation. Pour plus d'informations, consultez la FAQ sur la télémétrie des licences Citrix.

Modes de collecte de télémétrie

Mode de collecte de télémétrie automatisée

Ce mode est activé par défaut après la mise à niveau vers NetScaler Console sur site 14.1-25.53 / 13.1-53.22 ou une version ultérieure.

Conditions préalables pour le mode de collecte de télémétrie automatisée :

- Assurez-vous de disposer d'une connexion Internet ou d'un serveur proxy configuré dans NetScaler Console sur site pour l'accessibilité à Citrix Cloud. Pour plus d'informations, consultez Configuration système requise.
- Assurez-vous que les URL de point de terminaison suivantes sont accessibles :
  - URL du service de téléchargement : `https://download.citrixnetworkapi.net`
  - URL du service : `https://adm.cloud.com` (requise uniquement dans la version 14.1-43.x ou antérieure).
  - Canal activé automatiquement : `https://safehaven.adm.cloud.com`
- Assurez-vous que le port suivant est ouvert :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	DIRECTION DE LA COMMUNICATION
5140	UDP	Port pour recevoir les données de télémétrie de NetScaler Gateway	De NetScaler vers NetScaler Console

Après la mise à niveau vers la version 14.1-25.53 ou 13.1-53.22 et la navigation vers la page **Télémétrie NetScaler**, cliquez sur **Suivant** dans la fenêtre contextuelle suivante :



Mode de collecte de télémétrie manuel

Pour utiliser le mode de collecte de télémétrie manuel, vous devez d'abord désactiver **Security Advisory**, puis cliquer sur l'ellipse verticale et sélectionner **Désactiver**.



Dans la fenêtre contextuelle, cliquez sur **J'accepte de télécharger les données manuellement** pour désactiver la collecte de télémétrie automatisée. Le mode de collecte de télémétrie passe automatiquement à **Manuel**. En mode télémétrie manuel, les nouvelles mises à jour CVE ne sont pas disponibles et vous ne pouvez utiliser l'avis de sécurité qu'avec les CVE existantes ou les dernières mises à jour.

Après avoir opté pour le mode manuel, vous devez télécharger les données de télémétrie et effectuer le premier téléchargement dans le service NetScaler Console dans les 30 jours. Les téléchargements ultérieurs devront être effectués tous les 90 jours.

REMARQUE :

Un maximum de 2 Go d'espace disque NetScaler Console est utilisé pour enregistrer les données de télémétrie de 90 jours.

Depuis la page d'accueil **Télémétrie NetScaler**, cliquez sur **Télécharger la télémétrie** pour télécharger le fichier bundle (.tgz) qui contient les données de télémétrie requises.



Après avoir téléchargé le fichier de télémétrie, vous devez le télécharger vers le service NetScaler Console. Pour le télécharger dans le service NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Connectez-vous à Citrix Cloud (citrix.cloud.com). Si vous n'avez pas de compte Citrix Cloud, inscrivez-vous pour en créer un nouveau. Pour plus d'informations, consultez Créer un compte Citrix Cloud.
2. Sélectionnez un compte.
3. Sous **NetScaler Console Service**, cliquez sur **Gérer**.
4. Configurez un compte de service Console.
5. Dans le service NetScaler Console, accédez à **Paramètres > Téléchargement de télémétrie sur site de la console**.
6. Cliquez sur **Télécharger la télémétrie** et sélectionnez le fichier téléchargé (.tgz) pour terminer le processus de téléchargement.
7. Effectuez le premier téléchargement dans les 30 jours suivant la sélection du mode manuel. Répétez la même procédure et téléchargez le fichier de télémétrie tous les 90 jours par la suite.

REMARQUES :

- Le téléchargement échoue si le fichier n'est pas dans un format (.tgz) valide ou si le fichier ne passe pas les contrôles d'intégrité. Il est recommandé de le télécharger à nouveau et de réessayer de le charger. Si le problème persiste, contactez le service client.
- Vous pouvez désactiver le téléchargement des données de télémétrie facultatives. Pour désactiver cette option, vous devez d'abord désactiver **Security Advisory** sur la page **Télémétrie NetScaler**, puis accédez à **Paramètres > Administration > Activer ou désactiver le partage des données de fonctionnalités de la console**, et décochez la case **J'accepte de partager les données d'utilisation des fonctionnalités de la console**.

- Dans votre NetScaler Console sur site, une bannière de rappel apparaît 7 jours avant la date d'échéance du téléchargement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnostics pour le dépannage des problèmes de collecte et de téléchargement de télémétrie

Avant la version 14.1 build 56.x, les diagnostics aident à examiner la connectivité sortante vers ces URL de point de terminaison et vous informent si elles sont accessibles. NetScaler On-prem version 14.1 build 56.x et ultérieure fournit des diagnostics améliorés pour identifier et dépanner les problèmes de collecte et de téléchargement de télémétrie au niveau du collecteur (Console) et au niveau du périphérique (instances NetScaler individuelles).

Comportement des diagnostics à partir de la version 14.1 build 56.x

Remarque :

> À partir de la version 14.1 build 56.x, la fonctionnalité de diagnostic de télémétrie est améliorée pour identifier et dépanner les problèmes de collecte et de téléchargement de télémétrie au niveau du collecteur (Console) et au niveau du périphérique (instances NetScaler individuelles).

Toutes les instances NetScaler gérées doivent envoyer des données de télémétrie pour rester conformes. Cependant, les téléchargements et la collecte de télémétrie échouent en raison de problèmes de connectivité ou de configuration. La fonctionnalité de diagnostic sur la page de télémétrie NetScaler de Console on-prem vous aide à identifier et à dépanner rapidement les problèmes aux deux niveaux :

- Niveau du collecteur (Console) : Pour vérifier si les données ont été téléchargées avec succès.
- Niveau du périphérique (instances NetScaler individuelles) : Pour vérifier si les données ont été collectées à partir des instances NetScaler.



Fonctionnement

Voici les étapes générales impliquées dans le processus de diagnostic :

- Exécution automatique : Les diagnostics s'exécutent automatiquement toutes les 24 heures.
- Exécutions à la demande : Les utilisateurs peuvent exécuter les diagnostics manuellement si nécessaire, en particulier après avoir tenté de résoudre un problème.
- Indicateurs d'état : Les résultats sont affichés avec des statuts clairs :
    - Succès : Aucun problème détecté.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Nécessite une attention : Un ou plusieurs problèmes nécessitent une action de l'utilisateur.

REMARQUE :

Cliquez sur **Afficher les détails** ou sur les zones mises en évidence par une erreur pour obtenir des journaux d'erreurs détaillés et des étapes d'atténuation.

Diagnostics au niveau du collecteur (Console)

Cette section vérifie si la NetScaler Console collecte correctement les données des appareils gérés et les télécharge vers la destination requise.

CHAMP DE VÉRIFICATION	DESCRIPTION
Heure d'exécution	Horodatage de la dernière collecte de télémétrie à partir des instances NetScaler gérées.
Version du package	La vérification identifie la version du package de télémétrie installée sur Console sur site, garantissant ainsi la collecte des dernières données.
Statut de téléchargement Evergreen	(Mode automatique uniquement) Console sur site vérifie toutes les 24 heures la présence de packages de scripts de télémétrie mis à jour à partir de l'URL du service de téléchargement. Passez la souris sur l'icône d'information (i) pour voir la cause spécifique de l'échec. Pour obtenir plus de détails sur les étapes d'atténuation, cliquez sur le statut d'échec.
Statut de la connectivité	(Mode automatique uniquement) Confirme que les URL requises sont sur liste blanche et accessibles. Les problèmes de connexion, par exemple une mauvaise configuration du proxy, empêchent la Console d'atteindre ces URL. Passez la souris sur l'icône d'information (i) pour voir la cause spécifique de l'inaccessibilité. Pour obtenir plus de détails

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHAMP DE VÉRIFICATION	DESCRIPTION
	sur les étapes d'atténuation, cliquez sur le **statut Inaccessible**.
	- URL du service de téléchargement : Source pour les téléchargements des derniers paquets de télémétrie.
	- URL du canal activé automatiquement : Destination pour le téléchargement des données de télémétrie.

Diagnostics au niveau de l'appareil (NetScaler)

La Console exécute des diagnostics au niveau de l'appareil en poussant un script de collecte de télémétrie vers chaque instance NetScaler gérée, en collectant les données et en les préparant pour le téléchargement.

Le tableau des détails de télémétrie de l'appareil fournit les résultats de ce processus, notamment :

- Détails de l'appareil
- Statut de la télémétrie
- Codes d'erreur et messages d'erreur

Pour des informations détaillées sur les erreurs et les étapes d'atténuation, cliquez sur les détails de l'erreur surlignés en rouge.

Atténuation : Chaque code d'erreur est associé à une solution recommandée dans le tableau d'atténuation. Suivez la recommandation pour résoudre les problèmes.

Mappage de la table d'erreurs

CODE D'ERREUR	MESSAGE D'ERREUR	ACTION DU CLIENT
1161	Échec de la résolution du nom d'hôte du serveur	Impossible de résoudre l'adresse du serveur. Veuillez vérifier la **configuration du serveur DNS** dans votre

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE D'ERREUR	MESSAGE D'ERREUR	ACTION DU CLIENT
		réseau et le serveur/agent de la console NetScaler.
1162	Impossible de résoudre l'adresse du serveur. Veuillez vérifier la **configuration du serveur DNS** dans votre réseau et le serveur/agent de la console NetScaler.	Impossible de se connecter au serveur. Veuillez vérifier votre **pare-feu, les paramètres du proxy et la connexion réseau**. Vérifiez également que l'URL `download.citrixnetworkapi.net` est accessible depuis votre réseau ou via votre proxy.
1165	Erreur de proxy	Veuillez vérifier votre **configuration du proxy** et assurez-vous que la connectivité réseau fonctionne via le proxy.
1166	Échec de l'authentification du proxy	Veuillez vérifier vos **informations d'identification du proxy** dans la console NetScaler.
1170	Échec de la vérification du certificat SSL.	Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1171	Certificat SSL expiré	**Certificat SSL expiré**.
1172	Échec de la vérification du certificat SSL.	Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1173	Échec de la vérification du certificat SSL.	Cela peut être dû à un **certificat auto-signé**. Si votre réseau utilise un

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE D'ERREUR	MESSAGE D'ERREUR	ACTION DU CLIENT
		intercepteur SSL, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1261	Échec de la résolution du nom d'hôte du serveur	Impossible de résoudre l'adresse du serveur. Veuillez vérifier la **configuration du serveur DNS** dans votre réseau et sur le serveur/agent de la console NetScaler.
1262	Délai d'attente de connexion de la requête	Impossible de se connecter au serveur. Veuillez vérifier votre **pare-feu, vos paramètres de proxy et votre connexion réseau**. Vérifiez que les deux URL (`download.citrixnetworkapi.net` , `safehaven.adm.cloud.com`) sont accessibles depuis votre réseau ou via votre proxy.
1265	Erreur de proxy	Veuillez vérifier votre **configuration de proxy** et assurez-vous que la connectivité réseau fonctionne via le proxy.
1266	Échec de l'authentification du proxy.	Veuillez vérifier vos **informations d'identification du proxy** dans la console NetScaler.
1270	Échec de la vérification du certificat SSL	Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE D'ERREUR	MESSAGE D'ERREUR	ACTION DU CLIENT
		approprié est installé dans la console NetScaler.
1271	Certificat SSL expiré.	Le **certificat SSL du serveur a expiré**.
1272	Échec de la vérification du certificat SSL	Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1273	Échec de la vérification du certificat SSL	Cela peut être dû à un **certificat auto-signé**. Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1361	Échec de la résolution du nom d'hôte du serveur	Impossible de résoudre l'adresse du serveur. Veuillez vérifier la **configuration du serveur DNS** dans votre réseau et le serveur/agent de la console NetScaler.
1362	Délai d'attente de connexion de la requête.	Impossible de se connecter au serveur. Veuillez vérifier votre **pare-feu, les paramètres du proxy et la connexion réseau**. Vérifiez que l'URL `safehaven.adm.cloud.com` est accessible depuis votre réseau ou via votre proxy.
1365	Erreur de proxy	Veuillez vérifier votre **configuration de proxy** et assurez-vous que la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE D'ERREUR	MESSAGE D'ERREUR	ACTION DU CLIENT
		connectivité réseau fonctionne via le proxy.
1366	Échec de l'authentification du proxy	Veuillez vérifier vos **informations d'identification du proxy** dans la console NetScaler.
1370	Échec de la vérification du certificat SSL.	Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1371	Certificat SSL expiré	Le **certificat SSL du serveur a expiré**.
1372	Échec de la vérification du certificat SSL.	Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
1373	La vérification du certificat SSL a échoué.	Cela peut être dû à un **certificat auto-signé**. Si votre réseau utilise un **intercepteur SSL**, assurez-vous que le **certificat racine approprié est installé** dans la console NetScaler.
2000	La télémétrie a été ignorée sur cet appareil.	Cela peut être dû au fait que cet appareil est **géré par une autre console/service/agent NetScaler**. Veuillez vous assurer que l'autre collecteur envoie correctement les données de télémétrie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE D'ERREUR	MESSAGE D'ERREUR	ACTION DU CLIENT
2100	L'état de l'instance est « hors service » ou « non joignable ».	Veuillez vous assurer que l'**instance est en cours d'exécution et joignable**.
2250	Erreur d'authentification SSH	Veuillez vous assurer que le **profil de l'appareil est correctement configuré** dans la console NetScaler pour l'appareil.
2251	Délai d'attente de connexion SSH/connexion refusée.	La connexion peut être temporairement bloquée par un pare-feu ou une politique réseau, ou l'appareil peut être inaccessible. Veuillez **vérifier la connectivité réseau** et vous assurer que le **port SSH est accessible**.
2252	Échec de la vérification de la clé d'hôte	Vérifiez l'identité du serveur auprès de l'administrateur, puis supprimez l'ancienne clé : `ssh-keygen -R <server_address>`.
2350	Erreur d'authentification SSH.	Veuillez vous assurer que le **profil de l'appareil est correctement configuré** dans la console NetScaler pour l'appareil.
2351	Échec de la connexion SSH à l'appareil	La connexion peut être temporairement bloquée par un pare-feu ou une politique réseau, ou l'appareil peut être inaccessible. Veuillez **vérifier la connectivité réseau** et vous assurer que le **port SSH est accessible**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comportement du diagnostic avant la version 14.1 build 56.x

Dans la version 14.1 build 51.x et antérieures, le diagnostic permet d'examiner la connectivité sortante vers ces URL de point de terminaison et vous indique si elles sont accessibles.

- Une fois que les URL des points de terminaison sont accessibles, cliquez sur la page **Accéder à la télémétrie NetScaler®**.
- Si des prérequis échouent, la vérification diagnostique affiche les points de terminaison qui ne sont pas accessibles et vous devez vous assurer que les URL sont accessibles. Cliquez sur **afficher les prérequis** pour voir les détails.
- Vous pouvez exécuter un diagnostic en cliquant sur **Exécuter le diagnostic** pour confirmer si les URL des points de terminaison sont accessibles.
- Si aucune action n'est entreprise, votre NetScaler Console sur site pourrait ne pas être conforme au programme de télémétrie NetScaler.

Dans le cadre du canal activé automatiquement, vous pouvez utiliser la fonctionnalité **Avis de sécurité** avec les dernières mises à jour CVE dans NetScaler Console sur site. La fonctionnalité Avis de sécurité vous permet d'identifier les CVE qui mettent vos instances NetScaler en danger et recommande des mesures correctives. Vous pouvez consulter les derniers détails des CVE qui affectent vos instances NetScaler dans l'Avis de sécurité. Pour plus d'informations, consultez Avis de sécurité.

REMARQUE :

Vous pouvez également désactiver l'Avis de sécurité. Si vous désactivez l'**Avis de sécurité**, ou si vous vous désabonnez du mode de télémétrie automatisé, ou si l'une des conditions préalables échoue, les nouvelles mises à jour CVE ne sont pas disponibles et vous ne pouvez utiliser l'Avis de sécurité qu'avec les CVE existantes ou les dernières mises à jour.

- Une fois la collecte de télémétrie automatisée activée avec succès, le premier téléchargement a lieu dans les 24 heures. Les téléchargements suivants ont lieu toutes les 24 heures automatiquement. Le statut passe à **Succès** une fois le téléchargement terminé.
-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si le téléchargement échoue, assurez-vous que les URL des points de terminaison sont accessibles. Si le statut indique qu'elles sont accessibles et que le téléchargement échoue toujours, contactez le Service client.

Notifications pour les téléchargements de télémétrie

Par défaut, les notifications par e-mail sont activées pour les téléchargements de télémétrie. La condition préalable pour recevoir une notification par e-mail est de configurer une liste de distribution d'e-mails. Pour plus d'informations, consultez Configurer les paramètres de notification
En tant qu'administrateur, vous recevez des notifications par e-mail pour les scénarios suivants :

- **Échec de la collecte de télémétrie** - Des notifications par e-mail sont envoyées toutes les 24 heures jusqu'à ce que le problème soit résolu. La notification inclut les adresses IP NetScaler et Console affectées par le problème.
- **Échec du téléchargement en mode automatisé** - Une notification par e-mail est reçue toutes les 24 heures jusqu'à ce que le problème soit résolu.
- **Date limite imminente pour le téléchargement manuel** (uniquement si le mode manuel est activé) - Une notification par e-mail est reçue pendant l'événement et un autre e-mail après la fin du téléchargement.
- **Délai dépassé pour le téléchargement manuel** (uniquement si le mode manuel est activé) - Une notification par e-mail est reçue pendant l'événement et un autre e-mail après la fin du téléchargement.

REMARQUE :

La notification concernant le problème de collecte de télémétrie sur les appliances NetScaler apparaît également sous forme de bannière chaque fois qu'un utilisateur se connecte à l'interface utilisateur de la console.

Voici un exemple de notification par e-mail et de bannière en cas d'échec de la collecte de télémétrie sur les appliances NetScaler :



Vous pouvez désactiver la notification par e-mail. Pour désactiver :

1. Accédez à **Paramètres > Administration > Configurer la notification d'événement et le résumé**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans **Notification d'événement > Configurer les notifications système**, recherchez **TelemetryMonitoring**, supprimez cette notification et cliquez sur **Enregistrer**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gouvernance des données

Tous les clients NetScaler Console existants doivent être conformes au programme de télémétrie NetScaler en téléchargeant les données de télémétrie requises, soit en mode automatique, soit en mode manuel. Le programme de télémétrie NetScaler est activé à partir des versions 14.1-25.53 et ultérieures / 13.1-53.22 et ultérieures. Pour plus d'informations, consultez le programme de télémétrie NetScaler.

Citrix collecte des données de télémétrie de licence de base ainsi que des données de télémétrie d'utilisation des fonctionnalités et de déploiement de NetScaler® pour ses intérêts légitimes, y compris la conformité des licences. Les données de configuration et d'utilisation des fonctionnalités de NetScaler Console sont également collectées pour gérer, mesurer et améliorer les produits et services Citrix.

Le mode de collecte de télémétrie automatisé vous permet d'utiliser la fonctionnalité **Security Advisory** dans NetScaler Console sur site qui collecte les paramètres de télémétrie facultatifs. Vous pouvez désactiver les paramètres facultatifs, mais pas les paramètres obligatoires.

REMARQUES :

- Après la mise à niveau vers NetScaler Console version **14.1-25.53 ou ultérieure** / **13.1-53.22 ou ultérieure**, la configuration suivante est automatiquement transmise à vos instances NetScaler via NetScaler Console. Cette configuration collecte et stocke les métriques de télémétrie dans vos instances NetScaler :

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

- Si vous êtes en mode manuel ou en mode automatique (avec une condition préalable non remplie), NetScaler Console continue de vérifier la configuration ci-dessus toutes les 24 heures et de la transmettre aux instances NetScaler, si cette configuration est manquante. Si vous ne souhaitez pas que la configuration soit transmise, vous devez être en mode automatique (avec

© 1997–2026 Citrix Systems, Inc. All rights reserved.

toutes les conditions préalables remplies) ou effectuer une mise à niveau vers la version à venir (**14.1-29.x** ou **13.1-55.x**).

- Le fichier `/nsconfig/.telemetry.conf` est mis à jour avec la commande suivante pour la télémétrie Gateway. NetScaler Console vérifie cette commande toutes les heures et l'ajoute, si cette commande est manquante :

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Certains paramètres de télémétrie sont collectés via des scripts qui sont transmis de NetScaler Console aux instances NetScaler. Ces scripts sont en lecture seule et ne modifient rien dans NetScaler.
- Les informations collectées via la télémétrie, telles que les adresses e-mail, les noms d'utilisateur et les adresses IP, sont pseudonymisées de manière sécurisée en hachant les informations à la source à l'aide d'algorithmes de hachage unidirectionnels. Par conséquent, Citrix ne peut pas accéder à ces valeurs ni les lire. Ces données de télémétrie sont utilisées uniquement à des fins de correspondance logique des actifs.

Le tableau suivant fournit les détails des paramètres qui sont collectés dans le cadre du programme de télémétrie NetScaler :

CATÉGORIES	DESCRIPTION	À QUOI L'UTILISONS-NOUS ?	OBLIGATOIRE / FACULTATIF
Licence, et télémétrie de déploiement et d'utilisation de NetScaler	Informations sur les droits de licence, l'allocation, l'utilisation, les données de déploiement NetScaler de haut niveau et l'utilisation des fonctionnalités NetScaler.	Conformité des licences et pour gérer, mesurer et améliorer le service.	Requis
Télémétrie de déploiement et d'utilisation des fonctionnalités de NetScaler Console	Informations sur le déploiement de la Console et l'utilisation des fonctionnalités.	Pour gérer, mesurer et améliorer le service.	Facultatif

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour désactiver les paramètres facultatifs :

1. Dans NetScaler Console sur site, accédez à **Télémétrie NetScaler** et désactivez **Avis de sécurité**.
2. Accédez à **Paramètres > Administration > Activer ou désactiver le partage de données de fonctionnalités de la Console**, et décochez la case **J'accepte de partager les données d'utilisation des fonctionnalités de la Console**.

Si votre NetScaler Console est une version comprise entre 14.1-8.x et 14.1-21.x, la collecte de données est activée après avoir configuré Cloud Connect et activé la fonctionnalité Avis de sécurité. Pour plus d'informations, consultez Gouvernance des données pour Cloud Connect

Si votre NetScaler Console est en version 14.1-4.x ou inférieure, vous pouvez créer une identité client sur Citrix Cloud pour envoyer des statistiques importantes sur la santé, l'état et d'autres métriques de NetScaler Console depuis le déploiement sur site de NetScaler Console vers le compte Citrix Cloud. Citrix collecte des statistiques pour comprendre l'utilisation de NetScaler Console. Pour plus d'informations, consultez Gouvernance des données pour l'identité client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONDITIONS D'UTILISATION DES INFORMATIONS IoC

En utilisant les informations IoC (telles que définies ci-dessous), vous reconnaissez et acceptez les conditions d'utilisation suivantes :

Citrix Systems, Inc. et/ou ses filiales (« Citrix ») a développé un script logique d'indicateurs de compromission et des directives connexes concernant les indicateurs de compromission (collectivement, les « informations IoC ») pour aider les organisations à déterminer si leurs environnements sont potentiellement compromis.

Les informations IoC n'englobent pas toutes les techniques, tactiques ou procédures (« TTP ») que les acteurs de la menace peuvent utiliser lorsqu'ils ciblent des environnements pertinents. De plus, les acteurs de la menace modifient fréquemment les TTP et l'infrastructure. Pour ces raisons et d'autres, les informations IoC peuvent avoir une valeur médico-légale limitée et peuvent ne pas identifier les compromissions réelles. Il vous est fortement conseillé de faire appel aux services d'enquêteurs médico-légaux expérimentés pour évaluer votre environnement.

Les informations IoC sont fournies telles quelles. Citrix ne fait aucune garantie ou déclaration, expresse ou implicite, concernant les informations IoC, y compris, sans limitation, que les informations IoC sont exemptes d'erreurs ou répondent à des conditions de qualité marchande ou d'adéquation à un usage particulier.

Les informations IoC sont des informations confidentielles et propriétaires de Citrix et sont soumises aux termes et conditions de l'accord(s) de confidentialité applicable(s) en vigueur entre le destinataire de ces documents et Citrix. Aucune partie des informations IoC ne peut être reproduite, redistribuée ou transmise à un tiers sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable expresse de Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licences NetScaler Console

Licences

NetScaler Console nécessite une licence NetScaler vérifiée pour gérer et surveiller les instances NetScaler, lorsque les instances sont découvertes via le protocole `https`.

NetScaler Console prend en charge les éditions de licence suivantes. Contactez votre représentant commercial ou partenaire NetScaler pour acheter une licence NetScaler Console.

Édition Express – Vous pouvez gérer et surveiller n'importe quel nombre d'instances avec la licence Édition Express. Par défaut, la licence Édition Express est appliquée.

Édition Advanced - Elle permet de gérer les applications découvertes et d'afficher les analyses pour les serveurs virtuels achetés ainsi que pour les serveurs virtuels gratuits.

Points à noter :

- Pour la version **13.1-9.x ou antérieure**, vous pouvez gérer jusqu'à 30 applications découvertes ou serveurs virtuels et afficher les analyses. Au-delà des 30 applications découvertes ou des 30 serveurs virtuels, vous devez acheter et appliquer une licence Advanced. Par exemple, si vous achetez 100 licences de serveurs virtuels, vous avez le droit d'utiliser jusqu'à 130 licences de serveurs virtuels.
- Pour la version **13.1-12.x ou ultérieure**, vous pouvez gérer jusqu'à deux applications découvertes ou serveurs virtuels et afficher les analyses. Au-delà des deux applications découvertes ou des deux serveurs virtuels, vous devez acheter et appliquer une licence Advanced. Par exemple, si vous achetez 100 licences de serveurs virtuels, vous avez le droit d'utiliser jusqu'à 102 licences de serveurs virtuels.

Après la mise à niveau vers les versions de 13.1-12.x jusqu'à 14.1-17.x :

- Tous les serveurs virtuels gratuits par défaut Express restent fonctionnels pendant 30 jours. Vous pouvez sélectionner les deux serveurs virtuels et appliquer les deux licences par défaut dans un délai de 30 jours. Si aucune action de l'utilisateur n'est effectuée 30 jours après la mise à niveau, NetScaler Console applique aléatoirement la licence à deux serveurs virtuels et retire la licence des serveurs virtuels restants. Vous devez acheter et appliquer de nouvelles licences Advanced pour activer ces serveurs virtuels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Après la mise à niveau, voici les changements de comportement de NetScaler Console :
  - NetScaler Console accorde 30 jours supplémentaires pour prendre les mesures requises.
  - Pendant la période de 30 jours, l'allocation de nouveaux serveurs virtuels pour les 30 serveurs virtuels gratuits Express est bloquée.
    - Par exemple, si le nombre de licences de serveurs virtuels disponibles avant la mise à niveau vers la version 12.x était de 30 et que seulement 20 serveurs virtuels sous licence étaient utilisés, vous n'êtes autorisé à utiliser que les 20 serveurs virtuels et n'êtes pas autorisé à licencier les 10 serveurs virtuels restants pendant la période de 30 jours.
  - Cependant, pendant la période de 30 jours, en tant qu'administrateur, vous pouvez toujours appliquer des licences NetScaler Console Advanced et allouer de nouveaux serveurs virtuels.

Le tableau suivant fournit les détails de la licence :

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION AVANCÉE	LICENCE NETSCALER
Applications	Tableau de bord des applications	Jusqu'à deux serveurs virtuels.	Donne droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Les informations relatives au pare-feu d'applications Web NetScaler sur le tableau de bord des applications nécessitent une licence Premium (ou) Advanced avec App Firewall.
	Web Insight	Jusqu'à deux serveurs virtuels.	Donne droit à toutes les licences de serveurs virtuels achetées et à	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION AVANCÉE	LICENCE NETSCALER
			deux serveurs virtuels supplémentaires.	
	Graphique de service	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	NA
	Configuration > StyleBooks	Illimité	Illimité	NA
Sécurité	Tableau de bord de sécurité	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Les informations relatives au pare-feu d'applications Web NetScaler sur le tableau de bord de sécurité nécessitent une licence Premium (ou) Advanced avec App Firewall.
	Violations de sécurité	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels	Premium (ou) Advanced avec licence App Firewall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION AVANCÉE	LICENCE NETSCALER
			supplémentaires.	
	Utilisateurs et points de terminaison	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	NA
Gateway	HDX Insight	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Advanced (rapports < 1 heure) Premium (rapports = Illimité)
	Gateway Insight	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Advanced (rapports < 1 heure) Premium (rapports = Illimité)
Infrastructure	Analyse d'infrastructure	Illimité	Illimité	NA
	Instances	Illimité	Illimité	NA
	Tableau de bord SSL	Illimité	Illimité	NA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION AVANCÉE	LICENCE NETSCALER
	Événements	Illimité	Illimité	N/A
	Fonctions réseau	Illimité	Illimité	N/A
	Rapports réseau	Illimité	Illimité	N/A
	Licences mutualisées	Illimité	Illimité	N/A
	Configuration > Tâches de configuration, Modèles de configuration et Conseils de configuration	Illimité	Illimité	NA
	Tâches de mise à niveau	Illimité	Illimité	NA
	Orchestration	Illimité	Illimité	NA
Paramètres	RBAC et authentification externe (niveau d'instance)	Illimité	Illimité	NA
	RBAC et authentification externe	Illimité	Illimité	NA

*Pour l'intégration de Citrix Director avec la prise en charge de NetScaler Console, Citrix Director doit disposer d'une licence Premium.

Des licences pour davantage de serveurs virtuels sont disponibles par packs de 10 serveurs virtuels. Vous pouvez obtenir une licence valide et l'ajouter sur les serveurs NetScaler Console via l'interface graphique de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Haute disponibilité

Le serveur NetScaler Console peut contenir des licences VIP, CICO et de capacité groupée. Lorsque les licences sont émises pour un serveur NetScaler Console, elles sont liées à l'ID d'hôte du serveur. L'attribution de licences à un autre serveur NetScaler Console est restreinte.

Si vous configurez une paire haute disponibilité NetScaler Console en tant que serveur de licences, les serveurs principal et secondaire doivent disposer des mêmes fichiers de licence. Par conséquent, dans le déploiement haute disponibilité de NetScaler Console, NetScaler Console prend en charge l'attribution des mêmes fichiers de licence aux deux serveurs.

REMARQUE

- Si vous avez installé NetScaler Console version 12.1-49.x ou antérieure, vous disposez de 30 jours pour maintenir la licence sur le nœud secondaire. Après 30 jours, vous devez contacter Citrix pour réhéberger la licence d'origine.
- Dans la version 12.1-50.x et ultérieure, la licence NetScaler Console est automatiquement synchronisée avec le nœud secondaire.
- Les licences groupées sont automatiquement synchronisées avec le nœud secondaire dans la version 12.1-50.x et ultérieure.

Comment les licences sont-elles synchronisées entre les nœuds haute disponibilité de NetScaler Console ?

Chaque fois qu'un basculement se produit, le serveur secondaire assume le rôle de serveur principal. L'ID d'hôte réel du serveur principal est configuré comme l'ID d'hôte virtuel du nouveau serveur principal. Les fichiers de licence reconnaissent le nouveau serveur principal à l'aide de l'ID d'hôte virtuel.

- **ID d'hôte réel** - Cet ID est généré à partir d'une adresse MAC du serveur NetScaler Console. Chaque déploiement autonome de NetScaler Console possède un ID d'hôte unique.
- **ID d'hôte virtuel** - Cet ID est généré automatiquement lors du déploiement HA. L'ID d'hôte réel d'un serveur principal NetScaler Console est utilisé comme ID d'hôte virtuel du serveur secondaire. Cet ID est stocké dans la base de données NetScaler Console dans un format chiffré et toute modification de cet ID est restreinte. L'ID d'hôte virtuel est préféré à l'ID d'hôte réel.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supposons que le nœud 1 est le serveur principal et le nœud 2 est le serveur secondaire. L'ID d'hôte virtuel du nœud 1 est synchronisé avec le nœud 2.

1. Les fichiers de licence disponibles sur le nœud 1 sont synchronisés avec le nœud 2.
2. Tout nouveau fichier de licence sur le nœud 1 est synchronisé périodiquement avec le nœud 2.
3. NetScaler Console garantit que le serveur de licences ne s'exécute que sur le nœud 1 afin d'éviter le doublement de la capacité de licence.
4. Les instances NetScaler extraient les licences du nœud 1 à l'aide de l'adresse IP flottante.

Les licences sont verrouillées sur les instances NetScaler. Pour extraire des licences de NetScaler Console HA, les instances nécessitent l'adresse IP spécifique de NetScalerNetScaler. Lorsque vous appliquez des licences sur un serveur principal qui sera en charge de la gestion des licences, cela s'applique à toutes les futures licences sur cette instance. Vous ne pouvez supprimer les licences que du serveur sur lequel vous les avez installées.

Orchestration

Le module d'orchestration est indépendant de la gestion des licences et est toujours disponible.

Mettre à niveau les licences de serveur virtuel

Vous pouvez mettre à niveau la gestion des licences sur NetScaler Console pour surveiller et gérer davantage de serveurs virtuels hébergés sur NetScaler.

Pour mettre à niveau vos licences NetScaler :

1. Connectez-vous à NetScaler Console à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Infrastructure > Licences en pool**.
3. Accédez à **Fichiers de licence**, puis sélectionnez l'une des options suivantes :
    - **Télécharger les fichiers de licence depuis un ordinateur local**. Si une licence est déjà présente sur votre ordinateur local, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez utiliser pour allouer vos licences. Cliquez sur **Terminer**.
    - **Utiliser le code d'activation de licence**. Citrix envoie par e-mail le code d'accès à la licence que vous avez achetée. Saisissez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir les licences**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si vous sélectionnez cette option, NetScaler Console doit être connecté à Internet, ou un serveur proxy doit être disponible.

4. Vous pouvez ajouter d'autres licences à tout moment depuis la page Paramètres de licence.

Vérification

Vous pouvez vérifier les licences installées sur NetScaler Console en accédant à **Paramètres > Configuration des licences et de l'analyse**.



Gérer les serveurs virtuels

Vous pouvez sélectionner les serveurs virtuels ou les serveurs virtuels tiers que vous souhaitez gérer et surveiller via NetScaler Console.

POINTS À NOTER

- Par défaut, NetScaler Console attribue automatiquement des licences aux serveurs virtuels de manière aléatoire après chaque cycle d'interrogation des serveurs virtuels.
- Si le nombre total de serveurs virtuels découverts dans votre NetScaler Console est inférieur au nombre de licences de serveurs virtuels installées, NetScaler Console attribue par défaut des licences à tous les serveurs virtuels.

Pour sélectionner manuellement les serveurs virtuels ou pour limiter l'attribution de licences à un nombre restreint de serveurs virtuels, vous devez d'abord désactiver l'attribution automatique de licences aux serveurs virtuels, puis sélectionner les serveurs virtuels que vous souhaitez gérer.

Désactiver l'attribution automatique de licences aux serveurs virtuels

1. Accédez à **Paramètres > Configuration des licences et des analyses**.

   Le tableau de bord affiche les licences de serveurs virtuels disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de la licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans **Allocation de licences de serveurs virtuels**, désactivez **Serveurs virtuels sous licence automatique** et **Sélection automatique des serveurs virtuels non adressables**.



Sélectionner des serveurs virtuels tiers pour l'attribution de licences

1. Accédez à **Paramètres > Configuration des licences et des analyses**.

   Le tableau de bord affiche les licences de serveurs virtuels disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de la licence.

2. Dans **Résumé des serveurs virtuels tiers**, désactivez **Sélection automatique des serveurs virtuels tiers**.



Appliquer manuellement les licences de serveurs virtuels

Vous pouvez appliquer manuellement des licences à un serveur virtuel individuel.

1. Dans **Allocation de licences de serveur virtuel**, sélectionnez **Configurer les licences**.

   La page **Tous les serveurs virtuels** s'affiche.

2. Filtrez les serveurs virtuels sans licence à l'aide de la propriété : `Licensed: No`.
3. Sélectionnez le serveur virtuel que vous souhaitez licencier.
4. Cliquez sur **Licence**.

Configurer la licence de serveur virtuel basée sur une stratégie

Vous pouvez configurer une stratégie pour appliquer des licences aux serveurs virtuels. Cette stratégie contrôle le nombre de serveurs virtuels que vous souhaitez licencier automatiquement. Elle applique également des licences uniquement aux serveurs virtuels des instances sélectionnées.

Cliquez sur **Modifier les stratégies** et vous pouvez spécifier les éléments suivants :

- Définissez séparément la limite de serveurs virtuels sur les instances CPX pour appliquer les licences. NetScaler Console applique la licence aux serveurs virtuels sur les instances CPX jusqu'à une limite spécifiée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

Cette limite s'applique aux instances CPX, à l'exception des types de déploiement sidecar.

Pour afficher les instances CPX des types de déploiement sidecar, filtrez les serveurs virtuels à l'aide de la propriété : `License Type: Freely Managed`.

- Définissez la limite de serveurs virtuels sur les instances NetScaler sélectionnées (MPX/VPX/BLX) pour appliquer les licences. NetScaler Console applique les licences aux serveurs virtuels sur les instances NetScaler jusqu'à une limite spécifiée.
- Sélectionnez les instances NetScaler prioritaires pour appliquer les licences de serveur virtuel. Par conséquent, NetScaler Console ne peut appliquer de licence qu'aux serveurs virtuels des instances sélectionnées.

Modifier la politique pour appliquer les licences aux serveurs virtuels(/en-us/netscaler-application-delivery-management-software/media/configure-license-policy.png)

Afficher les serveurs virtuels sous licence

Une fois les licences appliquées aux serveurs virtuels, vous pouvez afficher les serveurs virtuels sous licence ou les serveurs virtuels tiers.

1. Accédez à **Paramètres > Configuration des licences et de l'analyse**.
2. Cliquez sur le type de serveur virtuel dans la section **Total sous licence** du **Résumé des licences des serveurs virtuels**.

Configurer la prise en charge automatique des licences pour les serveurs virtuels non adressables

Par défaut, NetScaler Console n'applique pas automatiquement les licences aux serveurs virtuels non adressables. Pour attribuer des licences aux serveurs virtuels non adressables, vous devez désactiver l'option de licence automatique et sélectionner manuellement les serveurs virtuels non adressables. Cela augmente vos efforts pour sélectionner manuellement les serveurs non adressables initialement lors de l'application des licences. Vous devez également sélectionner manuellement les nouveaux serveurs virtuels non adressables chaque fois qu'ils sont ajoutés à votre réseau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console propose une option sous **Allocation de licences de serveurs virtuels**. Si vous activez l'option **Sélectionner automatiquement les serveurs virtuels non adressables**, les licences sont appliquées automatiquement aux serveurs virtuels non adressables.

REMARQUE

- Par défaut, NetScaler Console ne sélectionne toujours pas automatiquement les serveurs virtuels non adressables pour l'octroi de licences.
- L'analyse des applications (tableau de bord des applications) est la seule analyse actuellement prise en charge sur les serveurs virtuels non adressables sous licence.

Licences

À partir de la version **14.1-21.x**, le concept de VIP sous licence est supprimé. Un nombre illimité de VIP est désormais disponible dans NetScaler Console sur site. Vous n'avez plus besoin d'acheter de licences de serveur virtuel NetScaler Console, car la référence de licence VIP sera bientôt en fin de vente (EOS) et en fin de renouvellement (EOR).

Le tableau suivant fournit les détails des licences :

FONCTIONNALITÉS	OPTIONS	LICENCE NETSCALER
Applications	Tableau de bord des applications	Les informations relatives au pare-feu d'applications Web NetScaler sur le tableau de bord des applications nécessitent une licence Premium (ou) Advanced avec App Firewall.
	Web Insight	N/A
	Service Graph	N/A
	Configuration > StyleBooks	N/A
Sécurité	Tableau de bord de sécurité	Les informations relatives au pare-feu d'applications Web NetScaler sur le tableau de bord de sécurité nécessitent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	LICENCE NETSCALER
		une licence Premium (ou) Advanced avec App Firewall.
	Violations de sécurité	Licence Premium (ou) Advanced avec App Firewall
	Utilisateurs et points de terminaison	N/A
Passerelle	HDX Insight	Advanced (rapports < 1 heure) Premium (rapports = Illimité)
	Gateway Insight	Advanced (rapports < 1 heure) Premium (rapports = Illimité)
Infrastructure	Analyse de l'infrastructure	N/A
	Instances	NA
	Tableau de bord SSL	NA
	Événements	NA
	Fonctions réseau	NA
	Rapports réseau	NA
	Licences en pool	NA
	Configuration > Tâches de configuration, Modèles de configuration et Conseils de configuration	NA
	Tâches de mise à niveau	NA
	Orchestration	NA
Paramètres	RBAC et authentification externe (niveau d'instance)	NA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	LICENCE NETSCALER
	RBAC et authentification externe	NA

*Pour l'intégration de Citrix Director avec la prise en charge de NetScaler Console – Citrix Director doit disposer d'une licence Premium.

Haute disponibilité

Le serveur NetScaler Console peut contenir des licences VIP, CICO et de capacité groupée. Lorsque les licences sont émises pour un serveur NetScaler Console, elles sont liées à l'ID d'hôte du serveur. L'attribution de licences à un autre serveur NetScaler Console est restreinte.

Si vous configurez une paire haute disponibilité NetScaler Console en tant que serveur de licences, les fichiers de licence appliqués sur le nœud principal sont synchronisés avec le nœud secondaire.

REMARQUE :

- Dans la version 12.1-50.x et ultérieure, les licences NetScaler Console sont automatiquement synchronisées du nœud principal vers le nœud secondaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exigences système

Avant d'installer NetScaler Console, vous devez comprendre les exigences logicielles, les exigences de navigateur, les informations de port, les informations de licence et les limitations.

Exigences pour NetScaler Console

COMPOSANT	EXIGENCE
RAM	32 Go
Processeur virtuel	8 processeurs
	Remarque : Nous recommandons l'utilisation de la technologie de disque SSD (Solid-State Drive) pour les déploiements de NetScaler Console.
Espace de stockage	L'espace de stockage par défaut requis est de 120 Go. L'exigence de stockage réelle dépend de l'estimation du dimensionnement de NetScaler Console.
	Si votre exigence de stockage NetScaler Console dépasse 120 Go, vous devez attacher un disque supplémentaire. Vous ne pouvez ajouter qu'un seul disque supplémentaire.
	Nous vous recommandons d'estimer le stockage et de joindre des disques supplémentaires au moment du déploiement initial.
	Pour plus d'informations, consultez Comment attacher un disque supplémentaire à NetScaler Console.
Interfaces réseau virtuelles	1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANT	EXIGENCE
Débit	1 Gbit/s ou 100 Mbit/s

Exigences pour l'agent NetScaler Console sur site

COMPOSANT	EXIGENCE
RAM	32 Go
Processeur virtuel	8 processeurs
Espace de stockage	30 Go
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

REMARQUE

Le processeur AMD est pris en charge dans :

- **NetScaler Console 13.1 build 4.43 ou version ultérieure**.
- **Agent NetScaler 13.1 build 17.42 ou version ultérieure**.

Version minimale de NetScaler requise pour les fonctionnalités de NetScaler Console

IMPORTANT

La version et le build de NetScaler Console doivent être **égaux ou supérieurs** à la version et au build de votre NetScaler. Par exemple, si vous avez installé NetScaler Console 12.1 Build 50.39, assurez-vous d'avoir installé NetScaler 12.1 Build 50.28/50.31 ou une version antérieure.

FONCTIONNALITÉ NETSCALER CONSOLE	VERSION DU LOGICIEL NETSCALER
StyleBooks	10.5 et versions ultérieures

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉ NETSCALER CONSOLE	VERSION DU LOGICIEL NETSCALER
Prise en charge d'OpenStack/CloudStack	11.0 et versions ultérieures, si une partition est requise
	11.1 et versions ultérieures, si une partition sur un réseau local virtuel partagé est requise
Prise en charge de NSX	11.1 Build 47.14 et versions ultérieures (VPX)
Prise en charge de Mesos/Marathon	10.5 et versions ultérieures
Sauvegarde/Restauration	Pour NetScaler, 10.1 et versions ultérieures
	Pour NetScaler SDX, 11.0 et versions ultérieures
Surveillance/Rapports et configuration à l'aide de tâches	10.1 et versions ultérieures
Fonctionnalités d'analyse	
Web Insight	10.5 et versions ultérieures
HDX Insight	10.1 et versions ultérieures
Violations de sécurité WAF	11.0.65.31 et versions ultérieures
Gateway Insight	11.0.65.31 et versions ultérieures
Cache Insight	10.5 et versions ultérieures*
SSL Insight	12.0 et versions ultérieures

* Les métriques de cache intégrées ne sont pas prises en charge dans NetScaler Console avec les instances NetScaler exécutant la version 11.0 build 66.x.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exigences pour l'analyse NetScaler Console

Versions minimales de Citrix Virtual Apps and Desktops requises pour les fonctionnalités de NetScaler Console

FONCTIONNALITÉ NETSCALER CONSOLE	VERSION DE CITRIX VIRTUAL APPS AND DESKTOPS
HDX Insight	Citrix Virtual Apps and Desktops 7.0 et versions ultérieures

REMARQUE

La fonctionnalité NetScaler Gateway (commercialisée sous le nom Access Gateway Enterprise pour les versions 9.3 et 10.x) doit être disponible sur l'instance NetScaler. NetScaler Console ne prend pas en charge les appliances Access Gateway Standard autonomes.

NetScaler Console peut générer des rapports pour les applications publiées sur Citrix Virtual Apps ou Citrix Virtual Desktops et accessibles via Citrix Workspace. Cependant, cette fonctionnalité dépend du système d'exploitation sur lequel Workspace est installé. Actuellement, un NetScaler n'analyse pas le trafic ICA pour les applications ou les bureaux accessibles via Citrix Workspace exécuté sur les systèmes d'exploitation iOS ou Android.

Clients légers pris en charge pour HDX™ insight

- Clients légers Dell Wyse basés sur Windows
- Clients légers Dell Wyse basés sur Linux
- Clients légers Dell Wyse basés sur ThinOS
- Clients légers 10ZiG basés sur Ubuntu
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

Licence d'instance NetScaler requise pour HDX insight

Les données collectées par NetScaler Console pour HDX Insight dépendent de la version et des licences des instances NetScaler surveillées. Les rapports HDX Insight sont affichés uniquement pour les appliances NetScaler Premium et Advanced exécutant la version 10.5 et ultérieure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LICENCE/ DURÉE NETSCALER	5 MINUTES	1 HEURE	1 JOUR	1 SEMAINE	> 1 MOIS
Standard	Non	Non	Non	Non	Non
Avancé	Oui	Oui	Non	Non	Non
Premium	Oui	Oui	Oui	Oui	Oui

Hyperviseurs pris en charge

Le tableau suivant répertorie les hyperviseurs pris en charge par NetScaler Console :

HYPERVISEUR	VERSIONS
XenServer	7.1, 7.4 et 8.0
VMware ESX	6.0, 6.5, 6.7, 7.0, 8.0 (à partir de 14.1-21.x et versions ultérieures) et 8.0.2b (à partir de 14.1-25.x et versions ultérieures)
Microsoft Hyper-V	2012 R2, 2016, 2019 et 2022
KVM générique	RHEL 7.4, RHEL 8.0, Ubuntu 16.04 et Ubuntu 18.04
Hyperviseur Nutanix (AHV)	6.5.2 (à partir de 14.1-38.x et versions ultérieures)

Systèmes d'exploitation et versions de Workspace pris en charge

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par NetScaler Console et les versions de Citrix Workspace actuellement prises en charge avec chaque système :

SYSTÈME D'EXPLOITATION	VERSION DE WORKSPACE
Windows	4.0 Édition Standard

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SYSTÈME D'EXPLOITATION	VERSION DE WORKSPACE
Linux	13.0.265571 et versions ultérieures
Mac	11.8, build 238301 et versions ultérieures
HTML5	1.5
Application Chrome	1.5

Navigateurs pris en charge

Le tableau suivant répertorie les navigateurs web pris en charge par NetScaler Console :

NAVIGATEUR WEB	VERSION
Microsoft Edge	79 et versions ultérieures
Google Chrome	51 et versions ultérieures
Safari	10 et versions ultérieures
Mozilla Firefox	52 et versions ultérieures

Ports pris en charge

NetScaler Console utilise l'adresse IP NetScaler (connue sous le nom de NSIP) pour communiquer avec NetScaler. Vous pouvez utiliser un agent comme intermédiaire entre l'instance NetScaler et NetScaler Console. Pour établir une communication avec ces serveurs, ouvrez les ports requis.

- Pour la communication AppFlow et de flux de journaux de NetScaler vers NetScaler Console, l'adresse IP de sous-réseau (connue sous le nom de SNIP) est utilisée.
- Pour la communication liée aux licences de NetScaler vers NetScaler Console, l'adresse NSIP est utilisée.
- Si l'adresse SNIP est activée pour l'accès de gestion et si NetScaler est ajouté dans NetScaler Console en utilisant l'adresse SNIP, alors l'adresse SNIP est utilisée comme adresse IP source pour les événements et les Syslogs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si vous avez configuré des NetScalers en mode haute disponibilité, NetScaler Console utilise NSIP pour communiquer avec NetScaler et les ports requis restent les mêmes.

Diagramme des ports réseau pour un déploiement sans agent :



Diagramme des ports réseau pour le déploiement incluant l'agent NetScaler® :



Diagramme des ports réseau pour le déploiement NetScaler Console en haute disponibilité :



Si deux serveurs NetScaler Console sont configurés en mode haute disponibilité, lors de l'ajout d'une instance :

- NetScaler Console communique avec NetScaler via l'adresse IP principale.
- NetScaler établit la connectivité avec NetScaler Console via l'adresse IP flottante de NetScaler Console. Cela implique que NetScaler dirige tout le trafic SNMP, Syslog et Analytics vers l'adresse IP flottante de NetScaler Console.

Les sections suivantes expliquent les ports requis et leur objectif :

- Serveur NetScaler Console
- Agent NetScaler
- Instance NetScaler
- Serveurs externes

Ports pour le serveur NetScaler Console

Le tableau suivant explique les ports requis qui doivent être ouverts sur le serveur NetScaler Console.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
80/443/5454/22	TCP	Port par défaut pour la communication et la synchronisation de la base de données entre les nœuds	Nœud principal NetScaler Console vers le nœud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
		NetScaler Console en mode haute disponibilité. **Remarque :** Ce port est également utilisé pour la télémétrie NetScaler.	secondaire NetScaler Console
443/8443/7443	TCP	Port pour la communication entre l'agent NetScaler et NetScaler Console.	L'agent NetScaler initie la communication avec NetScaler Console. Ensuite, NetScaler Console et l'agent interagissent l'un avec l'autre.
27000 et 7279	TCP	Ports de licence pour la communication entre le serveur de licences NetScaler Console et l'instance NetScaler. Ces ports sont également utilisés pour les licences groupées NetScaler.	NetScaler vers NetScaler Console
5005	UDP	Port pour échanger les signaux de pulsation entre les nœuds HA.	Nœud principal NetScaler Console vers le nœud secondaire. Nœud secondaire NetScaler Console vers le nœud principal.
5140	UDP	Port pour recevoir les données de	De NetScaler vers NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
		télémétrie de NetScaler Gateway.	

Si les instances NetScaler Console et NetScaler n'utilisent pas d'agent pour la communication, ouvrez les ports suivants sur le serveur NetScaler Console :

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
80/443	TCP	Pour la communication NITRO de NetScaler Console vers l'instance NetScaler.	De l'agent NetScaler vers NetScaler et de NetScaler vers l'agent NetScaler
4739	UDP	Pour la communication AppFlow de l'instance NetScaler vers NetScaler Console.	NetScaler vers l'agent NetScaler
162	UDP	Pour recevoir les événements SNMP de l'instance NetScaler vers NetScaler Console.	NetScaler vers l'agent NetScaler
514	UDP	Pour recevoir les messages syslog de l'instance NetScaler vers NetScaler Console.	NetScaler vers l'agent NetScaler
5557/5558	TCP	Pour la communication de flux de journaux (pour les violations de sécurité WAF, Web Insight et HDX	NetScaler vers NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
		Insight) de NetScaler vers NetScaler Console.	
5563	TCP	Pour recevoir les métriques NetScaler (compteurs), les événements système et les messages du journal d'audit d'une instance NetScaler vers NetScaler Console	De NetScaler vers NetScaler Console

Ports pour l'agent

Le tableau suivant explique les ports requis qui doivent être ouverts sur l'agent.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
80/443	TCP	Pour la communication NITRO de NetScaler Console vers l'instance NetScaler.	De l'agent NetScaler vers NetScaler et de NetScaler vers l'agent NetScaler
4739	UDP	Pour la communication AppFlow de l'instance NetScaler vers NetScaler Console.	NetScaler vers l'agent NetScaler
162	UDP	Pour recevoir les événements SNMP de l'instance NetScaler vers NetScaler Console.	NetScaler vers l'agent NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
514	UDP	Pour recevoir les messages syslog de l'instance NetScaler vers NetScaler Console.	NetScaler vers l'agent NetScaler
5557/5558	TCP	Pour la communication de flux de journaux (pour les violations de sécurité WAF, Web Insight et HDX Insight) de NetScaler vers NetScaler Console.	NetScaler vers NetScaler Console

Ports pour les instances NetScaler

Le tableau suivant explique les ports requis qui doivent être ouverts sur les instances NetScaler.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
80/443	TCP	Pour la communication NITRO de NetScaler Console vers l'instance NetScaler. Pour la communication NITRO entre les serveurs NetScaler Console en mode haute disponibilité.	De NetScaler Console vers NetScaler et de NetScaler vers NetScaler Console
22	TCP	Pour la communication SSH de NetScaler Console vers l'instance NetScaler.	De NetScaler Console vers NetScaler. Ou, de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
		Pour la synchronisation entre les serveurs NetScaler Console déployés en mode haute disponibilité. Et, ce port est requis pour la communication SSH entre l'agent NetScaler Console et NetScaler.	l'agent NetScaler vers NetScaler.
Aucun port réservé	ICMP	Pour détecter l'accessibilité réseau entre NetScaler Console et les instances NetScaler, ou le serveur NetScaler Console secondaire déployé en mode haute disponibilité.	NetScaler Console vers NetScaler
161	UDP	Pour interroger les événements des instances NetScaler.	NetScaler Console vers NetScaler

Ports pour l'agent intégré NetScaler

Le tableau suivant explique les ports requis qui doivent être ouverts pour un agent intégré NetScaler.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
443	TCP	Pour toutes les communications de NetScaler Console	NetScaler Console vers l'agent intégré NetScaler et agent intégré NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
		vers l'agent intégré NetScaler	vers NetScaler Console

REMARQUE :

Dans un déploiement NetScaler Console à haute disponibilité, toutes les communications de NetScaler Console utilisent l'adresse IP du nœud principal.

Ports pour les serveurs externes

Le tableau suivant explique les ports requis qui doivent être ouverts sur les serveurs externes :

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
25	TCP	Pour envoyer des notifications SMTP depuis NetScaler Console aux utilisateurs.	NetScaler Console vers les utilisateurs.
389/636	TCP	Port par défaut pour le protocole d'authentification. Pour la communication entre NetScaler Console et le serveur d'authentification externe LDAP.	NetScaler Console vers le serveur d'authentification externe LDAP
123	UDP	Port de serveur NTP par défaut pour la synchronisation avec plusieurs sources de temps.	NetScaler Console vers le serveur NTP
1812	RADIUS	Port par défaut pour le protocole	NetScaler Console vers le serveur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYPE	DÉTAILS	SENS DE LA COMMUNICATION
		d'authentification. Pour la communication entre NetScaler Console et le serveur d'authentification externe RADIUS.	d'authentification externe RADIUS
49	TACACS	Port par défaut pour le protocole d'authentification. Pour la communication entre NetScaler Console et le serveur d'authentification externe TACACS.	NetScaler Console vers le serveur d'authentification externe TACACS

Limitations

À partir de NetScaler ADM 12.1 ou version ultérieure, le format IPv6 des adresses IP est pris en charge. Pour configurer IPv6, accédez à **Paramètres > Administration**, sélectionnez **Adresse IP, deuxième carte réseau, nom d'hôte et serveur proxy** sous **Configurations réseau**, activez **IPv6**, fournissez les détails de configuration IPv6, puis cliquez sur **Enregistrer**.

Le tableau suivant décrit la liste des fonctionnalités prises en charge et non prises en charge pour IPv6 :

FONCTIONNALITÉS IPV6 PRISES EN CHARGE	FONCTIONNALITÉS IPV6 NON PRISES EN CHARGE
Accès de gestion pour l'interface graphique de NetScaler ADM	IP flottante haute disponibilité
Accès de gestion pour NetScaler	Syslogs reçus des ADC qui prennent en charge IPv6
Enregistrement et inventaire	StyleBooks sur les ADC qui prennent en charge IPv6

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS IPV6 PRISES EN CHARGE	FONCTIONNALITÉS IPV6 NON PRISES EN CHARGE
Tableau de bord réseau	Analyses
Tableau de bord SSL	Licences en pool
Tâches de configuration	
Audit de configuration	
Fonctions réseau	
Rapports réseau	
Sauvegarde et restauration des instances ADC	
Événements SNMP des instances NetScaler	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Démarrage

Ce document vous explique comment démarrer le déploiement et la configuration de NetScaler Console sur site pour la première fois. Ce document est destiné aux administrateurs réseau et d'applications qui gèrent les périphériques réseau Citrix (NetScaler et NetScaler Gateway). Suivez les étapes de ce document quel que soit le type de périphérique que vous prévoyez de gérer à l'aide de NetScaler Console.

Si vous êtes un utilisateur existant de NetScaler Console, il est recommandé de consulter les notes de publication, les exigences système et les détails de la licence avant de mettre à niveau votre serveur vers la dernière version de NetScaler Console.

Étape 1 - Examiner les exigences système

Avant de commencer à déployer NetScaler Console dans votre centre de données, examinez les exigences logicielles, les exigences de navigateur, les informations de port, les informations de licence et les limitations.

- **Informations sur les licences**. Vous pouvez ajouter un nombre illimité d'instances et d'entités sans licence. Cependant, vous ne pouvez afficher les informations d'analyse que pour deux serveurs virtuels sans appliquer de licence. Pour afficher les analyses pour plus de deux serveurs virtuels, vous devez acheter les licences appropriées. En savoir plus.
- **Exigences du système d'exploitation et du récepteur**. Examinez ces informations pour vous assurer que vous disposez de la version correcte du récepteur pour les systèmes d'exploitation pris en charge. En savoir plus.
- **Exigences du navigateur**. Pour accéder à l'interface graphique de NetScaler Console, vous devez vous assurer que vous disposez du navigateur requis et de la version correcte. En savoir plus.
- **Ports**. Assurez-vous que les ports requis sont ouverts pour que NetScaler Console puisse communiquer avec les instances NetScaler. En savoir plus.
- **Exigences des instances NetScaler**. Différentes fonctionnalités de NetScaler Console sont prises en charge sur différentes versions logicielles de NetScaler. Examinez ces informations pour vous assurer que vous avez mis à niveau vos instances NetScaler vers la version correcte. En savoir plus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 2 - Déployer NetScaler Console

Pour gérer et surveiller les applications et l'infrastructure réseau, vous devez d'abord installer NetScaler Console sur l'un des hyperviseurs. Vous pouvez déployer NetScaler Console en tant que serveur unique ou en mode haute disponibilité. Si vous utilisez NetScaler Insight Center, vous pouvez migrer vers NetScaler Console et bénéficier des fonctionnalités de gestion, de surveillance, d'orchestration et de gestion des applications en plus des fonctionnalités d'analyse.

- **Déploiement sur un seul serveur**. Dans un déploiement NetScaler Console sur un seul serveur, la base de données est intégrée au serveur et un seul serveur traite tout le trafic. Vous pouvez déployer NetScaler Console avec Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM. Voir :
  - NetScaler Console avec Citrix Hypervisor
  - NetScaler Console avec Microsoft Hyper-V
  - NetScaler Console avec VMware ESXi
  - NetScaler Console avec serveur Linux KVM
- **Déploiement haute disponibilité.** Un déploiement haute disponibilité (HA) de deux serveurs NetScaler Console assure des opérations ininterrompues. Dans une configuration haute disponibilité, les deux nœuds NetScaler Console doivent être déployés en mode actif-passif, sur le même sous-réseau, en utilisant la même version et build logicielle, et doivent avoir les mêmes configurations. Avec le déploiement HA, la possibilité de configurer l'adresse IP flottante sur le nœud principal de NetScaler Console élimine le besoin d'un équilibreur de charge NetScaler séparé. Pour en savoir plus, consultez [Configurer en déploiement haute disponibilité.

  ```
  ](deploy/high-availability-deployment.md)
  ```

Étape 3 - Ajouter des instances à NetScaler Console

Dans NetScaler Console, vous pouvez découvrir, gérer et surveiller toutes les instances NetScaler déployées sur site ou dans le cloud. Vous devez ajouter des instances au serveur NetScaler Console si vous souhaitez gérer et surveiller ces instances. Vous pouvez ajouter les instances suivantes à NetScaler Console :

- NetScaler
  - NetScaler MPX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

Lorsque vous ajoutez une instance au serveur NetScaler Console, le serveur communique implicitement avec les instances et collecte un inventaire de ces instances.

En savoir plus

Étape 4 - Activer l'analyse sur les serveurs virtuels

Pour afficher les données d'analyse du flux de trafic de votre application, vous devez activer la fonctionnalité Analytics sur les serveurs virtuels qui reçoivent le trafic pour les applications spécifiques.

En savoir plus

Étape 5 - Configurer le serveur NTP sur NetScaler Console

Vous devez configurer un serveur NTP (Network Time Protocol) dans NetScaler Console pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge de NetScaler Console a les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

En savoir plus

Étape 6 - Configurer les paramètres système pour des performances optimales de NetScaler Console

Avant de commencer à utiliser NetScaler Console pour gérer et surveiller vos instances et applications, il est recommandé de configurer quelques paramètres système qui garantissent des performances optimales de votre serveur NetScaler Console.

- **Configurer les alarmes système.** Configurez les alarmes système pour vous assurer d'être informé de tout problème système critique ou majeur. Par exemple, vous pourriez vouloir être averti si l'utilisation du CPU est élevée ou s'il y a plusieurs échecs de connexion au serveur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Configurer les notifications système**. Vous pouvez envoyer des notifications à des groupes d'utilisateurs sélectionnés pour diverses fonctions liées au système. Vous pouvez configurer un serveur de notification dans NetScaler Console, et vous pouvez configurer des serveurs de passerelle de messagerie électronique et de service de messages courts (SMS) pour envoyer des notifications par e-mail et par SMS aux utilisateurs. Cela garantit que vous êtes informé de toute activité au niveau du système, telle que la connexion d'un utilisateur ou le redémarrage du système.
- **Configurer les paramètres d'élagage du système**. Pour limiter la quantité de données de rapport stockées dans la base de données de votre serveur NetScaler Console, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont élaguées toutes les 24 heures (à 00h00).
- **Configurer les paramètres de sauvegarde du système**. NetScaler Console sauvegarde automatiquement le système tous les jours à 00h30. Par défaut, il enregistre trois fichiers de sauvegarde. Vous pourriez vouloir conserver un plus grand nombre de sauvegardes du système.
- **Configurer les paramètres de sauvegarde d'instance**. Si vous sauvegardez l'état actuel d'une instance NetScaler, vous pouvez utiliser les fichiers de sauvegarde pour restaurer la stabilité au cas où l'instance deviendrait instable. Cela est particulièrement important avant d'effectuer une mise à niveau. Par défaut, une sauvegarde est effectuée toutes les 12 heures et trois fichiers de sauvegarde sont conservés dans le système.
- **Configurer les paramètres d'élagage des événements d'instance**. Pour limiter la quantité de données de messages d'événements stockées dans la base de données de votre serveur NetScaler Console, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont élaguées toutes les 24 heures (à 00h00).
- **Configurer les paramètres de purge des journaux système d'instance**. Pour limiter la quantité de données de journaux système stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez purger les données de journaux système. Vous pouvez spécifier le nombre de jours après lesquels les données de journaux système suivantes seront supprimées de NetScaler Console :
  - Données Syslog génériques
  - Données AppFirewall
  - Données NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

En savoir plus

Prochaines étapes

Après avoir déployé et configuré NetScaler Console, vous pouvez commencer à gérer et à surveiller vos instances et applications.

Gestion des instances et applications NetScaler. Toutes les fonctionnalités de NetScaler Console sont prises en charge sur les instances NetScaler. Vous pouvez commencer à utiliser n'importe laquelle de ces fonctionnalités.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Interface utilisateur graphique améliorée

L'interface utilisateur graphique (GUI) de NetScaler Console offre une expérience enrichissante grâce à plusieurs fonctionnalités clés. Ces fonctionnalités offrent :

- **Espace d'écran optimisé :** Les utilisateurs peuvent afficher ou masquer la barre latérale selon leurs préférences.
- **Accès rapide aux favoris :** Épinglez les éléments de menu fréquemment utilisés pour une navigation plus rapide.
- **Visibilité améliorée des sous-menus :** Passez la souris sur les éléments de menu pour révéler les sous-menus, offrant une vue plus claire de toutes les options disponibles.
- **Structure de sous-menu améliorée :** Un système de sous-menu cohérent à trois niveaux assure une navigation fluide dans NetScaler Console, offrant une expérience uniforme partout.

Cette page vous présente les fonctionnalités de l'interface utilisateur graphique de NetScaler Console, offrant une expérience utilisateur enrichissante.

Menu Afficher au survol

Auparavant, le sous-menu de deuxième niveau était affiché sous forme d'arborescence. L'interface utilisateur graphique de NetScaler Console offre une navigation fluide où le menu secondaire apparaît au survol, révélant le sous-menu. Cette navigation améliore l'expérience de visualisation en affichant toutes les options du sous-menu sans avoir besoin de faire défiler.



Hiérarchie de menu simplifiée

La hiérarchie des menus est simplifiée à un maximum de trois niveaux. Les sous-menus qui étaient auparavant affichés au-delà du troisième niveau sont maintenant positionnés au troisième niveau. La navigation est mise à jour pour les éléments suivants :

- **Infrastructure > Configuration**
- **Licences NetScaler® > Licences en pool**
- **Gateway > HDX™ Insight**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Libellés de sous-menu mis à jour

Les noms de certains sous-menus sont modifiés pour s'aligner sur cette approche de navigation. Les modifications de navigation d'écran et les mises à jour des libellés de sous-menu sont les suivantes :

Infrastructure > Configuration

NAVIGATION D'ÉCRAN PRÉCÉDENTE	NAVIGATION D'ÉCRAN MODIFIÉE	Y A-T-IL UN CHANGEMENT DANS LE LIBELLÉ DU SOUS-MENU ?
Configuration > Tâches de configuration > Tâches	**Configuration > Tâches de configuration**	Oui
Configuration > Tâches de configuration > Modèles de configuration	**Configuration > Modèles de configuration**	Non
Configuration > Audit de configuration > Vue d'ensemble	**Configuration > Audit de configuration**	Oui
Configuration > Audit de configuration > Modèles d'audit	**Configuration > Modèles d'audit**	Non
Configuration > Audit de configuration > Conseils de configuration	**Configuration > Conseils de configuration**	Non

Licences NetScaler > Licences en pool

NAVIGATION D'ÉCRAN PRÉCÉDENTE	NAVIGATION D'ÉCRAN MODIFIÉE	Y A-T-IL UN CHANGEMENT DANS L'ÉTIQUETTE DU SOUS-MENU ?
Licences en pool > Licences de capacité de débit > Capacité de débit	**Licences en pool > Capacité de débit**	Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAVIGATION D'ÉCRAN PRÉCÉDENTE	NAVIGATION D'ÉCRAN MODIFIÉE	Y A-T-IL UN CHANGEMENT DANS L'ÉTIQUETTE DU SOUS-MENU ?
Licences en pool > Licences de capacité de débit > Licences CPX	**Licences en pool > Licences CPX**	Non
Licences en pool > Licences de capacité de débit > CICO	**Licences en pool > CICO**	Non
Licences en pool > Licences de capacité de débit > Instances FIPS	**Licences en pool > Instances FIPS**	Non
Licences en pool > Autogéré > Informations d'expiration de licence	**Licences en pool > Informations d'expiration autogérées**	Oui
Licences en pool > Autogéré > Licences de capacité de débit > Pool autogéré	**Licences en pool > Débit autogéré**	Oui
Licences en pool > Géré par soi-même > VCPU géré par soi-même	**Licences en pool > VCPU géré par soi-même**	Non

Passerelle > HDX Insight

NAVIGATION D'ÉCRAN PRÉCÉDENTE	NAVIGATION D'ÉCRAN MODIFIÉE	Y A-T-IL UN CHANGEMENT DANS L'ÉTIQUETTE DU SOUS-MENU ?
HDX Insight > Licences > Licences SSL VPN	**HDX Insight > Licences**	Oui

Paramètres

Il n'y a pas d'autres modifications sous **Paramètres**, à l'exception de la modification de l'étiquette ou du nom du sous-menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAVIGATION D'ÉCRAN PRÉCÉDENTE	NAVIGATION D'ÉCRAN MODIFIÉE	Y A-T-IL UN CHANGEMENT DANS L'ÉTIQUETTE DU SOUS-MENU ?
Paramètres > Gestion du stockage des données	Il n'y a aucun changement dans la navigation de l'écran.	L'étiquette du sous-menu est remplacée par **Paramètres > Stockage des données**

Menu réductible

Vous pouvez réduire ou développer l'intégralité du menu en cliquant sur une icône.

Menu développé

Cliquez sur l'icône **>>** dans le volet pour développer l'intégralité du menu.



Menu réduit

Cliquez sur **Réduire <<** dans le volet pour réduire l'intégralité du menu.



Basculement de la barre latérale

Vous pouvez optimiser l'espace de l'écran en basculant la visibilité de la barre latérale. Cliquez sur le bouton de basculement dans le fil d'Ariane pour masquer ou afficher la barre latérale.

Afficher la barre latérale



Masquer la barre latérale

Cette option optimise l'espace de l'écran en masquant la barre latérale.



Définir comme écran d'accueil

L'interface graphique de NetScaler Console affiche une icône à côté du nom d'un sous-menu qui est affiché comme une page. L'icône de l'écran d'accueil vous permet de définir votre page de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

destination. Elle n'apparaît que lorsque vous êtes sur cette page spécifique. Pour supprimer la page de la page d'accueil, cliquez simplement à nouveau sur l'icône.



Épingler les éléments favoris

La fonctionnalité **Épingler** offre un accès plus rapide à vos éléments favoris. Pour épingler un menu ou un sous-menu, survolez-le et cliquez sur l'icône d'épingle qui apparaît à côté de son nom.



Les menus épinglés sont affichés sous **ÉPINGLÉS** dans la barre latérale, ce qui les rend facilement accessibles.



Migrer vers le service

L'option **Migrer vers le service** est désormais disponible en tant que sous-menu du **Centre d'aide**. Auparavant, cette option était disponible dans le volet de navigation. Cela rationalise les options disponibles sous les éléments de menu appropriés.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Déployer

Avant d'utiliser NetScaler Console pour gérer et surveiller vos applications et votre infrastructure réseau, vous devez d'abord l'installer sur l'un des hyperviseurs ou sur un cluster Kubernetes. Si vous déployez NetScaler Console sur un hyperviseur, vous pouvez le déployer en tant que serveur unique ou en mode haute disponibilité. Le mode haute disponibilité n'est pas applicable sur un cluster Kubernetes. Si vous utilisez NetScaler Insight Center, vous pouvez migrer vers NetScaler Console et bénéficier des fonctionnalités de gestion, de surveillance, d'orchestration et de gestion des applications en plus des fonctionnalités d'analyse.

- **Déploiement sur un seul serveur** : Pour une NetScaler Console autonome déployée sur un hyperviseur, la base de données est intégrée au serveur et un seul serveur traite tout le trafic. Vous pouvez déployer NetScaler Console avec Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM. Voir :
  - NetScaler Console sur Citrix Hypervisor
  - NetScaler Console sur Microsoft Hyper-V
  - NetScaler Console sur Azure
  - NetScaler Console sur VMware ESXi
  - NetScaler Console sur un serveur Linux KVM
  - NetScaler Console sur hyperviseur Nutanix (Acropolis)
  - NetScaler Console sur cluster Kubernetes
- **Déploiement en haute disponibilité (HA)** : Un déploiement HA de deux serveurs NetScaler Console assure des opérations ininterrompues. Dans une configuration HA, les deux nœuds NetScaler Console doivent être déployés en mode actif-passif, sur le même sous-réseau, en utilisant la même version logicielle et la même build, et doivent avoir les mêmes configurations. Avec le déploiement HA, la possibilité de configurer l'adresse IP flottante sur le nœud principal de NetScaler Console élimine le besoin d'un équilibreur de charge NetScaler séparé. Voir : Configurer en déploiement haute disponibilité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

La haute disponibilité n'est pas applicable pour NetScaler Console déployée sur un cluster Kubernetes.

- **Déploiement léger** : Si vous prévoyez d'utiliser NetScaler Console uniquement pour Licences groupées ou flexibles, vous pouvez le déployer avec des spécifications inférieures. Pour plus d'informations, consultez Prérequis.
- **Migrer de NetScaler Insight Center vers NetScaler Console** : Vous pouvez migrer votre déploiement NetScaler Insight Center vers NetScaler Console sans perdre la configuration, les paramètres ou les données existants. Avec NetScaler Console, vous pouvez non seulement visualiser les différentes analyses générées par NetScaler, mais aussi gérer, surveiller et dépanner l'ensemble de l'infrastructure de livraison d'applications globale à partir d'une console unique et unifiée. Voir : Migration de NetScaler Insight Center vers NetScaler Console
- **Intégrer NetScaler Console avec Director** : Director s'intègre à NetScaler Console pour l'analyse réseau et la gestion des performances. Voir : Intégrer NetScaler Console avec Director

Conditions préalables à l'installation de NetScaler Console

Vous pouvez télécharger et installer NetScaler Console pour Microsoft HyperV, VMware ESXi, Linux KVM et les plateformes Citrix Hypervisor™ en tant qu'appliance virtuelle. Avant d'installer NetScaler Console, vous devez comprendre les exigences logicielles, les exigences du navigateur, les informations de port, les informations de licence et les limitations sur toutes ces plateformes.

Pour connaître les exigences spécifiques à la plateforme et les étapes détaillées d'installation de NetScaler Console, consultez les rubriques suivantes :

- NetScaler Console avec Citrix Hypervisor
- NetScaler Console avec Microsoft HyperV
- NetScaler Console avec VMware ESXi
- NetScaler Console avec un serveur Linux KVM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exigences générales pour NetScaler Console

COMPOSANT	EXIGENCE
RAM	32 Go
Processeur virtuel	8 processeurs
Espace de stockage	Citrix recommande d'utiliser la technologie Solid State Drive (SSD) pour les déploiements NetScaler Console.
	L'espace de stockage par défaut requis est de 120 Go. L'exigence de stockage réelle dépend de l'estimation du dimensionnement de NetScaler Console.
	Si votre exigence de stockage NetScaler Console dépasse 120 Go, vous devez attacher un disque supplémentaire.
	Citrix vous recommande d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial. Vous ne pouvez ajouter qu'un seul disque supplémentaire.
	Pour plus d'informations, consultez Comment attacher un disque supplémentaire à NetScaler Console.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

NetScaler® Console léger uniquement pour les licences groupées ou flexibles

Vous pouvez utiliser NetScaler Console uniquement pour les licences groupées ou flexibles avec des spécifications inférieures :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANT	EXIGENCE
RAM	8 Go
Processeur virtuel	4
Stockage	120 Go

REMARQUE :

Citrix vous recommande d'héberger le VHD de NetScaler Console sur un stockage local. Lorsqu'il est hébergé sur des périphériques de stockage dans un SAN, NetScaler Console pourrait ne pas fonctionner comme prévu. Par conséquent, le déploiement de NetScaler Console sur un SAN n'est pas pris en charge.

NetScaler Console sur Citrix Hypervisor

Pour installer NetScaler Console sur Citrix Hypervisor (anciennement connu sous le nom de XenServer), vous devez d'abord télécharger le fichier image .xva de NetScaler Console sur votre ordinateur local. Vous devez utiliser Citrix XenCenter pour effectuer l'installation de NetScaler Console.

REMARQUE :

NetScaler Console ne prend pas en charge XenMotion.

Prérequis

Avant d'installer NetScaler Console, vérifiez que les exigences suivantes sont remplies :

- Citrix Hypervisor version 7.1 ou ultérieure est installé sur du matériel qui répond aux exigences minimales.
- XenCenter est installé sur un poste de travail de gestion qui répond aux exigences minimales. Vous devez utiliser XenCenter pour installer NetScaler Console sur Citrix Hypervisor.
- Vous avez téléchargé le fichier image .XVA de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration système requise pour XenCenter®

XenCenter est une application cliente Windows. Elle ne peut pas s'exécuter sur la même machine que l'hôte Citrix Hypervisor™. Le tableau suivant décrit la configuration système minimale requise.

COMPOSANT	EXIGENCE
Système d'exploitation	Windows 7, Windows Server 2003 ou Windows 10
Cadre .NET	Version 2.0 ou ultérieure
Processeur	750 MHz (MHz), Recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte réseau	Carte réseau de 100 mégabits par seconde (Mbps) ou plus rapide

Installer NetScaler® Application Delivery Management

1. Importez le fichier image XVA dans votre Citrix Hypervisor, et depuis l'onglet **Console**, configurez les options de configuration réseau initiales.

   

2. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
3. Lorsque vous y êtes invité, connectez-vous à l'aide des informations d'identification nsrecover/nsroot.

   

   REMARQUE

   Après vous être connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

4. Exécutez le script de déploiement en tapant la commande à l'invite du shell : `/mps/deployment_type.py`

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Sélectionnez le type de déploiement comme **Serveur NetScaler Console**. Si vous ne sélectionnez aucune option, par défaut, il est déployé en tant que serveur.

   

6. Tapez **Oui** pour déployer NetScaler Console en tant que déploiement autonome.
7. Tapez **Oui** pour redémarrer le serveur NetScaler Console.

REMARQUE

Après avoir installé NetScaler Console, vous pouvez mettre à jour les paramètres de configuration initiale ultérieurement.

Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface graphique en tapant l'adresse IP du serveur NetScaler Console dans le navigateur web. Les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration de NetScaler Console.

NetScaler Console sur Microsoft Hyper-V

Pour installer NetScaler Console sur Microsoft Hyper-V, vous devez d'abord télécharger le fichier image NetScaler Console sur votre ordinateur local. Assurez-vous également que votre système dispose des extensions de virtualisation matérielle et vérifiez que les extensions de virtualisation du processeur sont disponibles.

Prérequis

Avant d'installer l'appliance virtuelle NetScaler Console, vérifiez que les exigences suivantes sont remplies :

- Microsoft Hyper-V version 6.2 ou ultérieure est installé sur un matériel qui répond aux exigences minimales.
- Installez Microsoft Hyper-V Manager sur un poste de travail de gestion qui répond aux exigences minimales du système.
- Vous avez téléchargé le fichier image NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exigences système de Microsoft Hyper-V

Microsoft Hyper-V est une application cliente Windows. Le tableau suivant décrit les exigences minimales du système.

COMPOSANT	EXIGENCE
Système d'exploitation	Windows Server 2012 R2
Framework .NET	Version 2.0 ou ultérieure
Processeur	750 MHz (MHz), Recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte réseau	Carte réseau de 100 mégabits par seconde (Mbps) ou plus rapide

Installation de NetScaler® Application Delivery Management

Le nombre de serveurs NetScaler Console que vous pouvez installer dépend de la mémoire disponible sur le serveur Hyper-V.

Pour installer NetScaler Console :

1. Démarrez le client Gestionnaire Hyper-V sur votre poste de travail.
2. Dans le menu **Action**, cliquez sur **Importer une machine virtuelle**.

   
3. Importez l'image Hyper-V, puis effectuez les opérations suivantes :

   a. Dans la boîte de dialogue Importer une machine virtuelle, dans la section **Localiser le dossier**, accédez au dossier dans lequel vous avez enregistré l'image Hyper-V de NetScaler Console, sélectionnez le dossier, puis cliquez sur **Suivant**.

   b. Dans la section Sélectionner une machine virtuelle, sélectionnez le nom de machine virtuelle approprié.

   c. Dans la section **Choisir le type d'importation**, sélectionnez l'option Copier la machine virtuelle (créer un nouvel ID unique) et cliquez sur Suivant.

   d. Dans la section **Choisir la destination**, vous pouvez spécifier les dossiers pour stocker les fichiers de la machine virtuelle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Par défaut, l'assistant importe les fichiers de la machine virtuelle vers les dossiers Hyper-V par défaut sur votre hôte local.

e. Dans la section **Choisir les dossiers de stockage**, vous pouvez sélectionner l'emplacement où vous souhaitez stocker les disques durs virtuels, puis cliquez sur **Suivant**.

f. Vous pouvez vérifier les détails de la machine virtuelle dans le volet de résumé, cliquez sur **Terminer**.

L'image NetScaler Console Hyper-V s'affiche dans le volet de droite.

4. Cliquez avec le bouton droit sur l'image NetScaler Console Hyper-V, puis cliquez sur **Paramètres**.
5. Dans le volet gauche de la boîte de dialogue qui apparaît, accédez à **Matériel** \> **Adaptateur réseau VM_Bus**, et dans le volet droit, dans la liste Réseau, sélectionnez le réseau approprié.
6. Cliquez sur **Appliquer**, puis cliquez sur **OK**.
7. Cliquez avec le bouton droit sur l'image NetScaler Console Hyper-V et cliquez sur **Connecter**.
8. Dans la fenêtre de la console, cliquez sur le bouton **Démarrer**.
9. Configurez les options de configuration réseau initiales.

   Configuration initiale(/en-us/netscaler-application-delivery-management-software/media/admha-initialconfig.png)
10. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
11. Lorsque vous y êtes invité, connectez-vous à l'aide des informations d'identification nsrecover/nsroot.

    Configuration initiale(/en-us/netscaler-application-delivery-management-software/media/nmas-deployment-changes.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Après vous être connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

12. Exécutez le script de déploiement en tapant la commande à l'invite de shell :

```
deployment_type.py
```

Configuration initiale(/en-us/netscaler-application-delivery-management-software/media/ha-deploymenttype.png)

13. Sélectionnez le type de déploiement comme **Serveur NetScaler Console**. Si vous ne sélectionnez aucune option, il est déployé par défaut en tant que serveur.

Configuration initiale(/en-us/netscaler-application-delivery-management-software/media/ha-deploymentconfig.png)

14. Tapez **Oui** pour déployer NetScaler Console en tant que déploiement autonome.
15. Tapez **Oui** pour redémarrer le serveur NetScaler Console.

REMARQUE

Après avoir installé NetScaler Console, vous pouvez mettre à jour les paramètres de configuration initiaux ultérieurement.

Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface graphique en saisissant l'adresse IP du serveur NetScaler Console dans la barre d'adresse de votre navigateur. Les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration de NetScaler Console.

NetScaler Console sur VMware ESXi

Ce document décrit comment installer les appliances virtuelles NetScaler Console sur VMware ESXi, à l'aide du client VMware vSphere.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prérequis

Avant de commencer l'installation d'une appliance virtuelle, vérifiez les exigences suivantes :

- Installez une version prise en charge de VMware ESXi. Pour la liste des versions prises en charge, consultez Hyperviseurs pris en charge.
- Installez VMware Client sur un poste de travail de gestion qui répond aux exigences minimales du système.
- Téléchargez les fichiers d'installation de NetScaler Console.

Remarque

- VMotion est pris en charge uniquement à partir de **NetScaler Console 13.0 Build 47.22 ou version ultérieure**. Vous pouvez planifier et automatiser la migration du serveur NetScaler Console déployé sur un hyperviseur ESXi, y compris les configurations vSphere haute disponibilité et vSphere DRS.
- Les VMware Tools pour NetScaler Console sont livrés dans le cadre de la version logicielle et ne peuvent pas être mis à niveau ou modifiés séparément.

Pour installer NetScaler Console

Suivez ces étapes pour installer une appliance virtuelle NetScaler Console sur VMware ESXi.

REMARQUE

Les étapes et les captures d'écran sont basées sur VMware ESXi version 6.0. L'interface graphique peut différer dans d'autres versions d'ESXi. La version VMware ESXi 7.0.1c numéro de build 17325551 avec l'adaptateur VMXNET3 est prise en charge dans **NetScaler Console 13.0 71.40 ou version ultérieure**. Reportez-vous à la documentation VMware pour les étapes spécifiques à la version.

1. Démarrez le client VMware vSphere sur votre poste de travail.
2. Dans la zone de texte **Adresse IP / Nom**, saisissez l'adresse IP du serveur VMware ESXi auquel vous souhaitez vous connecter.
3. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Dans la boîte de dialogue **Déployer le modèle OVF**, sous **Déployer à partir d'un fichier ou d'une URL**, sélectionnez le fichier .ovf, puis cliquez sur **Suivant**.

   REMARQUE

   Si un message d'avertissement apparaît avec le texte suivant : « L'identifiant du système d'exploitation n'est pas pris en charge sur l'hôte sélectionné, vérifiez si le serveur VMware prend en charge le système d'exploitation FreeBSD. » Cliquez sur **Oui**.

6. Sur la page **Détails du modèle OVF**, cliquez sur **Suivant**.
7. Saisissez un nom pour l'appliance virtuelle NetScaler Console, puis cliquez sur **Suivant**.
8. Spécifiez le format de disque en sélectionnant soit le format provisionné de manière dynamique (Thin provisioned format) soit le format provisionné de manière statique (Thick provisioned format).

   REMARQUE

   Nous vous recommandons de sélectionner le **format provisionné de manière statique**.

9. Cliquez sur **Terminer** pour démarrer le processus d'installation.

   

10. Vous êtes maintenant prêt à démarrer l'appliance virtuelle NetScaler Console.
11. Dans le volet de navigation, sélectionnez l'appliance virtuelle que vous avez installée. Dans le menu **Inventaire**, cliquez avec le bouton droit sur la **Machine virtuelle**, puis cliquez sur **Mettre à niveau le matériel virtuel**. Dans la boîte de dialogue **Confirmer la machine virtuelle**, cliquez sur **Oui**.

    

12. Dans le menu **Inventaire**, cliquez sur **Machine virtuelle**, puis sur **Modifier les paramètres**.
13. Dans la boîte de dialogue **Propriétés de la machine virtuelle**, sous l'onglet **Matériel**, cliquez sur **Mémoire**, puis dans le volet de droite, spécifiez la **taille de la mémoire** à 32 Go.
14. Cliquez sur **Processeurs**, puis dans le volet de droite, spécifiez les processeurs à 8. Cliquez sur **OK**.
15. Ajoutez un disque supplémentaire selon vos besoins.

    

© 1997–2026 Citrix Systems, Inc. All rights reserved.

16. Dans le volet de navigation, sélectionnez l'appliance virtuelle que vous avez installée. Dans le menu **Inventaire**, cliquez sur **Machine virtuelle**, cliquez sur **Alimentation**, puis cliquez sur **Mettre sous tension**.
17. Cliquez sur l'onglet **Console** pour afficher les options de configuration réseau initiale de NetScaler Console.

    
18. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
19. Lorsque vous y êtes invité, connectez-vous à l'aide des informations d'identification nsrecover/nsroot.

    

    REMARQUE

    Après vous être connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.
20. Exécutez le script de déploiement en tapant la commande à l'invite du shell :

    ```
    deployment_type.py
    ```

    
21. Sélectionnez le type de déploiement comme **Serveur NetScaler Console**. Si vous ne sélectionnez aucune option, il est déployé par défaut en tant que serveur.

    
22. Tapez **Oui** pour déployer NetScaler Console en tant que déploiement autonome.
23. Tapez **Oui** pour redémarrer le serveur NetScaler Console.

    REMARQUE

    Après avoir installé NetScaler Console, vous pouvez mettre à jour les paramètres de configuration initiale ultérieurement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface graphique en saisissant l'adresse IP du serveur NetScaler Console dans le navigateur. Les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration de NetScaler Console.

REMARQUE

Le temps d'installation typique de NetScaler Console est d'environ 10 minutes sur VMware ESXi, mais peut être plus long sur certains systèmes.

Automatiser le déploiement de l'agent NetScaler® sur VMware ESXi

NetScaler Console vous permet d'automatiser le déploiement des agents NetScaler sur VMware ESXi.

En tant qu'administrateur, vous pouvez automatiser les actions suivantes :

- Configurer l'agent NetScaler
- Enregistrer l'agent NetScaler et modifier le mot de passe par défaut de l'agent.

Configurer l'agent NetScaler

Pour automatiser la configuration de l'agent, ajoutez les valeurs des paramètres suivants dans le fichier .ovf :

1. `IPAddress`
2. `Netmask`
3. `Gateway`
4. `Nameserver`
5. `Hostname`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Le fichier .ovf est disponible dans le fichier image de l'agent. Pour télécharger le fichier de l'agent NetScaler, accédez à `<https://www.citrix.com/downloads/citrix-application-management/>`. Le modèle de nommage du fichier image de l'agent est le suivant : **MASAGENT-ESX-releasenumber-buildnumber.zip**

Enregistrer l'agent NetScaler et modifier le mot de passe par défaut

REMARQUE :

Avant d'enregistrer et de modifier le mot de passe par défaut, assurez-vous d'avoir ajouté les paramètres spécifiés dans Configurer l'agent NetScaler.

Pour automatiser l'enregistrement de l'agent NetScaler et la modification du mot de passe par défaut, ajoutez les valeurs des paramètres suivants dans le même fichier .ovf :

1. `NetScaler Console Server IP`
2. `NetScaler Console Username`
3. `NetScaler Console Password`
4. `Agent New Password`

Prérequis

Avant de commencer l'installation d'une appliance virtuelle, assurez-vous de :

- Installez VMware vSphere 8.x sur un poste de travail de gestion qui répond aux exigences minimales du système.
- Téléchargez les fichiers d'installation de NetScaler Console.

Comment configurer et enregistrer un agent NetScaler

1. Télécharger et modifier le fichier .OVF
2. Installer l'appliance virtuelle NetScaler Console sur VMware ESXi
3. Vérifier

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 1 : Télécharger et modifier le fichier .OVF

1. Extrayez les fichiers de **MASAGENT-ESX-releasenumber-buildnumber.zip** vers l'emplacement souhaité. Les fichiers suivants sont extraits :
   - fichier .ovf
   - fichier .vmdk
   - fichier .ova
   - fichier .mf
2. Ouvrez le fichier .ovf dans n'importe quel éditeur et ajoutez l'exemple de code `<ProductSection>..</ProductSection>` suivant après la balise `</VirtualHardwareSection>`

```
<ProductSection>

<Info>Information about the installed software</Info>

<Product>Application Delivery management</Product>

<Vendor>Citrix</Vendor>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ip">

<Label>IPAddress</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.netmask">

<Label>Netmask</Label>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.gateway">

<Label>Gateway</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.nameserver">

<Label>Nameserver</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.hostname">

<Label>Hostname</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ServerIP">

<Label>NetScaler Console Server IP</Label>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ServerUname">

<Label>NetScaler Console Username</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

ovf:type="string" ovf:key="eth0.ServerPassword">

<Label>NetScaler Console Password</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

ovf:type="string" ovf:key="eth0.NewPassword">

<Label>Agent New Password</Label>

</Property>



</ProductSection>
```

3. Pour les paramètres que vous souhaitez configurer, ajoutez leurs valeurs correspondantes dans ovf:value="VALUE"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pour configurer l'agent NetScaler, ajoutez les valeurs aux paramètres suivants :
  - `IPAddress`
  - `Netmask`
  - `Gateway`
  - `Nameserver`
  - `Hostname`
- Pour enregistrer et modifier le mot de passe par défaut de l'agent NetScaler, ajoutez les valeurs aux paramètres suivants :
  - `NetScaler Console Server IP`
  - `NetScaler Console Username`
  - `NetScaler Console Password`
  - `Agent New Password`

REMARQUE :

- Vous devez configurer l'agent NetScaler avant d'enregistrer et de modifier le mot de passe par défaut de l'agent.
- Si vous n'enregistrez pas et ne modifiez pas le mot de passe par défaut dans le fichier .ovf, effectuez ces actions manuellement après le déploiement de la VM.



4. Après avoir ajouté les paramètres et leurs valeurs, enregistrez le fichier .ovf.

Étape 2 : Installer l'appliance virtuelle NetScaler Console sur VMware ESXi

1. Connectez-vous au **VMWare vSphere Client** et saisissez les informations d'identification de l'administrateur. Cliquez sur **Login**.



2. Sélectionnez votre serveur ESXi, puis cliquez avec le bouton droit de la souris pour sélectionner **Deploy OVF Template**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Dans la page **Deploy OVF Template** :

   a. **Sélectionner un modèle OVF** : Sélectionnez **Fichier local** et accédez à l'emplacement où vous avez enregistré le fichier .ovf modifié et le fichier .vmdk. Sélectionnez les fichiers et cliquez sur **Ouvrir** pour les télécharger. Cliquez sur **Suivant**.

   b. **Sélectionner un nom et un dossier** : Ajoutez un nom pour l'appliance virtuelle et sélectionnez l'emplacement sur l'ESXi où vous souhaitez déployer la machine virtuelle. Cliquez sur **Suivant**.

   c. **Sélectionner une ressource de calcul** : Sélectionnez une ressource sur laquelle exécuter le modèle après son déploiement. Cliquez sur **Suivant**.

   d. **Vérifier les détails** : Vérifiez les détails du modèle OVF. Cliquez sur **Suivant**.

   e. **Sélectionner le stockage** : Sélectionnez une banque de données pour stocker le modèle OVF. Cliquez sur **Suivant**.

   f. **Sélectionner les réseaux** : Poursuivez avec les paramètres par défaut. Cliquez sur **Suivant**.

   g. **Personnaliser le modèle** : Passez en revue toutes les propriétés du modèle OVF. Tous les paramètres et valeurs que vous avez ajoutés dans le fichier .ovf dans la section Télécharger et modifier le fichier .OVF sont affichés.

   h. **Prêt à terminer** : Pour enregistrer les paramètres et démarrer le processus de déploiement, cliquez sur **Terminer**.

   Attendez que le déploiement soit terminé. Une fois que l'état de l'opération **Déployer le modèle OVF** est terminé à 100 %, votre agent est déployé.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT :

Ne mettez pas sous tension l'appliance virtuelle avant de modifier les paramètres.

4. Cliquez sur la nouvelle appliance virtuelle que vous avez installée et accédez à **Configurer > Paramètres > Options vApp > Modifier**.
5. Dans la fenêtre **Modifier les options vApp**, accédez à **Dans les détails OVF > Transport de l'environnement OVF**, et sélectionnez **VMware Tools**. Cliquez sur **OK**.



6. Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Mettre sous tension**. Alternativement, vous pouvez sélectionner l'onglet **Résumé** de la machine virtuelle et cliquer sur **Mettre sous tension**.



7. Dans l'onglet **Résumé**, sélectionnez **Lancer la console Web**. Dans la fenêtre **Lancer la console**, sélectionnez **Console Web**. Cliquez sur **Lancer**.



8. Dans la console, un message d'enregistrement réussi s'affiche une fois que l'agent NetScaler est enregistré auprès du serveur NetScaler Console. Pour vérifier que l'agent NetScaler a été déployé et que le mot de passe par défaut a été modifié, connectez-vous avec le nom d'utilisateur de l'agent NetScaler et le nouveau mot de passe.



Étape 3 : Vérifier

Pour vérifier que l'agent NetScaler est déployé :

1. Une fois l'agent NetScaler déployé, accédez à l'interface graphique de NetScaler Console en saisissant l'adresse IP du serveur NetScaler Console dans le navigateur.
2. Connectez-vous au serveur avec vos identifiants.
3. Accédez à **Infrastructure > Instances > Agents**. Le nouvel agent déployé s'affiche dans la plateforme ESX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console sur cluster Kubernetes

Avant d'installer les appliances virtuelles NetScaler Console sur un cluster Kubernetes, lisez la section des prérequis.

Prérequis

Assurez-vous que les prérequis suivants sont remplis avant d'installer NetScaler Console.

Cluster Kubernetes

- Le cluster Kubernetes doit être de la version suivante ou supérieure :
  - Version du serveur v1.20
  - Version du client v1.20

  Saisissez la commande `kubectl version` pour vérifier la version.
- L'application Helm installée sur le cluster doit avoir la version client v3.4.0 ou supérieure.

  Utilisez la commande `helm version` pour vérifier la version.
- L'interface réseau de conteneur (CNI) du cluster Kubernetes doit être Calico version v3.21.1 ou supérieure.
- Tous les nœuds subordonnés du cluster doivent avoir un client NFS installé. En effet, l'application NetScaler Console persiste les données et la configuration sur des volumes montés sur un serveur de fichiers réseau. Pour installer un client NFS sur un subordonné basé sur Ubuntu, saisissez les commandes suivantes :

`apt-get update` `apt install nfs-common`

- L'application NetScaler Console nécessite 32 Go de mémoire et 8 vCPU sur l'ensemble du cluster, ainsi que 120 Go d'espace sur NFS.

Partage NFS

L'application NetScaler Console a besoin de volumes persistants pour stocker des données telles que la configuration, les certificats, les images et autres. À cette fin, NetScaler Console nécessite des montages NFS. L'application nécessite deux dossiers provenant des montages réseau partagés :

- Un pour stocker des fichiers tels que des certificats, des images et autres
- L'autre pour la base de données

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque

> Il est recommandé d'avoir un NFS avec un SSD.

Ces deux dossiers peuvent être différents ou identiques. Les deux dossiers doivent avoir les permissions 777. Le premier dossier doit avoir un espace minimum de 10 Go. La taille du second dossier dépend de la quantité de données qui doivent être persistantes dans la base de données. La taille minimale est de 100 Go. Pour l'environnement de production, nous recommandons d'utiliser une solution NFS de qualité production.

Appliance NetScaler

L'appliance NetScaler est requise comme périphérique d'entrée (ingress). NetScaler rend les services d'application requis disponibles en dehors du cluster Kubernetes. L'appliance NetScaler doit être en dehors du cluster Kubernetes, et les nœuds de travail doivent être accessibles depuis NetScaler. Effectuez les étapes suivantes :

- Configurez une SNIP sur le NetScaler. NetScaler utilise cette SNIP pour atteindre les nœuds de travail du cluster Kubernetes.
- Identifiez une adresse IP libre à utiliser comme adresse IP de serveur virtuel pour rendre les services d'application requis disponibles en dehors du cluster Kubernetes.

Installer NetScaler Console sur un cluster Kubernetes

Suivez ces étapes pour installer une appliance NetScaler Console sur un cluster Kubernetes :

1. Accédez au site NetScaler et téléchargez le fichier du Helm Chart NetScaler Console pour Kubernetes.
2. Extrayez l'archive Helm Chart téléchargée dans le répertoire /var du nœud principal du cluster Kubernetes.
3. Ouvrez le fichier `values.yaml` dans le répertoire `/var/citrixadm`.
4. Saisissez un mot de passe pour la base de données dans le champ `dbpasswd` du fichier.
5. Modifiez les valeurs suivantes. L'application NetScaler Console utilise ces valeurs pour configurer l'appliance NetScaler afin que les services soient exposés au monde extérieur :
    - `ingressIP` : une adresse IP virtuelle configurée dans le NetScaler pour accéder à l'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `applicationID` : un ID unique pour distinguer la configuration d'entrée du reste de la configuration sur l'appliance NetScaler.
- `ingressADCIP` : adresse IP NetScaler (NSIP), qui est utilisée comme entrée pour l'application NetScaler Console.
- `ingressADCUsername` : un nom d'utilisateur pour accéder à l'appliance NetScaler. Cet utilisateur doit disposer de privilèges d'écriture.
- `ingressADCPassword` : Mot de passe de l'utilisateur.



6. Modifiez les valeurs suivantes dans la section **storage**. Ces valeurs spécifient la persistance requise pour stocker les fichiers nécessaires à l'application NetScaler Console.

   - `nfsServer` : Nom d'hôte ou adresse IP du serveur NFS
   - `path` : montez le chemin d'accès au dossier pour stocker les fichiers d'application.
   - `size` : au moins 10 Go.

   Remarque

   > L'unité de cette valeur est Gi. Par exemple, 10Gi, 20Gi.

7. Accédez à la section **storage** sous `pg-datastore` et modifiez les valeurs suivantes. Ces valeurs spécifient la persistance utilisée pour la création d'une base de données.

   - `nsfServer` : Nom d'hôte ou adresse IP du serveur NFS.
   - `size` : montez un chemin d'accès pour le dossier utilisé pour le datastore.
   - `path` : au moins 100 Go.

   Remarque

   > L'unité de cette valeur est Gi. Par exemple, 100Gi, 200Gi.

8. Accédez au répertoire /var/citrix du nœud principal et exécutez la commande suivante pour installer une application NetScaler Console : `helm install -n citrixadm --namespace <name> ./citrixadm`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque

> Cette commande helm n'est pas prise en charge dans la version 3.x de helm.

Cette commande installe également les pods requis dans votre cluster. L'argument d'espace de noms est facultatif. Si aucun espace de noms n'est fourni, Helm installe NetScaler Console dans l'espace de noms par défaut. Pour faciliter la gestion, installez NetScaler Console dans un espace de noms distinct.

9. Ouvrez votre navigateur et tapez `http://< virtual server IP address >` et connectez-vous à la NetScaler Console en utilisant `nsroot/nsroot` comme informations d'identification. Pour un accès sécurisé, tapez `https://< virtual server IP address >`.

Remarque

> Lors du déploiement, l'application NetScaler Console crée des tables dans le datastore, ce qui peut prendre un certain temps. Selon les ressources allouées par Kubernetes aux différents pods de l'application NetScaler Console, le service peut prendre 5 à 15 minutes pour démarrer.

NetScaler Console sur serveur Linux KVM

Les plateformes de virtualisation sur lesquelles NetScaler Console peut être provisionné incluent Linux-KVM.

Avant d'installer NetScaler Console sur Linux-KVM, assurez-vous que votre système dispose des extensions de virtualisation matérielle et vérifiez que les extensions de virtualisation du processeur sont disponibles. Vérifiez que `virsh` (un outil en ligne de commande pour la gestion des machines virtuelles) est disponible sur l'hyperviseur.

Utilisez vos informations d'identification d'administrateur pour vous connecter au site Web Citrix.com, accéder aux derniers fichiers d'installation de NetScaler Console et les télécharger sur votre ordinateur. Ensuite, installez NetScaler Console sur votre plateforme Linux-KVM et configurez-le pour votre réseau.

Prérequis

Avant d'installer l'appliance virtuelle NetScaler Console, vérifiez que Linux-KVM version 3.6.11-4 ou ultérieure est installé sur un matériel qui répond aux exigences minimales.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration matérielle requise

COMPOSANT	EXIGENCE
Processeur	Un processeur x86 64 bits avec les fonctionnalités de virtualisation matérielle incluses dans le processeur Intel VT-X. Fournissez au moins 2 cœurs de processeur pour héberger Linux-KVM. **Remarque** Pour vérifier si votre processeur prend en charge l'hôte Linux, entrez la commande suivante à l'invite de commande du shell Linux de l'hôte : `*. egrep'\^flags.* ( vmx | svm ) '/proc/cpuinfo*`. Si les paramètres du BIOS pour l'extension sont désactivés, vous devez les activer dans le BIOS. Il n'y a pas de recommandation spécifique pour la vitesse du processeur, mais plus la vitesse est élevée, meilleures sont les performances de NetScaler Console.
Mémoire (RAM)	Minimum 4 Go pour le noyau Linux de l'hôte. Ajoutez de la mémoire supplémentaire selon les besoins des machines virtuelles.
Disque dur	Calculez l'espace pour le noyau Linux de l'hôte et les exigences des machines virtuelles. Une seule machine virtuelle NetScaler Console nécessite 120 Go d'espace disque.

REMARQUE

Les exigences en matière de mémoire et de disque dur spécifiées concernent le déploiement de NetScaler Console sur la plateforme OpenStack, en considérant qu'aucune autre machine virtuelle n'est exécutée sur l'hôte. Les exigences matérielles pour OpenStack dépendent du nombre de machines virtuelles qui y sont exécutées.

Exigences logicielles

Nous recommandons des noyaux plus récents, tels que la version 64 bits du noyau 3.6.11-4 ou ultérieure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exigences réseau

NetScaler Console ne prend en charge qu'une seule interface réseau paravirtualisée virtIO. Assurez-vous de connecter cette interface au réseau de gestion de l'hôte Linux-KVM, afin que NetScaler Console et Linux-KVM puissent communiquer.

Télécharger les fichiers d'installation de NetScaler Console

Pour télécharger les fichiers d'installation de NetScaler Console depuis `www.citrix.com` :

1. Ouvrez un navigateur web et tapez www.citrix.com dans la barre d'adresse.
2. Passez la souris sur l'option **Se connecter** et cliquez sur **Mon compte**, saisissez vos identifiants Citrix, puis cliquez à nouveau sur **Se connecter**.
3. Accédez à la section **Téléchargements**.
4. Dans la liste **Téléchargements**, sélectionnez **NetScaler® Application Delivery Management**.
5. Sur la page **NetScaler Application Delivery Management**, sélectionnez la version. Par exemple, sélectionnez **Version 13.0**.
6. Cliquez sur **Logiciel produit** pour le développer, puis cliquez sur la dernière version. Par exemple, sélectionnez **NetScaler MAS Release (Feature Phase) 13.0 Build 36.27**.

   La page de la version sélectionnée s'affiche.
7. Dans la liste **Accéder au téléchargement**, sélectionnez **NetScaler MAS image for KVM, 13.0 Build xx.xx**
8. Cliquez sur **Télécharger le fichier**, acceptez le CLUF et téléchargez le fichier image compressé dans n'importe quel dossier de votre machine locale.

Installer NetScaler Application Delivery Management sur Linux-KVM

1. À l'aide de SSH, connectez-vous à l'hôte KVM.
2. À l'invite de commande CLI, en utilisant l'un des programmes de transfert de fichiers, copiez l'image dans un dossier sur le serveur.
3. Accédez au répertoire où vous avez enregistré l'image téléchargée.
4. Effectuez les opérations suivantes à la ligne de commande :

   a. Répertoriez les fichiers dans le répertoire et vérifiez la présence du fichier image.

   b. Utilisez la commande tar pour décompresser le fichier image NetScaler Application Delivery Management. Le package décompressé contient les composants suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. Un fichier XML de domaine qui spécifie les attributs de NetScaler Console

ii. Un fichier texte qui spécifie la somme de contrôle de l'image disque du domaine

iii. Une image disque de domaine

```
tar -xvfz MAS-KVM.tgz

MAS-KVM.xml

MAS-KVM.qcow2

checksum.txt
```

iv. Créez une copie de MAS-KVM.xml sous le nom MAS1-KVM.xml, comme option de sauvegarde. Ouvrez le fichier MAS1-KVM.xml à l'aide de l'éditeur vi.

v. Modifiez MAS1-KVM.xml pour les attributs réseau suivants :

i. `name` - Spécifiez le nom.

ii. `mac` - Spécifiez l'adresse MAC.

iii. `source file` - Spécifiez le chemin d'accès absolu de l'image disque source. Le chemin d'accès au fichier doit être absolu.

REMARQUE

Le nom de domaine et l'adresse MAC doivent être uniques.

iv. `mode` - Spécifiez le mode.

v. `model type` - Définissez sur virtIO.

vi. `source dev` - Spécifiez l'interface.

```
<name> MAS1-KVM</name>

<mac address='52:54:00:29:74:b3'/>

<source file='/var/ MAS-KVM.qcow2'/>

<source dev='eth0' mode='bridge'/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<model type='virtio'/>
```

vi. Définissez les attributs de la VM dans le fichier MAS1-KVM.xml à l'aide de la commande suivante : `virsh define \<FileName\>.xml`

```
virsh define MAS-KVM.xml

Domain MAS defined from MAS-KVM.xml
```

vii. Démarrez la NetScaler Console en saisissant la commande suivante : `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS

Domain MAS started
```

viii. Vous pouvez vous connecter à la machine virtuelle NetScaler Console à l'aide de la commande suivante : `virsh console \<DomainName\>`

```
virsh console MAS

Connected to domain MAS

Escape character is ^]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer le NetScaler Application Delivery Management

REMARQUE

Sur certains hôtes KVM Linux, les invités FreeBSD ne parviennent pas à redémarrer correctement s'ils ont plus d'un processeur. Lorsque l'appliance virtuelle NetScaler Console est redémarrée, l'interface de ligne de commande et l'interface graphique de NetScaler Console ne répondent plus. Pour plus de détails, consultez `<https://bugs.launchpad.net/qemu/+bug/1329956>`

Pour éviter que l'interface de ligne de commande et l'interface graphique de NetScaler Console ne répondent plus lors du redémarrage de l'appliance virtuelle NetScaler Console, arrêtez toutes les machines virtuelles sur l'hôte KVM et effectuez les opérations suivantes sur l'hôte KVM :

1. Supprimez le module kvm_intel à l'aide de la commande suivante : `rmmod kvm\_intel`
2. Désactivez **APICv** et rechargez le module kvm_intel à l'aide de la commande suivante : `modprobe kvm\_intel enable\_apicv=N`
3. Démarrez les machines virtuelles sur l'hôte KVM.

Après avoir installé NetScaler Console, attendez environ 10 minutes que les services soient disponibles, puis connectez-vous à NetScaler Console.

1. À l'invite de commandes, utilisez les informations d'identification de l'administrateur système par défaut pour vous connecter au système :
   - Nom d'utilisateur : `nsroot`
   - Mot de passe : `nsroot`

   REMARQUE

   Après vous être connecté pour la première fois, modifiez le mot de passe administratif. Ensuite, configurez le MAS pour qu'il fonctionne dans votre réseau. Vous pouvez modifier le mot de passe à partir de l'interface utilisateur de NetScaler Console. Depuis la page d'accueil de NetScaler Console, accédez à **Paramètres > Administration des utilisateurs > Utilisateurs**. Sélectionnez l'utilisateur, cliquez sur **Modifier**, puis mettez à jour le mot de passe dans le champ Mot de passe.
2. À l'invite, tapez : *shell*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Tapez **networkconfig** pour accéder au menu de configuration réseau initiale de NetScaler Console. Configurez l’adresse IP de gestion.
4. Pour terminer la configuration réseau initiale de NetScaler Console, suivez les invites. La console affiche les options de configuration réseau initiale de NetScaler Console pour la définition des paramètres suivants pour NetScaler Console. Le nom d’hôte est renseigné par défaut.

   a. Saisissez **2** pour mettre à jour l'adresse IPv4 de NetScaler Console - adresse IP de gestion à laquelle vous accédez à une NetScaler Console
   b. Saisissez **3** pour mettre à jour le masque de sous-réseau - masque de sous-réseau associé à l'adresse IP de gestion
   c. Saisissez **4** pour mettre à jour l'adresse IPv4 de la passerelle - adresse IP de la passerelle par défaut pour le sous-réseau de l'adresse IP de gestion de la NetScaler Console
   d. Saisissez **7** pour enregistrer et quitter - enregistre vos modifications de configuration et quitte le système.

   

5. Exécutez le script de déploiement en tapant la commande à l'invite de commande du shell : `deployment_type.py`
6. Dans l'écran de déploiement qui apparaît, sélectionnez le type de déploiement comme **serveur NetScaler Console**.

   

7. Tapez **Oui** pour déployer NetScaler Console en tant que déploiement autonome.
8. Tapez **Oui** pour redémarrer le serveur NetScaler Console.
9. Après le redémarrage du serveur NetScaler Console, connectez-vous à NetScaler Console en utilisant les informations d'identification de l'administrateur par défaut nsroot/nsroot via la ligne de commande ou l'interface graphique.

   Vous pouvez ensuite accéder à NetScaler Console en tapant l'adresse IP du serveur NetScaler Console dans la barre d'adresse de votre navigateur. Les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont *nsroot/nsroot*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console sur hyperviseur Nutanix (Acropolis)

REMARQUE :

Cette fonctionnalité est disponible dans la version 14.1-38.xx et versions ultérieures.

Vous pouvez utiliser l'image logicielle KVM pour configurer le serveur NetScaler® Console sur l'hyperviseur Nutanix. Avant de commencer, assurez-vous d'avoir configuré Nutanix Prism pour créer une VM pour NetScaler Console.

Configuration matérielle requise

COMPOSANT	CONFIGURATION REQUISE
CPU	Un processeur x86 64 bits avec les fonctionnalités de virtualisation matérielle incluses dans le processeur Intel VT-X. Fournissez au moins 8 cœurs de CPU pour héberger Linux-KVM.
Mémoire (RAM)	Minimum 4 Go pour le noyau Linux hôte. Ajoutez de la mémoire supplémentaire selon les besoins des VM.
Disque dur	Calculez l'espace pour le noyau Linux hôte et les exigences des VM. Une seule VM NetScaler Console nécessite 120 Go d'espace disque.

Télécharger le fichier d'installation de NetScaler Console

Pour télécharger le fichier d'installation de NetScaler Console :

1. Connectez-vous à la page www.citrix.com/downloads.
2. Sélectionnez **NetScaler Console** dans la liste des produits.
3. Sous **Release 14.1**, sélectionnez la version 14.1-38.x ou ultérieure.

   La page de la version sélectionnée s'affiche.
4. Dans la liste **Jump to Download**, sélectionnez **Citrix ADM image for KVM, 14.1 Build xx.xx**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Cliquez sur **Download File**, acceptez l'EULA et téléchargez le fichier image compressé dans n'importe quel dossier de votre machine locale.

Configurer NetScaler Console sur l'hyperviseur Nutanix

1. Décompressez le fichier `.tgz`.
2. Connectez-vous à Nutanix Prism.
3. Accédez à **Settings** et choisissez **Image Configuration**.
   a. Spécifiez un nom d'image.
   b. Sélectionnez **DISK** comme type d'image.
   c. Sélectionnez un conteneur de stockage.
   d. Dans **Image Source**, sélectionnez Télécharger un fichier, puis téléchargez le fichier avec l'extension `.qcow2`.
   e. Cliquez sur **Save**.

   

   Après avoir téléchargé et enregistré, l'image et son statut sont affichés :

   
4. Accédez à VM et cliquez sur **Créer une VM**.
5. Sur la page **Créer une VM**, supprimez le **lecteur de CD-ROM**.
6. Ajoutez un nouveau disque.
   a. Sélectionnez **DISQUE** dans la liste **Type**.
   b. Sélectionnez **Cloner à partir du service d'image** dans la liste **Opération**.
   c. Sélectionnez **SCSI** dans la liste **Type de bus**.
   d. Sélectionnez l'image NetScaler Console dans la liste.
   e. Cliquez sur **Ajouter**.

   

   Le disque est ajouté.

   
7. Ajoutez les détails NIC suivants à la VM :

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Cliquez sur **Enregistrer**.
9. Spécifiez les détails de calcul. Utilisez les valeurs par défaut pour NetScaler Console et l'agent NetScaler.

   

10. Cliquez sur **Enregistrer**.

    Une fois que la VM est répertoriée et affichée comme éteinte, vous devez ajouter le port série pour démarrer la VM.

11. Connectez-vous en SSH à la VM du contrôleur (CVM) en utilisant le nom d'utilisateur et le mot de passe que vous avez définis pour ce compte. Vous trouverez une liste des adresses IP des CVM dans la section Matériel de la console Prism Element.
12. Saisissez **ACLI**.
13. Utilisez la commande suivante pour créer le port série. Saisissez le nom de l'appliance VPX dans `vmname`

    ```
    vm.serial_port_create <vmname> type=kServer index=0
    ```

Configuration réseau

1. Mettez la VM sous tension.
2. Lancez la console VNC.

   

3. Une fois la VM démarrée, connectez-vous en utilisant les informations d'identification par défaut (**nsrecover**/**nsroot**).
4. À l'invite, tapez : *shell*
5. Tapez **networkconfig** pour accéder au menu de configuration réseau initial de NetScaler Console. Configurez l'adresse IP de gestion.
6. Pour terminer la configuration réseau initiale de NetScaler Console, suivez les invites. La console affiche les options de configuration réseau initiale de NetScaler Console pour définir les paramètres suivants. Le nom d'hôte est renseigné par défaut.

   a. Saisissez **2** pour mettre à jour l'adresse IPv4 de NetScaler Console - adresse IP de gestion pour accéder à NetScaler Console.

   b. Saisissez **3** pour mettre à jour le masque de sous-réseau - masque de sous-réseau associé à l'adresse IP de gestion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Saisissez **4** pour mettre à jour l'adresse IPv4 de la passerelle - adresse IP de la passerelle par défaut pour le sous-réseau de l'adresse IP de gestion de NetScaler Console.

d. Saisissez **7** pour enregistrer et quitter - enregistre vos modifications de configuration et quitte le système.



Vous pouvez accéder à NetScaler Console en tapant l'adresse IP du serveur NetScaler Console dans la barre d'adresse de votre navigateur. Les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont *nsroot/nsroot*.

NetScaler Console sur Red Hat OpenShift Virtualization

REMARQUE :

La prise en charge de l'installation de NetScaler Console sur Red Hat® OpenShift® Virtualization (RHOCPV) est disponible à partir de la version 14.1-72.xx de NetScaler Console.

Vous pouvez déployer NetScaler® Console sur Red Hat® OpenShift® Virtualization (RHOCPV) en tant que machine virtuelle. Cela vous permet de gérer les instances NetScaler dans des environnements basés sur OpenShift.

Configuration matérielle requise

COMPOSANT	CONFIGURATION MINIMALE REQUISE
Processeur	Minimum 8 vCPU
Mémoire (RAM)	Minimum 32 Gio
Disque dur	Minimum 120 Gio (disque de démarrage)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

La configuration matérielle requise s'applique à la machine virtuelle NetScaler Console déployée sur RHOCPV. Les valeurs sont basées sur le type d'instance recommandé à usage général (série U – 2xlarge) utilisé lors du déploiement. Assurez-vous que les nœuds de votre cluster RHOCPV disposent d'une capacité suffisante pour exécuter la machine virtuelle NetScaler Console en fonction de ces exigences.

Prérequis

Exigences de la plateforme

- Cluster RHOCPV (OpenShift Virtualization) déployé
- Accès à la console web OpenShift ou à la CLI (oc)
- KubeVirt activé

REMARQUE :

Pour NetScaler déployé sur RHOCPV, la version minimale prise en charge est 14.1–66.64. Pour plus d'informations, consultez l'instance NetScaler VPX sur Red Hat OpenShift® Virtualization (RHOCPV).

Architecture de déploiement

- NetScaler Console s'exécute en tant que machine virtuelle sur RHOCPV
- L'agent NetScaler peut être déployé sur RHOCPV

Installer NetScaler Console sur Red Hat OpenShift Virtualization

Effectuez les étapes suivantes pour installer NetScaler Console sur RHOCPV.

Étape 1 - Préparer l'environnement

1. Assurez-vous que votre cluster RHOCPV est opérationnel.
2. Vérifiez que vous disposez des droits d'administrateur pour créer les machines virtuelles.
3. Assurez-vous que l'opérateur de virtualisation est activé pour créer et gérer des machines virtuelles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 2 - Télécharger le fichier d'installation de NetScaler Console

Pour télécharger le fichier d'installation de NetScaler Console :

1. Connectez-vous à la page `<https://www.citrix.com/downloads>`.
2. Sélectionnez **NetScaler Console** dans la liste des produits.
3. Sous **Release 14.1**, sélectionnez la version 14.1-72.x ou ultérieure. La page de la version sélectionnée s'affiche.
4. Dans la liste **Accéder au téléchargement**, sélectionnez **Image NetScaler Console/NetScaler Console Agent pour KVM, 14.1 Build 72.57**.
5. Cliquez sur **Télécharger le fichier**, acceptez le CLUF et téléchargez le fichier image compressé dans n'importe quel dossier de votre machine locale.

Étape 3 - Télécharger l'image vers le volume amorçable RHOCPV

1. Connectez-vous à votre console Red Hat OpenShift.
2. Dans le tableau de bord, accédez à **Virtualisation > Volumes amorçables**.
3. Cliquez sur **Ajouter un volume** dans le coin supérieur droit et sélectionnez **avec formulaire** pour ajouter un volume amorçable au cluster.
4. Dans le champ **Télécharger l'image PVC**, téléchargez le fichier image NetScaler Console/Agent avec l'extension `.qcow2`.
5. Spécifiez un **Nom de volume** et sélectionnez le **Stockage** disponible.
6. Spécifiez le champ **Préférence de métadonnées de volume** comme **hérité**.
7. Cliquez sur **Enregistrer**.



Étape 4 - Créer la machine virtuelle

Pour créer une machine virtuelle à partir d'un type d'instance :

1. Accédez à **Virtualisation > Machines virtuelles** et cliquez sur **Créer**.
2. Sélectionnez l'onglet **Types d'instance**.
3. Sélectionnez le volume amorçable que vous avez créé à l'étape 3.



4. Sélectionnez un type d'instance qui correspond aux spécifications matérielles de la machine virtuelle pour votre modèle NetScaler Console. Pour plus de détails, consultez Exigences matérielles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Saisissez un nom pour la machine virtuelle.
6. Cliquez sur **Personnaliser la machine virtuelle**.
7. Détachez le disque par défaut (ici `cloudinitdesk`) s'il est présent et conservez le disque amorçable de 120 Go.

   
8. Dans la section **Réseau**, sélectionnez `virtio` comme modèle d'interface, puis choisissez le réseau requis dans la liste.

   
9. Cliquez sur **Create VirtualMachine**.

Étape 5. Démarrer la machine virtuelle

Démarrez la machine virtuelle et vérifiez qu'elle atteint l'état d'exécution.

Étape 6. Accéder à NetScaler Console

Accédez à NetScaler Console à l'aide de l'URL suivante :

```
https://<console-ip-address>
```

NetScaler Console sur Azure Cloud

À partir de la version 14.1-43.x, NetScaler Console offre davantage d'options de déploiement où NetScaler Console peut être déployé en tant que machine virtuelle (VM) sur Azure via l'Azure Government Marketplace. Le service NetScaler Console n'est pas une option viable pour les clients dont les déploiements cloud sont isolés (air-gapped) et ne disposent pas de connectivité Internet. NetScaler Console déployé en tant que VM sur Azure vous permet de gérer et de surveiller efficacement vos instances NetScaler VPX à l'aide de NetScaler Console au sein des déploiements Azure.

REMARQUE :

NetScaler Console sur Azure Cloud est disponible uniquement sur l'Azure Government Marketplace.

Prérequis

Avant de configurer, assurez-vous d'avoir accès à Azure Cloud et à un groupe de ressources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Nous vous recommandons de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités requises avant de provisionner NetScaler Console.

Configurer NetScaler Console

Dans Azure Cloud :

1. Accédez à la Marketplace, recherchez NetScaler Console, puis cliquez sur **Sélectionner**.

   Après avoir sélectionné l'image, vous serez redirigé vers le flux de travail **Créer une machine virtuelle**.

2. Spécifiez les éléments suivants :

   a. **Groupe de ressources** - Sélectionnez un groupe de ressources dans la liste.

   b. **Nom de la machine virtuelle** - Un nom de votre choix.

   c. **Région** - Sélectionnez une région dans la liste.

   d. **Image** - Remplie automatiquement puisque vous l'avez sélectionnée depuis la Place de marché.

   e. Sélectionnez la taille de la VM dans la liste (8 vCPU, 32 Go de RAM sont recommandés).

   f. **Type d'authentification** - Sélectionnez Clé publique SSH.

      REMARQUE :

      L'option de mot de passe n'est pas prise en charge.

   g. **Nom d'utilisateur** - Modifiez le nom en `nsroot`. Le nom d'utilisateur par défaut pour accéder à NetScaler Console est `nsroot`.

   h. **Source de la clé publique SSH** - Vous pouvez utiliser une paire de clés existante ou en créer une nouvelle.

   i. **Ports entrants publics** - Sélectionnez **Aucun**.

   j. Cliquez sur **Vérifier + Créer**.

      Le résumé de la VM s'affiche. Validez tout, puis cliquez sur **Créer**.

   k. Le déploiement de la VM indique que le statut est en cours. Une fois le déploiement terminé, cliquez sur **Accéder à la ressource**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les informations sur la VM s'affichent et vous pouvez consulter les adresses IP publiques et privées de la VM sous **Mise en réseau**. Vous pouvez vous connecter (`nsroot` / `nsroot`) en utilisant l'adresse IP publique via un navigateur.

REMARQUE :

Si vous souhaitez utiliser l'adresse IP privée, assurez-vous de disposer d'un Azure Virtual Desktop exécuté dans le même réseau cloud Azure pour accéder à NetScaler Console via l'adresse IP privée.

l. Vérifiez si le processus NetScaler Console est démarré et en cours d'exécution en vous connectant à la machine virtuelle via SSH avec le nom d'utilisateur `nsrecover` et le mot de passe `nsroot`.

m. Une fois les processus backend démarrés et en cours d'exécution, vous pouvez vous connecter à l'interface graphique de NetScaler Console en utilisant le mot de passe `nsroot`. Lors de la première connexion, le système vous invite à modifier le mot de passe par défaut.

Paire HA NetScaler Console sur Azure Cloud

Dans Azure, la haute disponibilité pour NetScaler Console est obtenue à l'aide d'un équilibreur de charge Azure (ALB). L'ALB surveille les instances en envoyant des sondes d'intégrité aux nœuds principal et secondaire. L'instance principale répond avec `200 OK`, tandis que l'instance secondaire ne répond pas. Sur la base de ces réponses, l'ALB envoie le trafic exclusivement à l'instance principale. En cas de basculement, le nouveau principal commence à répondre avec `200 OK`, et l'ALB lui envoie automatiquement le trafic.

Prérequis

Assurez-vous que :

- Vous avez accès à Azure Cloud et au groupe de ressources.

REMARQUE :

Nous vous recommandons de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités requises avant de provisionner NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Vous créez deux instances autonomes de NetScaler Console sur Azure Cloud.
- Les ports requis sont ouverts pour la communication. Pour plus d'informations, consultez Configuration système requise.

Configurer la paire HA NetScaler Console

Après avoir configuré deux instances autonomes de NetScaler Console :

1. Connectez-vous à l'une des interfaces graphiques de NetScaler Console.
2. Accédez à **Paramètres > Paramètres de haute disponibilité**.

   REMARQUE :

   - Pour configurer une paire HA, vous devez fournir l'adresse IP privée de l'autre NetScaler Console.
   - L'IP flottante peut être n'importe quelle IP disponible du VNet Azure (réseau virtuel).

3. Cliquez sur **Configurer la haute disponibilité (HA) de NetScaler Console**, fournissez les détails du nœud secondaire, l'adresse IP flottante, puis cliquez sur **Configurer**.

   

4. Dans la fenêtre de confirmation, cliquez sur **Oui**. Les instances NetScaler Console redémarrent pour former une paire HA.
5. Une fois la configuration de la paire HA terminée, connectez-vous à la NetScaler Console principale et accédez à **Paramètres > Déploiement HA** pour valider les nœuds principal et secondaire.

   

L'étape suivante consiste à configurer l'adresse IP flottante comme IP frontale de l'équilibreur de charge Azure dans Azure Cloud. Dans le portail Azure Cloud, recherchez « équilibreur de charge », sélectionnez **Équilibreurs de charge** dans les résultats, puis cliquez sur **Créer** :

1. Dans **Informations de base**, créez un équilibreur de charge Azure (ALB) dans le même groupe de ressources et la même région où les machines virtuelles de la console sont configurées.

   a. Sélectionnez SKU : **Standard**, Type : **Interne** et Niveau : **Régional** sous **Détails de l'instance**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans **Configuration IP frontale**, ajoutez une IP frontale avec l'IP flottante configurée pour la paire HA de la console.
3. Dans **Pools de back-end**, ajoutez l'adresse IP des deux instances de la console.
4. **Règles d'équilibrage de charge** : Configurez les règles suivantes avec le protocole, le port, le port back-end, la sonde d'intégrité et l'IP flottante activés :

NOM DE LA RÈGLE	PROTOCOLE	PORT	PORT DE BACKEND	IP FLOTTANTE
Règle-80	TCP	80	80	Oui
Règle-443	TCP	443	443	Oui
Règle-5454	TCP	5454	5454	Oui
Règle-22	TCP	22	22	Oui
Règle-8443	TCP	8443	8443	Oui
Règle-7443	TCP	7443	7443	Oui
Règle-27000	TCP	27000	27000	Oui
Règle-7279	TCP	7279	7279	Oui
Règle-5563	TCP	5563	5563	Oui
Règle-4739	UDP	4739	4739	Oui
Règle-5140	UDP	5140	5140	Oui
Règle-162	UDP	162	162	Oui
Rule-514	UDP	514	514	Oui
Rule-5557	UDP	5557	5557	Oui
Rule-5558	UDP	5558	5558	Oui

5. **Sonde d'intégrité** : Créez une vérification d'intégrité HTTP avec tous les ports requis répertoriés à l'étape 4. Cette sonde d'intégrité active la console principale en tant qu'Active et la console secondaire en tant que Passive. Par exemple :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Port : 443

b. URL : `/mas_health`

c. Code de réponse attendu : 200

Pour plus d'informations sur la création d'un équilibreur de charge, consultez Créer un équilibreur de charge dans la documentation Azure.

Après avoir configuré l'équilibreur de charge, vous pouvez utiliser l'adresse IP frontale d'ALB pour accéder à NetScaler Console.

REMARQUE :

Assurez-vous de disposer d'un Azure Virtual Desktop exécuté dans le même réseau Azure pour accéder à NetScaler Console via l'adresse IP frontale.

NetScaler Console sur Amazon Web Services (AWS)

À partir de la version **14.1-47.x**, vous pouvez déployer NetScaler Console à l'aide d'une AMI sur AWS Marketplace dans **AWS GovCloud**.

Prérequis

Pour lancer une AMI NetScaler Console au sein d'un cloud privé virtuel (VPC) AWS à l'aide de l'interface graphique Amazon, vous avez besoin :

- D'un compte AWS
- D'un cloud privé virtuel (VPC) AWS
- De vous assurer que les ports requis, tels que 22, 80 et 443, sont ouverts lorsque vous créez un groupe de sécurité dans AWS. Pour plus d'informations, consultez Configuration système requise.

Configurer NetScaler Console

1. Connectez-vous à la place de marché AWS à l'aide de vos identifiants AWS.
2. Recherchez AMI et sélectionnez **AMIs**.
3. Dans la zone de recherche, tapez NetScaler Console, sélectionnez NetScaler Console, puis cliquez sur **Lancer l'instance à partir de l'AMI**.
4. Sous **Type d'instance**, sélectionnez l'option 8 vCPU et 32 Go de mémoire dans la liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Par défaut, l'AMI NetScaler Console est de 500 Go.

5. Sous **Paire de clés (connexion)**, sélectionnez une paire de clés existante ou créez-en une nouvelle.
6. Sous **Paramètres réseau**, cliquez sur **Modifier** et :
   a. Sélectionnez le VPC dans la liste.
   b. Sélectionnez ou créez un nouveau sous-réseau.
   c. Activez **Attribution automatique d'IP publique** pour lancer NetScaler Console à l'aide d'une adresse IP publique.
   d. Sélectionnez ou créez un groupe de sécurité.

      REMARQUE :

      Assurez-vous que les ports requis tels que les ports 22, 443 et 80 sont ouverts. Pour plus d'informations, consultez Configuration système requise.

   e. Cliquez sur **Lancer l'instance**. Un ID d'instance est créé.
7. Cliquez sur l'ID d'instance.

   Vous devrez peut-être attendre que la **vérification de l'état** affiche « réussi » (coche verte).
8. Une fois les vérifications de sécurité réussies, cliquez sur l'ID d'instance pour afficher les détails.

   Utilisez l'adresse IP pour lancer l'interface graphique de NetScaler Console. Si vous souhaitez utiliser une adresse IP privée, assurez-vous de disposer d'un VDI dans AWS.

   Le tableau suivant décrit le processus de connexion AWS via SSH, l'interface graphique et la console série (une console accessible depuis AWS) :

   | | SSH | | Console série | | GUI | |

	nsracine	**nsrécupération**	**nsracine**	**nsrécupération**	**nsroot**	**Utilisateur personnalisé**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mot de passe	Autorisé (Le mot de passe par défaut est `nsroot`)	Autorisé (Le mot de passe par défaut est `nsroot`)	Non autorisé	Autorisé (Le mot de passe par défaut est `nsroot`)	Autorisé (Le mot de passe par défaut est `nsroot`)	Autorisé (Mot de passe défini par l'utilisateur)
Clé publique	Autorisé	s/o	s/o	s/o	s/o	s/o

Configurer le déploiement haute disponibilité

La haute disponibilité (HA) fait référence à un système toujours disponible pour un utilisateur sans aucune interruption des services. La configuration de la haute disponibilité est cruciale en cas d'indisponibilité du système, de pannes de réseau ou d'application, et constitue une exigence clé pour toute entreprise. Un déploiement haute disponibilité de deux nœuds NetScaler Console en mode actif-passif avec les mêmes configurations assure des opérations ininterrompues.

Scénario de déploiement



REMARQUE

La limite de stockage maximale validée pour un déploiement HA NetScaler Console unique est de 3 To. Pour plus d'informations, consultez le guide de déploiement.

Important

Pour accéder à NetScaler Console 12.1 build 48.18 ou versions ultérieures via HTTPS :
Si vous avez configuré une instance NetScaler pour équilibrer la charge de NetScaler Console en mode haute disponibilité, supprimez d'abord l'instance NetScaler. Ensuite, configurez une adresse IP flottante pour accéder à NetScaler Console en mode haute disponibilité.
Voici les avantages du déploiement haute disponibilité dans NetScaler Console :

- Un mécanisme amélioré pour surveiller les pulsations entre le nœud principal et le nœud secondaire.
- Fournit une réplication physique en continu de la base de données au lieu d'une réplication bidirectionnelle logique.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Possibilité de configurer l'adresse IP flottante sur le nœud principal pour éliminer le besoin d'un équilibreur de charge NetScaler séparé.
- Fournit un accès facile à l'interface utilisateur de NetScaler Console à l'aide de l'adresse IP flottante.
- L'interface utilisateur de NetScaler Console est fournie uniquement sur le nœud principal. En utilisant le nœud principal, vous pouvez éliminer le risque d'accéder au nœud secondaire et d'y apporter des modifications.
- La configuration de l'adresse IP flottante gère la situation de basculement et la reconfiguration des instances n'est pas nécessaire.
- Offre une capacité intégrée à détecter et à gérer les situations de split-brain.

Le tableau suivant décrit les termes utilisés dans le déploiement à haute disponibilité.

TERMES	DESCRIPTION
Nœud principal	Premier nœud enregistré dans le déploiement à haute disponibilité.
Nœud secondaire	Deuxième nœud enregistré dans le déploiement à haute disponibilité.
Battement de cœur	Un mécanisme utilisé pour échanger des messages entre le nœud principal et le nœud secondaire dans la configuration à haute disponibilité. Les messages déterminent l'état et la santé de l'application sur chaque nœud individuel.
Adresse IP flottante	Une adresse IP flottante est une adresse IP qui peut être instantanément déplacée d'un nœud à un autre dans le même sous-réseau. En interne, elle est configurée comme un alias sur l'interface réseau du nœud principal. En cas de basculement, l'adresse IP flottante est déplacée de manière transparente de l'ancien nœud principal vers le nouveau. Elle est utile dans une configuration à haute disponibilité car elle permet aux clients de communiquer avec les nœuds à haute disponibilité en utilisant une seule adresse IP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour plus d'informations sur les détails des ports et des protocoles, consultez Ports.

Composants de l'architecture haute disponibilité

La figure suivante présente l'architecture de deux nœuds NetScaler Console déployés en mode haute disponibilité.



Dans un déploiement haute disponibilité, un nœud NetScaler Console est configuré comme nœud principal (MAS 1) et l'autre comme nœud secondaire (MAS 2). Si le nœud principal tombe en panne pour une raison quelconque, le nœud secondaire prend le relais en tant que nouveau nœud principal.

Outil de surveillance

L'outil de surveillance est un processus interne utilisé pour surveiller, alerter et gérer les situations de basculement. L'outil est actif et s'exécute sur chaque nœud en haute disponibilité. Il est responsable du démarrage des sous-systèmes, de l'initialisation de la base de données sur les deux nœuds, de la décision concernant le nœud principal ou secondaire en cas de basculement, et ainsi de suite.

Nœud principal

Le nœud principal accepte les connexions et gère les instances. Tous les processus tels qu'AppFlow, SNMP, LogStream, syslog, etc., sont gérés par le nœud principal. L'accès à l'interface utilisateur de NetScaler Console est disponible sur le nœud principal. L'adresse IP flottante est configurée sur le nœud principal.

Nœud secondaire

Le nœud secondaire écoute les messages de pulsation envoyés par le nœud principal. La base de données sur le nœud secondaire est uniquement en mode réplique en lecture. Aucun des processus n'est actif sur le nœud secondaire et l'interface utilisateur de NetScaler Console n'est pas accessible sur le nœud secondaire.

Réplication physique en continu

Les nœuds principal et secondaire se synchronisent via un mécanisme de pulsation. Avec la réplication physique en continu de la base de données, le nœud secondaire démarre en mode

© 1997–2026 Citrix Systems, Inc. All rights reserved.

réplique en lecture. Le nœud secondaire écoute les messages de pulsation reçus du nœud principal. Si le nœud secondaire ne reçoit aucune pulsation pendant une période de 180 secondes, le nœud principal est considéré comme étant hors service. Ensuite, le nœud secondaire prend le relais en tant que nœud principal.

Messages de pulsation

Les messages de pulsation sont des paquets de datagrammes utilisateur (UDP) qui sont envoyés et reçus entre le nœud principal et le nœud secondaire. Ils surveillent tous les sous-systèmes de NetScaler Console et la base de données pour échanger des informations sur l'état du nœud, la santé, les processus, etc. Les informations sont partagées entre les nœuds haute disponibilité chaque seconde. Des notifications sont envoyées sous forme d'alertes à l'administrateur en cas de basculement ou de rupture des états de haute disponibilité.

Adresse IP flottante

L'adresse IP flottante est associée au nœud principal dans la configuration de haute disponibilité. C'est un alias donné à l'adresse IP du nœud principal, que le client peut utiliser pour se connecter à NetScaler Console sur le nœud principal. Étant donné que l'adresse IP flottante est configurée sur le nœud principal, la reconfiguration de l'instance n'est pas nécessaire en cas de basculement. Les instances se reconnectent à la même adresse IP pour atteindre le nouveau nœud principal.

Points clés à noter

- Dans une configuration de haute disponibilité, les deux nœuds NetScaler Console sont déployés en mode actif-passif. Ils doivent se trouver sur les mêmes sous-réseaux, utiliser la même version et build logicielle, et avoir les mêmes configurations.
- Adresse IP flottante :
  - L'adresse IP flottante est configurée sur le nœud principal.
  - Les instances n'ont pas besoin d'être reconfigurées en cas de basculement.
  - Vous pouvez accéder à un nœud de haute disponibilité depuis l'interface utilisateur, soit en utilisant l'adresse IP du nœud principal, soit l'adresse IP flottante.

    REMARQUE :

    Nous vous recommandons d'utiliser l'adresse IP flottante pour accéder à l'interface utilisateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Base de données :
  - Dans une configuration de haute disponibilité, tous les fichiers de configuration sont synchronisés automatiquement du nœud principal vers le nœud secondaire à un intervalle d'une minute.
  - La synchronisation de la base de données se produit instantanément par réplication physique de la base de données.
  - La base de données sur le nœud secondaire est en mode réplique en lecture.
- Mise à niveau de NetScaler Console :
  - Les processus internes mettent implicitement à niveau NetScaler Console à partir des versions antérieures.

    REMARQUE :

    Une fois la mise à niveau réussie, vous devez configurer l'adresse IP flottante.
- Le port UDP par défaut 5005 est disponible sur les deux nœuds pour l'envoi des pulsations et la réception des messages.
- Adresse MAC Le paramètre de l'option « Modifications d'adresse MAC » dans un hyperviseur affecte le trafic qu'une machine virtuelle reçoit. Autorisez les modifications d'adresse MAC sur le commutateur virtuel afin que l'adresse IP flottante se déplace de manière transparente vers le nouveau nœud principal après le basculement. Par exemple, lors du déploiement de NetScaler Console en haute disponibilité sur VMware ESXi, assurez-vous d'accepter les modifications d'adresse MAC. ESXi autorise désormais les requêtes de modification de l'adresse MAC active vers une adresse différente de l'adresse MAC initiale.

  REMARQUE :

  Pour NetScaler Console déployé sur ESXi version 6.7, vous pouvez également définir l'option **Modifications d'adresse MAC** sur **Rejeter**. Après le basculement, le trafic circule vers le nouveau nœud principal de manière transparente, quelle que soit la configuration des **Modifications d'adresse MAC**. Par conséquent, l'acceptation des modifications d'adresse MAC n'est pas obligatoire.

  Si NetScaler Console est déployé sur une version d'ESXi inférieure à 6.7, assurez-vous que l'option **Modifications d'adresse MAC** est définie sur **Accepter** uniquement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Conditions préalables

Avant de configurer la haute disponibilité pour les nœuds NetScaler Console, notez les conditions préalables suivantes :

- Le déploiement haute disponibilité de NetScaler Console est pris en charge à partir de la version 12.0 build 51.24 de NetScaler Console.
- Téléchargez le fichier image NetScaler Console (.xva) depuis le site NetScaler : `<https://www.citrix.com/downloads/>`

Nous vous recommandons de définir la priorité du processeur (dans les propriétés de la machine virtuelle) au niveau le plus élevé afin d'améliorer le comportement de planification et la latence du réseau.

Le tableau suivant répertorie les exigences minimales pour les ressources de calcul virtuelles :

COMPOSANT	EXIGENCE
RAM	**32 Go**
CPU virtuel	**8 CPU**
Espace de stockage	Nous vous recommandons d'utiliser la technologie de disque SSD (Solid-State Drive) pour les déploiements de NetScaler Console. La valeur par défaut est de 120 Go. L'exigence de stockage réelle dépend de l'estimation du dimensionnement de NetScaler Console. Si votre exigence de stockage NetScaler Console dépasse 120 Go, vous devez attacher un disque supplémentaire. **Remarque :** Vous ne pouvez ajouter qu'un seul disque supplémentaire. Nous vous recommandons d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à NetScaler Console.
Interfaces réseau virtuelles	1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANT	EXIGENCE
Débit	1 Gbit/s ou 100 Mbit/s
Hyperviseur	**Versions**
Citrix Hypervisor	6.2 et 6.5
VMware ESXi	5.5 et 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu et Fedora

Pour configurer NetScaler Console en mode haute disponibilité

À partir de la version 14.1 build 17.x, vous pouvez déployer une configuration de haute disponibilité directement depuis l'interface graphique de NetScaler Console du nœud principal.

1. Enregistrer le premier serveur (nœud principal).
2. Enregistrer le deuxième serveur (nœud secondaire).
3. Déployer la configuration de haute disponibilité dans l'interface graphique du nœud principal.

Enregistrer le premier serveur (nœud principal)

Pour enregistrer le nœud principal :

1. Utilisez le fichier image .xva téléchargé depuis le site NetScaler et importez-le dans votre hyperviseur.

   REMARQUE :

   L'importation et le démarrage du fichier image .xva peuvent prendre quelques minutes. Vous pouvez voir l'état en bas de l'écran.

   

2. Une fois l'importation réussie, cliquez avec le bouton droit de la souris et cliquez sur **Démarrer**.

   

3. À partir de l'onglet **Console**, configurez NetScaler Console avec les configurations réseau initiales.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Une fois la configuration réseau initiale terminée, le système vous invite à vous connecter. Connectez-vous en utilisant les informations d'identification suivantes : *nsrecover/nsroot*.

REMARQUE :

Après vous être connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

Enregistrer le deuxième serveur (nœud secondaire)

1. Utilisez le fichier image **.xva** téléchargé depuis le site NetScaler et importez-le dans votre hyperviseur.
2. À partir de l'onglet **Console**, configurez NetScaler Console avec les configurations réseau initiales, comme indiqué dans l'image suivante.
3. Une fois la configuration réseau initiale terminée, le système vous invite à vous connecter. Connectez-vous en utilisant les informations d'identification suivantes : *nsrecover/nsroot*.

REMARQUES :

- Après vous être connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.
- Le système affichera des messages d'erreur en cas de problème de configuration.
- Le système redémarre et les configurations prennent quelques minutes pour être effectives.

Déployer la configuration de haute disponibilité à partir de l'interface graphique du nœud principal

Après avoir enregistré les nœuds principal et secondaire, connectez-vous à l'interface graphique du nœud principal pour configurer la paire de haute disponibilité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque :

- Avant de déployer les nœuds dans une paire de haute disponibilité, assurez-vous que le nœud secondaire a terminé son redémarrage après la configuration réseau initiale.

Pour déployer une paire de haute disponibilité à partir du nœud principal, suivez ces étapes :

1. Connectez-vous à l'interface graphique du nœud principal.
2. Accédez à **Paramètres > Administration > Paramètres de haute disponibilité > Configurer la haute disponibilité (HA) de NetScaler Console**.
3. Sur la page **Configurer la haute disponibilité (HA) de NetScaler Console**, saisissez les détails suivants pour le nœud secondaire :
   - Adresse IP du nœud pair
   - Mot de passe du nœud pair
   - Adresse IP flottante
4. Cliquez sur Configurer.
5. Sur la page **Confirmer**, cliquez sur **Oui**.

   Configurer la paire HA(/en-us/netscaler-application-delivery-management-software/media/configure-ha-pair.png)

   Les nœuds principal et secondaire sont redémarrés pour former une paire haute disponibilité, ce qui prend généralement environ 10 minutes.

   Remarques :

   - Vous pouvez maintenant commencer à utiliser l'**adresse IP flottante**.
   - Une adresse IP flottante est obligatoire pour le déploiement de nœuds en haute disponibilité.
   - Une fois le déploiement en haute disponibilité terminé, utilisez l'adresse IP flottante pour accéder à l'interface utilisateur de NetScaler Console.
6. Accédez à **Paramètres > Déploiement** pour valider le déploiement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque :

Le nœud secondaire peut prendre environ 10 minutes pour démarrer. Jusque-là, l'état du nœud secondaire est affiché comme **Hors service**.

Pour plus d'informations, consultez la section Questions fréquemment posées.

Désactiver la haute disponibilité

Vous pouvez désactiver la haute disponibilité sur une paire haute disponibilité NetScaler Console et convertir les nœuds en serveurs NetScaler Console autonomes.

REMARQUE :

Désactivez la haute disponibilité à partir du nœud principal.

Pour désactiver la haute disponibilité :

1. Dans un navigateur web, saisissez l'adresse IP du nœud principal du serveur NetScaler Console.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Dans l'onglet **Système**, accédez à **Déploiement** et cliquez sur **Rompre la haute disponibilité**.

   Une boîte de dialogue s'affiche. Cliquez sur **Oui** pour rompre le déploiement de haute disponibilité.

Redéployer la haute disponibilité

Après avoir désactivé la haute disponibilité pour un déploiement autonome, vous pouvez la redéployer en mode haute disponibilité. Le redéploiement de la haute disponibilité est similaire au premier déploiement de la haute disponibilité. Pour plus de détails, consultez Déployer la configuration de haute disponibilité à partir de l'interface graphique du nœud principal.

REMARQUE :

Après avoir désactivé la haute disponibilité de NetScaler® Console, utilisez un seul nœud de console comme serveur de licences autonome. Le second nœud doit être réapprovisionné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scénarios de basculement de haute disponibilité

Un basculement se produit si l'une des conditions suivantes est rencontrée :

- **Défaillance du nœud** : Le nœud principal tombe en panne, aucun battement de cœur n'est détecté du nœud principal pendant 180 secondes.
- **Défaillance de l'état de l'application** : Le nœud principal est opérationnel, mais l'un des processus NetScaler Console est arrêté.

Afficher les messages du journal de synchronisation de la base de données

Dans la paire HA de NetScaler Console, les fichiers de configuration sont synchronisés automatiquement du nœud principal vers le nœud secondaire et la réplication physique en continu de la base de données a lieu.

Cependant, s'il y a une erreur de réplication en continu, le bouton **Synchroniser la base de données** apparaît. Vous pouvez cliquer sur le bouton **Synchroniser la base de données** pour démarrer le processus de synchronisation de la base de données.



Pour afficher la progression de la synchronisation de la base de données, cliquez sur **Afficher les journaux**. Le message **Journaux de synchronisation de la base de données** apparaît et vous pouvez afficher les détails de la progression de la synchronisation en temps réel.



Scénario de split-brain

Lorsqu'il n'y a pas de communication entre les deux nœuds en raison d'une interruption de la liaison réseau, alors :

- Le nœud principal continue de fonctionner comme principal
- Le nœud secondaire prend le relais en tant que principal en raison de l'échec de la réception des signaux de pulsation (heartbeats)
- Les deux nœuds exécuteraient leurs instances de base de données individuelles

Par exemple, dans une entreprise, deux nœuds NetScaler Console ont été déployés en tant que principal et secondaire. En raison d'une éventuelle interruption de la liaison réseau, la communication entre les deux nœuds NetScaler Console est complètement interrompue. Puisqu'il n'y a pas d'échange de signaux de pulsation (heartbeats) pendant plus de 180 secondes, les deux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nœuds se considèrent comme le nœud principal. Les deux nœuds agissent comme des nœuds actifs et exécutent leurs propres instances de base de données.

À partir de NetScaler Console 12.1 ou d'une version ultérieure, cette situation de split-brain est gérée avec élégance après la restauration de la liaison réseau et des signaux de pulsation (heartbeats). La synchronisation de la haute disponibilité est restaurée automatiquement. Le temps de récupération dépend des données et de la vitesse de la liaison entre les nœuds.

REMARQUE :

Pendant la condition de split-brain, les modifications survenues sur l'ancien nœud principal sont réinitialisées avec le nouveau nœud principal lorsqu'il est rejoint en haute disponibilité. Les modifications survenues sur le nouveau nœud principal pendant le split-brain restent intactes.

Licences

Le serveur NetScaler Console peut contenir des licences VIP, CICO et de capacité mutualisée. Lorsque les licences sont émises pour un serveur NetScaler Console, elles sont liées à l'ID d'hôte du serveur. L'attribution de licences à un autre serveur NetScaler Console est restreinte.

Si vous configurez une paire haute disponibilité NetScaler Console en tant que serveur de licences, les fichiers de licence appliqués sur le principal sont synchronisés avec le secondaire.

REMARQUE :

- À partir de la version 12.1-50.x et ultérieure, les licences NetScaler Console sont automatiquement synchronisées du nœud principal vers le nœud secondaire.

Configurer la haute disponibilité sur différents sous-réseaux de couche 3 (HA sur L3)

À partir de la version 14.1-66.x, NetScaler Console prend en charge les déploiements en haute disponibilité (HA) sur différents sous-réseaux de couche 3 (L3).

Cette amélioration offre les fonctionnalités suivantes :

- Les nœuds NetScaler Console principaux et secondaires peuvent être déployés dans différents sous-réseaux L3 ou centres de données.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'adresse IP flottante (VIP) est configurée et gérée par un équilibreur de charge externe.
- L'équilibreur de charge transfère le trafic client vers le nœud NetScaler Console actif.
- La synchronisation HA entre les nœuds reste inchangée.

Pour les concepts généraux de la HA, les rôles des nœuds et le comportement de synchronisation, consultez la documentation HA.

NetScaler Console prend en charge les déploiements HA sur différents sous-réseaux en utilisant un équilibreur de charge externe pour gérer les adresses IP flottantes, éliminant ainsi les dépendances L2.

Auparavant, NetScaler Console exigeait que les nœuds principal et secondaire résident dans le même sous-réseau, car l'adresse IP flottante était détenue et gérée en interne par la paire HA. Cela créait une dépendance de couche 2 et limitait les déploiements sur des réseaux segmentés ou géographiquement séparés. Cela restreignait les déploiements HA aux environnements de couche 2 et empêchait les clients de :

- Déployer la HA sur différents sous-réseaux.
- Distribuer les nœuds entre les centres de données.
- S'aligner sur les architectures de réseau d'entreprise routées.

Architecture de haut niveau

- L'adresse IP flottante (VIP) est configurée sur un équilibreur de charge externe.
- NetScaler Console ne prend pas en charge le VIP dans ce déploiement.
- L'équilibreur de charge transfère le trafic vers le nœud actif en fonction des vérifications de santé.
- La synchronisation HA se poursuit directement entre les nœuds via la connectivité L3.
- La prise en charge du VIP basée sur ARP au sein de NetScaler Console n'est pas utilisée.

REMARQUE :

L'équilibreur de charge recommandé est NetScaler, bien que les équilibreurs de charge tiers soient également pris en charge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Déploiement et configuration

Prérequis

- Un équilibreur de charge externe compatible couche 3 déployé et accessible par :
  - Clients
  - Les deux nœuds NetScaler Console
- Connectivité réseau entre les nœuds principal et secondaire.

Flux de travail

1. Déployez deux nœuds NetScaler Console (principal et secondaire) dans des sous-réseaux L3 ou des centres de données distincts.
2. Déployer et configurer un équilibreur de charge externe.
3. Créez une adresse IP flottante (VIP) sur l'équilibreur de charge (front-end) et ajoutez les deux nœuds NetScaler Console en tant que cibles de backend.
4. Créez des règles d'équilibrage de charge pour le VIP en utilisant les protocoles et ports suivants.

SERVEUR VIRTUEL LB	PROTOCOLE	PORT
HTTP	TCP	80
HTTPS	TCP	443
BD et HA	TCP	5454
NTP	UDP	123
SNMP	UDP	162
SYSLOG	UDP	514
LICENCE	TCP	27000
DÉMON DU FOURNISSEUR	TCP	7279

5. Configurez les moniteurs d'intégrité sur toutes les cibles backend afin que l'équilibreur de charge ne transmette le trafic qu'au nœud actif.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MONITEUR / OBJECTIF	PROTOCOLE / PORT
HA et BD	TCP / 5454
SNMP	UDP / 162
Syslog	UDP / 514
NTP	UDP / 123

6. Configurez la paire HA de NetScaler Console et spécifiez l'adresse IP flottante qui est configurée en externe.

Configurer la haute disponibilité dans NetScaler Console

1. Connectez-vous à l'interface graphique de NetScaler Console sur le nœud que vous souhaitez configurer comme principal.
2. Accédez à **Paramètres > Paramètres de haute disponibilité**.
3. Sélectionnez **Configurer la haute disponibilité (HA) de NetScaler Console** et fournissez les détails du nœud secondaire.
4. Saisissez l'adresse IP virtuelle (VIP) configurée sur l'équilibreur de charge externe, sélectionnez **L'adresse IP flottante est configurée en externe** et cliquez sur **Enregistrer**.

   REMARQUE :

   Configurez l'adresse IP flottante (VIP) sur l'équilibreur de charge externe. NetScaler Console ne possède ni ne gère cette VIP dans le modèle HA de sous-réseaux différents.

   
5. Les instances NetScaler Console redémarrent pour former une paire HA.
6. Une fois la HA configurée, connectez-vous au nœud principal et accédez à **Paramètres > Déploiement HA** pour valider l'état primaire et secondaire.

   

Configurer NetScaler en tant qu'équilibreur de charge externe

Configurez l'adresse IP flottante (VIP) et les règles de transfert sur votre équilibreur de charge externe afin que le trafic client soit envoyé uniquement au nœud NetScaler Console actif. Les étapes exactes varient selon le fournisseur de l'équilibreur de charge. Les exigences suivantes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

s'appliquent généralement et peuvent être mises en œuvre sur NetScaler ou un équilibreur de charge tiers :

1. Créez tous les serveurs virtuels avec la même adresse IP virtuelle (frontend) que les clients utilisent pour accéder à NetScaler Console.
2. Créez des groupes de services pour chacun des serveurs virtuels et liez les deux nœuds NetScaler Console en tant que membres du groupe de services.
3. Lie les groupes de services aux serveurs virtuels respectifs.
4. Créez des moniteurs qui indiquent de manière fiable le nœud actif et liez-les aux groupes de services configurés à l'étape 2.

REMARQUE :

Assurez-vous que tous les ports nécessaires sont ouverts entre l'équilibreur de charge et les deux nœuds NetScaler Console, comme défini dans Configuration système requise.

Exemple de script de configuration d'équilibrage de charge NetScaler

Ajouter des serveurs virtuels d'équilibrage de charge

```
add lb vserver ADM-LB HTTP <EXTERNAL_VIP> 80 -persistenceType NONE
-cltTimeout 180



add lb vserver ADM-LB-HTTPS SSL <EXTERNAL_VIP> 443 -persistenceType NONE
-cltTimeout 180



add lb vserver ADM-LB-SNMP UDP <EXTERNAL_VIP> 162 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-SYSLOG UDP <EXTERNAL_VIP> 514 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-DB_HA TCP <EXTERNAL_VIP> 5454 -persistenceType NONE
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-cltTimeout 9000



add lb vserver ADM-LB-LICENSE TCP <EXTERNAL_VIP> 27000 -persistenceType
NONE -cltTimeout 9000



add lb vserver ADM-LB-NTP UDP <EXTERNAL_VIP> 123 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-VENDOR-DEMON TCP <EXTERNAL_VIP> 7279
-persistenceType NONE -cltTimeout 9000
```

Ajouter des groupes de services

```
add serviceGroup ADM-SVCG-HTTP HTTP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-HTTPS SSL -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES

-cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO



add serviceGroup ADM-SVCG-SNMP UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-SYSLOG UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add serviceGroup ADM-SVCG-DB_HA TCP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-NTP UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-LICENSE TCP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-VENDOR-DEMON TCP -maxClient 0 -maxReq 0 -cip
DISABLED -usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA
NO -TCPB NO -CMP NO
```

Lier les serveurs virtuels d'équilibrage de charge aux groupes de services

```
bind lb vserver ADM-LB ADM-SVCG-HTTP



bind lb vserver ADM-LB-HTTPS ADM-SVCG-HTTPS



bind lb vserver ADM-LB-SNMP ADM-SVCG-SNMP



bind lb vserver ADM-LB-SYSLOG ADM-SVCG-SYSLOG



bind lb vserver ADM-LB-DB_HA ADM-SVCG-DB_HA
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind lb vserver ADM-LB-NTP ADM-SVCG-NTP

bind lb vserver ADM-LB-LICENSE ADM-SVCG-LICENSE

bind lb vserver ADM-LB-VENDOR-DEMON ADM-SVCG-VENDOR-DEMON
```

Lier les groupes de services aux nœuds NetScaler Console

```
bind serviceGroup ADM-SVCG-HTTP <PRIMARY_IP> 80

bind serviceGroup ADM-SVCG-HTTP <SECONDARY_IP> 80

bind serviceGroup ADM-SVCG-HTTPS <PRIMARY_IP> 443

bind serviceGroup ADM-SVCG-HTTPS <SECONDARY_IP> 443

bind serviceGroup ADM-SVCG-SNMP <PRIMARY_IP> 162

bind serviceGroup ADM-SVCG-SNMP <SECONDARY_IP> 162
```

Ajouter des moniteurs d'équilibrage de charge

```
add lb monitor monitor-snmp UDP-ECV -send "Udp data" -destPort 162
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add lb monitor monitor-syslog UDP-ECV -send "Udp data" -LRTM DISABLED
-destPort 514


add lb monitor monitor-db TCP-ECV -LRTM DISABLED -destPort 5454


add lb monitor monitor-ntp UDP-ECV -send "Udp data" -LRTM DISABLED
-destPort 123
```

Lier les moniteurs et les membres aux groupes de services

```
bind serviceGroup ADM-SVCG-SNMP -monitorName monitor-snmp


bind serviceGroup ADM-SVCG-SYSLOG <PRIMARY_IP> 514


bind serviceGroup ADM-SVCG-SYSLOG <SECONDARY_IP> 514


bind serviceGroup ADM-SVCG-SYSLOG -monitorName monitor-syslog


bind serviceGroup ADM-SVCG-DB_HA <PRIMARY_IP> 5454


bind serviceGroup ADM-SVCG-DB_HA <SECONDARY_IP> 5454


bind serviceGroup ADM-SVCG-DB_HA -monitorName monitor-db
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind serviceGroup ADM-SVCG-NTP <PRIMARY_IP> 123

bind serviceGroup ADM-SVCG-NTP <SECONDARY_IP> 123

bind serviceGroup ADM-SVCG-NTP -monitorName monitor-ntp

bind serviceGroup ADM-SVCG-LICENSE <PRIMARY_IP> 27000

bind serviceGroup ADM-SVCG-LICENSE <SECONDARY_IP> 27000

bind serviceGroup ADM-SVCG-VENDOR-DEMON <PRIMARY_IP> 7279

bind serviceGroup ADM-SVCG-VENDOR-DEMON <SECONDARY_IP> 7279
```

Activer les modes et mettre à jour les groupes de services

```
enable ns mode USIP

enable ns mode MBF

set serviceGroup ADM-SVCG-SYSLOG -usip YES

set serviceGroup ADM-SVCG-SNMP -usip YES
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Avantages

- **Déploiements flexibles et résilients** : Activez la haute disponibilité (HA) sur différents sous-réseaux ou centres de données, améliorant l'isolation des pannes et la disponibilité.
- **Alignement avec les architectures réseau modernes** : Prend en charge les environnements d'entreprise routés (L3) et segmentés sans les contraintes de la couche 2.
- **Tire parti de l'infrastructure existante** : S'intègre avec NetScaler ADC ou des équilibreurs de charge tiers pour une gestion du trafic évolutive et flexible.

Configurer la reprise après sinistre pour la haute disponibilité

Une catastrophe est une interruption soudaine des fonctions commerciales causée par des calamités naturelles ou des événements d'origine humaine. Les catastrophes affectent les opérations des centres de données, après quoi les ressources et les données perdues sur le site sinistré doivent être entièrement reconstruites et restaurées. La perte de données ou les temps d'arrêt dans le centre de données sont critiques et compromettent la continuité des activités.

La fonction de reprise après sinistre (DR) de NetScaler Console offre des capacités complètes de sauvegarde et de récupération du système pour NetScaler Console déployée en mode haute disponibilité. Au moment de la récupération, les certificats, les fichiers de configuration et une sauvegarde complète de la base de données sont disponibles sur le site de récupération.

Le tableau suivant décrit les termes utilisés lors de la configuration de la reprise après sinistre dans NetScaler Console.

TERMES	DESCRIPTION
Site principal (Centre de données A)	Le site principal dispose de nœuds NetScaler Console déployés en mode haute disponibilité.
Site de récupération (Centre de données B)	Le site de récupération dispose d'un nœud de reprise après sinistre déployé en mode autonome. Ce nœud est en mode lecture seule et n'est pas opérationnel tant que le site principal n'est pas hors service.
Nœud de reprise après sinistre	Le nœud de récupération est un nœud autonome déployé sur le site de récupération. Ce nœud est rendu opérationnel (pour devenir le nouveau primaire) en cas de catastrophe sur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TERMES	DESCRIPTION
	le site principal et si celui-ci est non fonctionnel.

REMARQUE

Le site principal et le site DR communiquent entre eux via les ports 5454 et 22, et ces ports sont activés par défaut.

Pour plus d'informations sur les détails des ports et des protocoles, consultez Ports.

Activer l'authentification de base

L'authentification de base doit être temporairement activée pour :

- Terminer l'enregistrement initial des agents et des nœuds de reprise après sinistre.
- Lancer le processus de validation du système d'activation de licence (LAS) à partir de l'interface graphique de NetScaler.

REMARQUE

L'authentification de base n'est requise que pour l'enregistrement initial.

Configurer l'authentification de base

1. Accédez à **Paramètres > Administration > Configurations système > Système, fuseau horaire, URL autorisées et paramètres de l'agent**.
2. Cliquez sur **Paramètres de base**.
3. Sélectionnez **Activer l'authentification de base**.
4. Cliquez sur **OK**.

REMARQUE

Activez l'option d'authentification de base avant que le site de reprise après sinistre ne soit configuré avec succès ; sinon, l'erreur suivante s'affiche :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`Not valid username/password or incorrect host IP, or the host is unable to respond to the request.`.

Flux de travail de reprise après sinistre

L'image suivante montre le flux de travail de reprise après sinistre, la configuration initiale avant le sinistre et le flux de travail après le sinistre.

Configuration initiale avant le sinistre



L'image montre la configuration de reprise après sinistre avant le sinistre.

Le site principal dispose de nœuds NetScaler Console déployés en mode haute disponibilité. Pour en savoir plus, consultez Déploiement haute disponibilité

Le site de récupération dispose d'un nœud de reprise après sinistre NetScaler Console autonome déployé à distance. Le nœud de reprise après sinistre est en mode lecture seule et reçoit des données du nœud principal pour créer une sauvegarde des données. Les instances NetScaler du site de récupération sont également découvertes, mais aucun trafic ne les traverse. Pendant le processus de sauvegarde, toutes les données, fichiers et configurations sont répliqués sur le nœud de reprise après sinistre à partir du nœud principal.

Prérequis

Avant de configurer le nœud de reprise après sinistre, notez les prérequis suivants :

- Pour activer les paramètres de reprise après sinistre, le site principal doit avoir des nœuds NetScaler Console configurés en mode haute disponibilité.
- La paire HA NetScaler Console (sur le site principal) et le nœud autonome (sur le site DR) doivent avoir la même version logicielle, la même build et les mêmes configurations.

Nous vous recommandons de définir la priorité du processeur (dans les propriétés de la machine virtuelle) au niveau le plus élevé afin d'améliorer le comportement de planification et la latence du réseau.

Le tableau suivant répertorie les exigences minimales pour configurer le nœud de reprise après sinistre :

COMPOSANT	EXIGENCE
RAM	32 Go

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANT	EXIGENCE
Processeur virtuel	8 processeurs
Espace de stockage	Nous recommandons l'utilisation de la technologie de disque SSD (Solid-State Drive) pour les déploiements de NetScaler Console. La valeur par défaut est de 120 Go. L'espace de stockage réel requis dépend de l'estimation du dimensionnement de NetScaler Console. Si votre besoin en stockage NetScaler Console dépasse 120 Go, vous devez attacher un disque supplémentaire. **Remarque** Vous ne pouvez ajouter qu'un seul disque supplémentaire. Nous vous recommandons d'estimer le stockage et d'attacher plus de disques au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à NetScaler Console.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Hyperviseur	**Versions**
Citrix Hypervisor	6.2 et 6.5
VMware ESXi	5.5 et 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu et Fedora

Configuration initiale de la reprise après sinistre

- Déployer NetScaler Console en mode haute disponibilité
- Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console
- Activer et désactiver les paramètres de reprise après sinistre depuis l'interface utilisateur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Déployer NetScaler Console en mode haute disponibilité

Pour configurer les paramètres de reprise après sinistre, assurez-vous que NetScaler Console est déployé en mode haute disponibilité. Pour plus d'informations sur le déploiement de NetScaler Console en haute disponibilité, consultez Déploiement en haute disponibilité

REMARQUE

- NetScaler Console déployé en mode haute disponibilité doit être mis à niveau vers la version 13.1 de NetScaler Console.
- **L'adresse IP flottante est obligatoire** pour enregistrer le nœud de reprise après sinistre auprès du nœud principal.

Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console à l'aide de la console DR

Pour enregistrer le nœud de reprise après sinistre de NetScaler Console :

1. Téléchargez le fichier image `.xva` depuis le site NetScaler et importez-le dans votre hyperviseur.
2. Depuis l'onglet **Console**, configurez NetScaler Console avec les configurations réseau initiales.

   REMARQUE

   Le nœud de reprise après sinistre peut se trouver sur un sous-réseau différent.

   
3. Une fois la configuration réseau initiale terminée, le système vous invite à vous connecter. Connectez-vous en utilisant les informations d'identification suivantes : `nsrecover` / `nsroot`.

   IMPORTANT

   Ne modifiez pas les informations d'identification du nœud DR (`nsrecover` / `nsroot`) pendant l'enregistrement. Vous pouvez modifier les informations d'identification du nœud DR après avoir enregistré le nœud DR avec succès.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Pour déployer le nœud de reprise après sinistre, tapez **/mps/deployment_type.py** et appuyez sur Entrée. Le menu de configuration du déploiement de NetScaler Console s'affiche.

   

5. Sélectionnez **2** pour enregistrer le nœud de reprise après sinistre.

   

6. La console demande l'adresse IP flottante du nœud haute disponibilité et le mot de passe.
7. Entrez l'adresse IP flottante et le mot de passe pour enregistrer le nœud de reprise après sinistre auprès du nœud principal.

   

   Le nœud de reprise après sinistre est maintenant enregistré avec succès.

   

   REMARQUE

   - Le nœud de reprise après sinistre n'a pas d'interface graphique.
   - Une fois l'enregistrement réussi, les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont `nsroot` / `nsroot`.

8. Si vous souhaitez modifier le mot de passe du nœud DR, exécutez le script suivant :

   ```
   /mps/change_freebsd_password.sh <username> <password>
   ```

   Exemple :

   ```
   /mps/change_freebsd_password.sh nsroot new_password
   ```

Déployer le nœud de reprise après sinistre à l'aide de l'interface graphique de NetScaler Console

Une fois le nœud de reprise après sinistre enregistré avec succès à l'aide de la console DR, déployez le nœud DR à partir de l'interface graphique de NetScaler Console. Cette étape active les paramètres de reprise après sinistre du site principal de NetScaler Console.

1. Accédez à **Système > Administration système > Paramètres de reprise après sinistre.**
2. Sur la page **Reprise après sinistre**, sélectionnez **Déployer le nœud DR**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

> **REMARQUE**
>
> Le temps nécessaire à la sauvegarde du système dépend de la taille des données et de la vitesse de la liaison WAN.

Après avoir déployé le nœud DR avec succès dans l'interface graphique de NetScaler Console, vous pouvez surveiller l'état de la base de données, la mémoire, le CPU et l'utilisation du disque du nœud DR.

Pour désactiver les paramètres de reprise après sinistre, sélectionnez **Supprimer le nœud DR**. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

Pour réactiver le nœud DR, reconfigurez le nœud DR pour votre paire haute disponibilité :

1. Connectez-vous au nœud DR à l'aide d'un hyperviseur ou d'une console SSH.
2. Configurez le nœud DR en suivant la procédure disponible à l'adresse Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console à l'aide de la console DR.
3. Déployer le nœud de reprise après sinistre à l'aide de l'interface graphique de NetScaler Console.

Pour plus d'informations, consultez la FAQ.

> **IMPORTANT**
>
> - Il incombe à l'administrateur de détecter qu'un sinistre s'est produit sur le site principal.
> - Le workflow de reprise après sinistre est initié manuellement par l'administrateur après la panne du site principal.
> - Un administrateur doit initier manuellement le processus en exécutant un script de récupération sur le nœud de reprise après sinistre sur le site de récupération.
> - Si vous mettez à niveau la paire HA sur le site principal, vous devez également mettre à niveau manuellement le nœud autonome sur le site DR.

Workflow après le sinistre

Lorsque le site principal tombe en panne après un sinistre, le workflow de reprise après sinistre doit être initié comme suit :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. L'administrateur identifie qu'un sinistre a frappé le site principal et qu'il n'est pas opérationnel.
2. L'administrateur initie le processus de récupération.
3. L'administrateur doit exécuter manuellement l'un des scripts de récupération suivants sur le nœud de reprise après sinistre en fonction de vos besoins (sur le site de récupération) :

   - Configurer SNMP, Syslog et Analytics sur le nœud DR :

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
     ```

   - Configurer également le nœud DR en tant que serveur de licences :

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -reconfig-ls
     <IP-address-of-the-primary-site>
     ```

4. En interne, les instances NetScaler sont automatiquement reconfigurées pour envoyer les données au nœud de reprise après sinistre qui est maintenant devenu le nouveau site principal.

   L'image suivante montre le flux de travail de reprise après sinistre après qu'une catastrophe a frappé le site principal.

   

   REMARQUE :

   Après avoir lancé le script sur le site DR, le site DR devient le nouveau site principal. Vous pouvez également accéder à l'interface utilisateur DR.

Après la reprise après sinistre

Une fois la catastrophe survenue et l'administrateur ayant lancé le script de récupération, le site DR devient le nouveau site principal.

Si vous souhaitez restaurer ultérieurement les configurations sur le site d'origine, consultez Restaurer les configurations sur le site principal d'origine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- Si vous avez installé NetScaler Console 12.1.49.x ou des versions antérieures, vous bénéficiez d'une période de grâce de 30 jours pour contacter Citrix afin de réhéberger la licence d'origine sur la NetScaler Console (sur le site DR).
- Pour les versions 12.1.50.x ou ultérieures, la licence NetScaler Console est automatiquement synchronisée avec le site DR (il n'est pas nécessaire de contacter Citrix pour la licence).
- Si vous avez appliqué des licences en pool pour les instances, les instances NetScaler avec la version **11.1 65.x ou ultérieure**, **12.1 58.x ou ultérieure**, **13.0 47.x ou ultérieure**, et NetScaler SDX **13.0 76.x ou ultérieure** prennent en charge la mise à jour automatique du serveur de licences sur le site DR. Pour toutes les autres versions, vous devez reconfigurer manuellement les instances sur le site DR.

Rétablir les configurations sur le site principal d'origine

Après la catastrophe, le nœud de reprise après sinistre (DR) configuré devient le nouveau site principal et le trafic client transite par ce nœud.

Pour plus d'informations, consultez Flux de travail après la catastrophe.

Lorsque votre site principal d'origine est exempt de sinistre et que vous décidez de déplacer toutes les opérations vers le site principal, reconfigurez le site principal d'origine pour qu'il corresponde aux configurations du nœud DR.

Avant de commencer, assurez-vous que le site principal et le site DR sont tous deux actifs.

Pour rétablir les modifications sur le site principal d'origine à partir du site DR, effectuez les étapes suivantes :

1. Connectez-vous au site principal d'origine et exécutez la commande suivante :

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
   ```

   Cette commande configure uniquement Syslog, SNMP et Analytics sur le site principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si vous souhaitez configurer le site principal en tant que serveur de licences en pool pour les instances NetScaler, exécutez la commande suivante :

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
```

La commande `-O` récupère l'adresse IP du site DR et reconfigure le site principal en tant que serveur de licences en pool.

2. Reconfigurez le site DR. Voir, Déployer la configuration de reprise après sinistre.

Une fois que vous avez rétabli les configurations du site DR vers le site principal d'origine, le trafic client transite par le nœud principal de NetScaler Console.

Configurer la reprise après sinistre pour un nœud autonome

Vous pouvez également configurer une reprise après sinistre pour NetScaler Console déployé en mode autonome.

Le tableau suivant décrit les termes utilisés lors de la configuration de la reprise après sinistre dans NetScaler Console.

TERMES	DESCRIPTION
Site principal (centre de données A)	Le site principal dispose d'un nœud NetScaler Console déployé en mode autonome.
Site de récupération (centre de données B)	Le site de récupération dispose d'un nœud de reprise après sinistre déployé en mode autonome. Ce nœud est en mode lecture seule et n'est pas opérationnel tant que le site principal n'est pas hors service.
Nœud de reprise après sinistre	Le nœud de récupération est un nœud autonome déployé sur le site de récupération. Ce nœud est rendu opérationnel (pour devenir le nouveau nœud principal) en cas de sinistre sur le site principal et si celui-ci est non fonctionnel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Le site principal et le site de reprise après sinistre communiquent entre eux via les ports 5454 et 22, et ces ports sont activés par défaut.

Pour plus d'informations sur les détails des ports et des protocoles, consultez Ports.

Flux de travail de reprise après sinistre

Le site principal dispose d'un nœud NetScaler Console déployé en mode autonome.

Le site de récupération dispose d'un nœud de reprise après sinistre déployé à distance. Le nœud de reprise après sinistre est en mode lecture seule et reçoit des données du nœud principal pour créer une sauvegarde des données. Les instances NetScaler du site de récupération sont également découvertes, mais aucun trafic ne les traverse. Pendant le processus de sauvegarde, toutes les données, fichiers et configurations sont répliqués sur le nœud de reprise après sinistre à partir du nœud principal.

Conditions préalables

Avant de configurer le nœud de reprise après sinistre, notez les conditions préalables suivantes :

- Pour activer les paramètres de reprise après sinistre, le site principal doit avoir NetScaler Console configuré en mode autonome.
- Le NetScaler Console autonome (sur le site principal) et le nœud de reprise après sinistre (sur le site DR) doivent avoir la même version logicielle, la même build et les mêmes configurations.

Nous vous recommandons de définir la priorité du CPU (dans les propriétés de la machine virtuelle) au niveau le plus élevé pour améliorer le comportement de planification et la latence du réseau.

Le tableau suivant répertorie les exigences minimales pour configurer le nœud de reprise après sinistre :

COMPOSANT	EXIGENCE
RAM	32 Go
CPU virtuel	8 CPU
Espace de stockage	Nous recommandons d'utiliser la technologie de disque SSD (Solid-State Drive) pour les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANT	EXIGENCE
	déploiements NetScaler Console. La valeur par défaut est de 120 Go. L'exigence de stockage réelle dépend de l'estimation du dimensionnement de NetScaler Console. Si votre exigence de stockage NetScaler Console dépasse 120 Go, vous devez attacher un disque supplémentaire. **Remarque** Vous ne pouvez ajouter qu'un seul disque supplémentaire. Nous vous recommandons d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à NetScaler Console.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Hyperviseur	**Versions**
Citrix Hypervisor	6.2 et 6.5
VMware ESXi	5.5 et 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu et Fedora

Configuration initiale de la reprise après sinistre

- Déployer NetScaler Console
- Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console
- Activer et désactiver les paramètres de reprise après sinistre depuis l'interface utilisateur

Déployer NetScaler Console

Pour configurer les paramètres de reprise après sinistre, assurez-vous que NetScaler Console est déployé en mode autonome. Pour plus d'informations, consultez déploiement sur un seul serveur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console à l'aide de la console DR

Pour enregistrer le nœud de reprise après sinistre de NetScaler Console :

1. Téléchargez le fichier image `.xva` depuis le site NetScaler et importez-le dans votre hyperviseur.
2. Depuis l'onglet **Console**, configurez NetScaler Console avec les configurations réseau initiales.

   REMARQUE

   Le nœud de reprise après sinistre peut se trouver sur un sous-réseau différent.

   
3. Une fois la configuration réseau initiale terminée, le système vous invite à vous connecter. Connectez-vous en utilisant les informations d'identification suivantes – `nsrecover` / `nsroot`.

   IMPORTANT

   Ne modifiez pas les informations d'identification du nœud DR (`nsrecover` / `nsroot`) pendant l'enregistrement. Vous pouvez modifier les informations d'identification du nœud DR après avoir enregistré le nœud DR avec succès.
4. Pour déployer le nœud de reprise après sinistre, tapez **/mps/deployment_type.py** et appuyez sur Entrée. Le menu de configuration du déploiement de NetScaler Console s'affiche.

   
5. Sélectionnez **2** pour enregistrer le nœud de reprise après sinistre.

   
6. La console vous invite à saisir l'adresse IP et le mot de passe du nœud autonome.
7. Saisissez l'adresse IP et le mot de passe du nœud autonome pour enregistrer le nœud de reprise après sinistre.

   Le nœud de reprise après sinistre est maintenant enregistré avec succès.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Le nœud de reprise après sinistre n'a pas d'interface graphique.
- Une fois l'enregistrement réussi, les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont `nsroot` / `nsroot`.

8. Si vous souhaitez modifier le mot de passe du nœud DR, exécutez le script suivant :

```
/mps/change_freebsd_password.sh <username> <password>
```

Exemple :

```
/mps/change_freebsd_password.sh nsroot new_password
```

Déployer le nœud de reprise après sinistre à l'aide de l'interface graphique de NetScaler Console

Après que le nœud de reprise après sinistre est enregistré avec succès à l'aide de la console DR, déployez le nœud DR à partir de l'interface graphique de NetScaler Console. Cette étape active les paramètres de reprise après sinistre à partir du site principal de NetScaler Console.

1. Accédez à **Système \> Administration système \> Paramètres de reprise après sinistre.**
2. Sur la page **Reprise après sinistre**, sélectionnez **Déployer le nœud DR**.
3. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

REMARQUE

Le temps nécessaire à la sauvegarde du système dépend de la taille des données et de la vitesse de la liaison WAN.

Après avoir déployé le nœud DR avec succès dans l'interface graphique de NetScaler Console, vous pouvez surveiller l'état de la base de données, la mémoire, le CPU et l'utilisation du disque du nœud DR.

Pour désactiver les paramètres de reprise après sinistre, sélectionnez **Supprimer le nœud DR**. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour réactiver le nœud DR, reconfigurez le nœud DR pour votre paire haute disponibilité :

1. Connectez-vous au nœud DR à l'aide d'un hyperviseur ou d'une console SSH.
2. Configurez le nœud DR en suivant la procédure disponible à l'adresse Déployer et enregistrer le nœud de reprise après sinistre de NetScaler Console à l'aide de la console DR.
3. Déployez le nœud de reprise après sinistre à l'aide de l'interface graphique de NetScaler Console.

Pour plus d'informations, consultez la FAQ.

IMPORTANT

- Il incombe à l'administrateur de détecter qu'un sinistre s'est produit sur le site principal.
- Le flux de travail de reprise après sinistre est initié manuellement par l'administrateur après la panne du site principal.
- Un administrateur doit initier manuellement le processus en exécutant un script de récupération sur le nœud de reprise après sinistre du site de récupération.
- Si vous mettez à niveau le nœud autonome sur le site principal, vous devez également mettre à niveau manuellement le nœud autonome sur le site de DR.

Flux de travail après le sinistre

Lorsque le site principal tombe en panne après un sinistre, le flux de travail de reprise après sinistre doit être initié comme suit :

1. L'administrateur identifie qu'un sinistre a frappé le site principal et que celui-ci n'est pas opérationnel.
2. L'administrateur initie le processus de récupération.
3. L'administrateur doit exécuter manuellement l'un des scripts de récupération suivants sur le nœud de reprise après sinistre en fonction de vos besoins (sur le site de récupération) :
   - Configurer SNMP, Syslog et Analytics sur le nœud DR :

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
     ```

   - Configurer également le nœud DR en tant que serveur de licences :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
/mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -reconfig-ls
<IP-address-of-the-primary-site>
```

4. En interne, les instances NetScaler sont automatiquement reconfigurées pour envoyer les données au nœud de reprise après sinistre qui est désormais devenu le nouveau site principal.

REMARQUE :

Après avoir initié le script sur le site de DR, le site de DR devient le nouveau site principal. Vous pouvez également accéder à l'interface utilisateur de DR.

Après la reprise après sinistre

Une fois le sinistre survenu et l'administrateur ayant initié le script de récupération, le site de DR devient le nouveau site principal.

Si vous souhaitez restaurer les configurations sur le site d'origine ultérieurement, consultez Restaurer les configurations sur le site principal d'origine.

IMPORTANT

- Si vous avez installé NetScaler Console 12.1.49.x ou des versions antérieures, vous bénéficiez d'une période de grâce de 30 jours pour contacter Citrix afin de réhéberger la licence d'origine sur NetScaler Console (sur le site de reprise après sinistre).
- Pour les versions 12.1.50.x ou ultérieures, la licence NetScaler Console est automatiquement synchronisée avec le site de reprise après sinistre (il n'est pas nécessaire de contacter Citrix pour la licence).
- Si vous avez appliqué des licences en pool pour les instances, les instances NetScaler avec la version **11.1 65.x ou ultérieure**, **12.1 58.x ou ultérieure**, **13.0 47.x ou ultérieure**, et NetScaler SDX **13.0 76.x ou ultérieure** prennent en charge la mise à jour automatique du serveur de licences sur le site de reprise après sinistre. Pour toutes les autres versions, vous devez reconfigurer manuellement les instances sur le site de reprise après sinistre.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Restaurer les configurations sur le site principal d'origine

Après un sinistre, le nœud de reprise après sinistre (DR) configuré devient le nouveau site principal et le trafic client transite par ce nœud.

Pour plus d'informations, consultez Flux de travail après le sinistre.

Lorsque votre site principal d'origine est exempt de sinistre et que vous décidez de déplacer toutes les opérations vers le site principal, reconfigurez le site principal d'origine pour qu'il corresponde aux configurations du nœud de reprise après sinistre.

Avant de commencer, assurez-vous que le site principal et le site de reprise après sinistre sont tous deux actifs.

Pour restaurer les modifications sur le site principal d'origine à partir du site de reprise après sinistre, effectuez les étapes suivantes :

1. Connectez-vous au site principal d'origine et exécutez la commande suivante :

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
   password> -L <primary-node-password> &
   ```

   Cette commande configure uniquement Syslog, SNMP et Analytics sur le site principal.

   Si vous souhaitez configurer le site principal en tant que serveur de licences en pool pour les instances NetScaler, exécutez la commande suivante :

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
   password> -L <primary-node-password>  -O yes &
   ```

   La commande `-O` récupère l'adresse IP du site de reprise après sinistre et reconfigure le site principal en tant que serveur de licences en pool.

2. Reconfigurez le site de reprise après sinistre. Voir, Déployer la configuration de reprise après sinistre.

Une fois que vous avez réussi à restaurer les configurations du site de reprise après sinistre vers le site principal d'origine, le trafic client transite par le nœud principal de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer les agents sur site pour un déploiement multisite

Dans les versions précédentes de NetScaler Console, les instances NetScaler déployées dans des centres de données distants pouvaient être gérées et surveillées depuis NetScaler Console exécutée dans un centre de données principal. Les instances NetScaler envoyaient les données directement à la NetScaler Console principale, ce qui entraînait une consommation de bande passante WAN. De plus, le traitement des données analytiques utilisait les ressources CPU et mémoire de la NetScaler Console principale.

Vous pouvez avoir des centres de données situés partout dans le monde. Les agents jouent un rôle essentiel dans les scénarios suivants :

- Installer des agents dans des centres de données distants afin de réduire la consommation de bande passante WAN.
- Limiter le nombre d'instances envoyant directement du trafic à la NetScaler Console principale pour le traitement des données.

REMARQUE

- L'installation d'agents pour les instances dans un centre de données distant est recommandée mais non obligatoire. Si nécessaire, les utilisateurs peuvent ajouter directement des instances NetScaler à la NetScaler Console principale.
- Si vous avez installé des agents pour un ou plusieurs centres de données distants, la communication entre les agents et le site principal s'effectue via une adresse IP flottante. Pour plus d'informations, consultez port.
- Vous pouvez installer des agents et appliquer des licences en pool aux instances dans un ou plusieurs centres de données distants. Dans ce scénario, la communication entre le site principal et un ou plusieurs centres de données distants s'effectue via l'adresse IP flottante.
- L'agent NetScaler Console sur site ne prend pas en charge les licences en pool.

À partir de NetScaler Console 12.1 ou version ultérieure, les instances peuvent être configurées avec des agents pour communiquer avec la NetScaler Console principale située dans un centre de données différent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les agents fonctionnent comme un intermédiaire entre la NetScaler Console principale et les instances découvertes dans différents centres de données. Voici les avantages de l'installation d'agents :

- Les instances sont configurées pour les agents afin que les données non traitées soient envoyées directement aux agents au lieu de la NetScaler Console principale. Les agents effectuent le premier niveau de traitement des données et envoient les données traitées au format compressé à la NetScaler Console principale pour stockage.
- Les agents et les instances sont colocalisés dans le même centre de données afin que le traitement des données soit plus rapide.
- Le clustering des agents permet la redistribution des instances NetScaler en cas de défaillance d'un agent. Lorsqu'un agent d'un site tombe en panne, le trafic des instances NetScaler est basculé vers un autre agent disponible sur le même site.

REMARQUE

Le nombre d'agents à installer par site dépend du trafic traité.

Architecture

La figure suivante montre des instances NetScaler dans deux centres de données et un déploiement de NetScaler Console en haute disponibilité utilisant une architecture multisite basée sur des agents.



Le site principal dispose des nœuds NetScaler Console déployés dans une configuration de haute disponibilité. Les instances NetScaler du site principal sont directement enregistrées auprès de NetScaler Console.

Dans le site secondaire, des agents sont déployés et enregistrés auprès du serveur NetScaler Console du site principal. Ces agents fonctionnent en cluster pour gérer un flux de trafic continu en cas de basculement d'un agent. Les instances NetScaler du site secondaire sont enregistrées auprès du serveur NetScaler Console principal via des agents situés sur ce site. Les instances envoient les données directement aux agents au lieu de les envoyer à la NetScaler Console principale. Les agents traitent les données reçues des instances et les envoient à la NetScaler Console principale dans un format compressé. Les agents communiquent avec le serveur NetScaler Console via un canal sécurisé et les données envoyées via ce canal sont compressées pour une meilleure efficacité de la bande passante.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activer l'authentification de base

L'authentification de base doit être temporairement activée pour :

- Terminer l'enregistrement initial des agents et des nœuds de reprise après sinistre.
- Lancer l'extraction du système d'activation de licence (LAS) depuis l'interface graphique de NetScaler.

REMARQUE :

L'authentification de base n'est requise que pour l'enregistrement initial.

Configurer l'authentification de base

1. Accédez à **Paramètres > Administration > Configurations système > Système, fuseau horaire, URL autorisées et paramètres de l'agent**.
2. Cliquez sur **Paramètres de base**.
3. Sélectionnez **Activer l'authentification de base**.
4. Cliquez sur **OK**.

Pour commencer

- Installer l'agent dans un centre de données
  - Enregistrer l'agent
  - Associer l'agent à un site
- Ajouter des instances NetScaler
  - Ajouter une nouvelle instance
  - Mettre à jour une instance existante

Installer l'agent dans un centre de données

Vous pouvez installer et configurer l'agent pour permettre la communication entre la console NetScaler principale et les instances NetScaler gérées dans un autre centre de données.

Vous pouvez installer un agent sur les hyperviseurs suivants dans votre centre de données d'entreprise :

- Citrix Hypervisor™

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VMware ESXi
- Microsoft Hyper-V
- Serveur Linux KVM

REMARQUE

Les agents sur site pour le déploiement multisite sont pris en charge uniquement avec le déploiement haute disponibilité de NetScaler Console.

Avant de commencer l'installation de l'agent, assurez-vous de disposer des ressources informatiques virtuelles requises que l'hyperviseur doit fournir pour chaque agent.

COMPOSANT	EXIGENCE
RAM	32 Go
CPU virtuel	8 CPU
Espace de stockage	30 Go
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

Ports

Pour la communication, les ports suivants doivent être ouverts entre l'agent et le serveur NetScaler Console sur site.

TYPE	PORT	DÉTAILS	SENS DE LA COMMUNICATION
TCP	8443, 7443, 443	Pour la communication sortante et entrante entre l'agent et le serveur NetScaler Console sur site.	Agent NetScaler vers NetScaler Console

Les ports suivants doivent être ouverts entre l'agent et les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	PORT	DÉTAILS	SENS DE LA COMMUNICATION
TCP	80	Pour la communication NITRO entre l'agent et l'instance NetScaler.	De NetScaler Console à NetScaler et de NetScaler à NetScaler Console
TCP	22	Pour la communication SSH entre l'agent et l'instance NetScaler. Pour la synchronisation entre les serveurs NetScaler Console déployés en mode haute disponibilité.	De NetScaler Console à NetScaler et de l'agent NetScaler à NetScaler
UDP	4739	Pour la communication AppFlow entre l'agent et l'instance NetScaler.	De NetScaler à NetScaler Console
ICMP	Aucun port réservé	Pour détecter l'accessibilité réseau entre NetScaler Console et les instances NetScaler, ou le serveur NetScaler Console secondaire déployé en mode haute disponibilité.	
UDP	161, 162	Pour recevoir les événements SNMP de l'instance NetScaler vers l'agent.	Port 161 - De NetScaler Console vers NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TYPE	PORT	DÉTAILS	SENS DE LA COMMUNICATION
			Port 162 - De NetScaler vers NetScaler Console
UDP	514	Pour recevoir les messages syslog de l'instance NetScaler vers l'agent.	De NetScaler vers NetScaler Console
TCP	5557	Pour la communication Logstream entre l'agent et les instances NetScaler.	De NetScaler vers NetScaler Console

Enregistrer l'agent

1. Utilisez le fichier image de l'agent téléchargé depuis le site NetScaler et importez-le dans votre hyperviseur. Le modèle de nommage du fichier image de l'agent est le suivant : **MASAGENT-\<HYPERVISOR\>-\<Version.no\>.** Par exemple : **MASAGENT-XEN-13.0-xy.xva**
2. Depuis l'onglet **Console**, configurez NetScaler Console avec les configurations réseau initiales.
3. Saisissez le nom d'hôte de NetScaler Console, l'adresse IPv4 et l'adresse IPv4 de la passerelle. Sélectionnez l'option 7 pour enregistrer et quitter la configuration.

   
4. Une fois l'enregistrement réussi, la console vous invite à vous connecter. Utilisez *nsrecover/ nsroot* comme identifiants.
5. Pour enregistrer l'agent, saisissez **/mps/register_agent_onprem.py**. Les identifiants d'enregistrement de l'agent NetScaler s'affichent comme illustré dans l'image suivante.
6. Saisissez l'adresse IP flottante de NetScaler Console et les identifiants de l'utilisateur.

   

Une fois l'enregistrement réussi, l'agent redémarre pour terminer le processus d'installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après le redémarrage de l'agent, accédez à l'interface graphique de NetScaler Console, depuis le menu principal, allez à la page **Infrastructure > Instances > Agents** pour vérifier l'état de l'agent. L'agent nouvellement ajouté s'affiche à l'état **Actif**.

REMARQUE

NetScaler Console affiche la version de l'agent et vérifie également si l'agent est à la dernière version. L'icône de téléchargement indique que l'agent n'est pas à la dernière version et doit être mis à niveau. Nous vous recommandons de mettre à niveau la version de l'agent vers la version de NetScaler Console.

Attacher un agent à un site

1. Sélectionnez l'agent et cliquez sur **Attacher le site.**
2. Dans la page **Attacher un site**, sélectionnez un site dans la liste ou créez un site à l'aide du bouton plus (+).
3. Cliquez sur **Enregistrer.**

REMARQUE

- Par défaut, tous les agents nouvellement enregistrés sont ajoutés au centre de données par défaut.
- Il est important d'associer l'agent au site correct. En cas de défaillance d'un agent, les instances NetScaler qui lui sont attribuées sont automatiquement basculées vers d'autres agents fonctionnels du même site.

Actions de l'agent

Vous pouvez appliquer diverses actions à un agent sous **Infrastructure > Agents > Sélectionner des actions**.

Sous **Sélectionner une action**, vous pouvez utiliser les fonctionnalités suivantes :

Installer un nouveau certificat : si vous avez besoin d'un certificat d'agent différent pour répondre à vos exigences de sécurité, vous pouvez en ajouter un.

Modifier le mot de passe par défaut : pour assurer la sécurité de votre infrastructure, modifiez le mot de passe par défaut d'un agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Générer un fichier de support technique : générez un fichier de support technique pour un agent NetScaler sélectionné. Vous pouvez télécharger ce fichier et l'envoyer au support technique de Citrix pour investigation et dépannage.

Ajouter des instances NetScaler

Les instances sont des appliances NetScaler ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller depuis NetScaler Console via des agents. Vous pouvez ajouter les appliances NetScaler et les appliances virtuelles suivantes à NetScaler Console ou aux agents :

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Citrix SSL Forward Proxy

Pour plus d'informations, consultez Ajouter des instances à NetScaler Console.

Attacher une instance existante à l'agent

Si une instance est déjà ajoutée à la console NetScaler principale, vous pouvez l'associer à un agent en modifiant un agent.

1. Accédez à **Infrastructure > Instances** et sélectionnez le type d'instance. Par exemple, NetScaler.
2. Cliquez sur **Modifier** pour modifier une instance existante.
3. Cliquez pour sélectionner l'agent.
4. Depuis la page **Agent**, sélectionnez l'agent auquel vous souhaitez associer l'instance, puis cliquez sur **OK**.

REMARQUE

Assurez-vous de sélectionner le **Site** auquel vous souhaitez associer l'instance.

Accéder à l'interface graphique d'une instance pour valider les événements

Une fois les instances ajoutées et l'agent configuré, accédez à l'interface graphique d'une instance pour vérifier si la destination du piège est configurée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans NetScaler Console, accédez à **Infrastructure > Instances**. Sous **Instances**, sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, NetScaler VPX), puis cliquez sur l'adresse IP d'une instance spécifique.

L'interface graphique de l'instance sélectionnée s'affiche dans une fenêtre contextuelle.

Par défaut, l'agent est configuré comme destination de trap sur l'instance. Pour confirmer, connectez-vous à l'interface graphique de l'instance et vérifiez les destinations de trap.

IMPORTANT

L'ajout d'un agent pour les instances NetScaler dans les centres de données distants est recommandé mais non obligatoire.

Si vous souhaitez ajouter l'instance directement au MAS principal, ne sélectionnez pas **d'agent** lors de l'ajout d'instances.

Basculement de l'agent NetScaler

Le basculement de l'agent peut se produire sur un site comportant au moins deux agents enregistrés. Lorsqu'un agent devient inactif (état DOWN) sur le site, NetScaler Console redistribue les instances NetScaler de l'agent inactif vers d'autres agents actifs.

IMPORTANT

- Assurez-vous que la fonctionnalité **Basculement de l'agent** est activée sur votre compte. Pour activer cette fonctionnalité, consultez Activer ou désactiver les fonctionnalités de NetScaler Console.
- Si un agent exécute un script, assurez-vous que ce script est présent sur tous les agents du site. Ainsi, l'agent modifié peut exécuter le script après le basculement de l'agent.

Pour associer un site à un agent dans l'interface graphique de NetScaler Console, consultez Associer un agent à un site.

Pour réaliser un basculement d'agent, sélectionnez les agents NetScaler un par un et associez-les au même site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Par exemple, deux agents 10.106.1xx.2x et 10.106.1xx.3x sont attachés et opérationnels sur le site de Bangalore. Si un agent devient inactif, NetScaler Console le détecte et affiche l'état comme étant « down ».

Lorsqu'un agent NetScaler devient inactif (état « Down ») sur un site, NetScaler Console attend cinq minutes que l'agent redevienne actif (état « Up »). Si l'agent reste inactif, NetScaler Console redistribue automatiquement les instances parmi les agents disponibles sur le même site.

NetScaler Console déclenche la redistribution des instances toutes les 30 minutes pour équilibrer la charge entre les agents actifs du site.

Configurer le seuil d'inaccessibilité de l'agent et la notification

Si un agent est hors service ou inaccessible pendant une certaine durée, vous pouvez recevoir une notification sur l'état de l'agent par e-mail, Slack, PagerDuty et ServiceNow. Dans **Infrastructure > Instances > Agents**, cliquez sur **Paramètres**, spécifiez la durée entre 5 et 60 minutes, et sélectionnez la méthode de notification que vous souhaitez utiliser.



Communication sécurisée entre les agents NetScaler® Console et NetScaler Console

Une communication sécurisée entre les agents NetScaler Console et NetScaler Console est disponible pour les versions 14.1-34.x ou ultérieures. Vous pouvez activer cette communication sécurisée en vérifiant le certificat SSL du serveur Console. Auparavant, la communication entre les agents NetScaler Console et le serveur NetScaler Console sur site ne vérifiait pas le certificat SSL du serveur Console, ce qui entraînait des vulnérabilités de sécurité potentielles.

Pour activer cette communication sécurisée :

1. Assurez-vous que la NetScaler Console a des certificats SSL configurés.
2. Connectez-vous à l'agent NetScaler Console.
3. Placez le certificat racine de l'autorité de certification à l'emplacement **/mpsconfig/console_onprem_cacert**. Il est utilisé pour valider le certificat du serveur. Le nom du certificat racine de l'autorité de certification doit être **cacert.pem**.
4. Configurez la communication sécurisée en exécutant la commande suivante. **Configure_secure_communication_with_server.py**
5. Cela demande le FQDN (nom de domaine complet) ou l'adresse IP du serveur NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Saisissez le FQDN ou l'adresse IP pour terminer l'exécution du script.

   

7. Le script vérifie le certificat du serveur présenté par un FQDN ou une adresse IP, en utilisant le certificat racine de l'autorité de certification fourni. La communication sécurisée est activée si la validation du certificat réussit.
8. Ce script peut être invoqué avant ou après l'enregistrement de l'agent auprès de la console NetScaler.

REMARQUE :

Ceci s'applique uniquement aux agents basés sur des machines virtuelles.

Installer un agent NetScaler® en tant que microservice sur un cluster Kubernetes

Si vous utilisez NetScaler Console sur site, l'agent conteneur est utilisé pour plusieurs raisons stratégiques et techniques spécifiques. Voici quelques-unes des raisons importantes :

- **Gestion transparente des charges de travail natives du cloud** - La principale raison d'utiliser l'agent conteneur est de gérer NetScaler CPX (la version conteneurisée de NetScaler).
- **Contrôle localisé** : L'agent agit comme un proxy de licence entre votre console sur site et les instances NetScaler CPX exécutées au sein d'un cluster Kubernetes.
- **Connectivité simplifiée (architecture de microservices)** - Si votre NetScaler Console et votre cluster Kubernetes se trouvent sur des réseaux différents, l'agent conteneur agit comme une passerelle sécurisée « intra-cluster ».

REMARQUES :

- Vous pouvez également configurer un agent sur site et enregistrer l'agent sur le réseau où le cluster Kubernetes est hébergé.
- À partir de la version 14.1 build 60.x de NetScaler Console, NetScaler Console prend en charge l'utilisation d'un agent de console conteneurisé. L'utilisation d'un agent de console conteneurisé offre une connectivité et une surveillance simplifiées des instances gérées sur les plateformes Kubernetes ou OpenShift.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Démarrage

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > Agents**.
2. Dans la liste **Sélectionner une action**, sélectionnez l'option **Télécharger le microservice d'agent**.
3. Dans la page **Télécharger le microservice d'agent**, spécifiez les paramètres suivants :
   - **ID d'application** – Un identifiant de chaîne pour définir le service de l'agent dans le cluster Kubernetes et distinguer cet agent des autres agents du même cluster.
   - **Mot de passe** – Spécifiez un mot de passe pour que NetScaler CPX utilise ce mot de passe pour intégrer NetScaler CPX à NetScaler Console via l'agent.
   - **Confirmer le mot de passe** – Spécifiez le même mot de passe pour confirmation.

     REMARQUE :

     - Vous ne devez pas utiliser le mot de passe par défaut (`nsroot`).
4. Cliquez sur **Télécharger le fichier YAML**.

Installer l'agent NetScaler dans le cluster Kubernetes

Effectuez les étapes suivantes sur le nœud principal Kubernetes :

1. Enregistrez le fichier YAML téléchargé.
2. Exécutez la commande suivante :

   ```
   kubectl create -f <yaml file>
   ```

   Exemple :

   ```
   kubectl create -f onprem6540.yaml
   ```

L'agent est créé avec succès.

☐ Dans NetScaler Console, accédez à **Infrastructure > Instances > Agents** pour afficher l'état de l'agent.

☐

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir configuré l'agent, vous pouvez ajouter les instances NetScaler CPX et afficher les analyses dans le graphique de service. Pour plus d'informations, consultez :

- Ajout d'instances NetScaler NetScaler CPX à NetScaler Console
- Configuration du graphique de service

Installer un opérateur OpenShift d'agent NetScaler Console pour le déploiement sur site de NetScaler Console

Si vous utilisez NetScaler Console sur site, l'agent conteneur est utilisé pour plusieurs raisons stratégiques et techniques spécifiques. Voici quelques-unes des raisons importantes :

- **Gestion transparente des charges de travail cloud-native** - La principale raison d'utiliser l'agent conteneur est de gérer NetScaler CPX (la version conteneurisée de NetScaler).
- **Contrôle localisé** - L'agent agit comme un proxy de licence entre votre NetScaler Console sur site et les instances NetScaler CPX exécutées au sein d'un cluster Kubernetes.
- **Connectivité simplifiée (architecture de microservices)** - Si votre NetScaler Console et votre cluster Kubernetes se trouvent sur des réseaux différents, l'agent conteneur agit comme une passerelle sécurisée "intra-cluster".

REMARQUE :

L'agent NetScaler Console est pris en charge pour les déploiements sur site de NetScaler Console à partir de NetScaler Console sur site 14.1.60.x.

Un opérateur est une boîte à outils open source qui vous permet de déployer et de gérer les applications Kubernetes de manière efficace, automatisée et évolutive. En tant qu'administrateur, vous pouvez déployer un agent dans le cluster OpenShift à l'aide de l'**opérateur d'agent NetScaler® ADM**.

REMARQUE :

Un agent configuré dans le cluster OpenShift n'est pas automatiquement mis à niveau par défaut.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prérequis

Avant de déployer, assurez-vous que :

- Vous disposez des contraintes de contexte de sécurité privilégiées pour contrôler les autorisations des pods. Pour l'agent, exécutez la commande suivante pour obtenir les contraintes de contexte de sécurité privilégiées pour le compte de service :

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- Exécutez la commande suivante pour créer un secret de connexion d'agent (`loginsecret`) :

  ```
  oc create secret generic admlogin --from-literal=username=nsroot --
  from-literal=password=<NetScaler Console-agent-password> -n <namespace>
  ```

- Exécutez la commande suivante pour créer un secret pour le serveur NetScaler Console (secret `accessSecret`) :

  ```
  oc create secret generic testonprem--from-literal=username=nsroot --
  from-literal=password=< NetScaler Console password> -n <namespace>
  ```

Installer l'opérateur d'agent

1. Connectez-vous à la console du cluster OpenShift.
2. Accédez à **Operators > OperatorHub**.
3. Dans la barre de recherche, indiquez le nom de l'agent, sélectionnez l'**opérateur d'agent NetScaler ADM**, puis cliquez sur **Installer**.

   

4. Dans la page **Installer l'opérateur**, vous avez deux options :

   a. **Tous les espaces de noms sur le cluster (par défaut)** - Permet à l'opérateur d'agent de s'abonner à tous les espaces de noms disponibles dans le cluster et vous permet d'initialiser l'instance de l'opérateur d'agent à partir de n'importe quel espace de noms sur le cluster.

   b. **Un espace de noms spécifique sur le cluster** - Permet à l'opérateur d'agent de s'abonner à un espace de noms sélectionné sur le cluster et vous ne pouvez initialiser l'instance de l'opérateur d'agent qu'à partir de l'espace de noms sélectionné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, l'opérateur d'agent est affecté à un espace de noms appelé **Default**. Sélectionnez **Automatique** sous **Approbation de la mise à jour**, puis cliquez sur **Installer**.

Attendez que l'opérateur d'agent soit abonné avec succès.

5. Accédez à **Charges de travail > Pods** et vérifiez que le pod `netscaler-adm-agent-operator-controller` est opérationnel.
6. Une fois le pod opérationnel, vous devez voir deux instances pour l'agent Console dans l'**opérateur d'agent NetScaler ADM**. Cliquez sur **Opérateur d'agent NetScaler ADM sur site** pour déployer l'agent.



7. Sélectionnez la **vue YAML** pour mettre à jour les paramètres, puis cliquez sur **Créer**.

   REMARQUE :

   Assurez-vous qu'il n'y a qu'une seule instance d'agent par cluster OpenShift.

   Les trois paramètres suivants sont obligatoires :

   - `accessSecret` : Le secret nommé `testonprem` est créé.
   - `AdmURL` : L'adresse IP de NetScaler Console.
   - `loginsecret` : Le secret nommé `admlogin` est créé.



8. Accédez à **Charges de travail > Pods** et assurez-vous que les pods de l'agent sont opérationnels.



Supprimer une instance d'agent

Vous pouvez supprimer l'instance de l'agent du cluster en accédant à **Operators > Installed Operators**. Dans l'onglet **NetScaler ADM Agent Operator**, sélectionnez l'instance, puis sélectionnez **Delete AdmAgentOnPrems** dans la liste.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Désinstaller l'opérateur d'agent

Si vous souhaitez désinstaller le pod de l'opérateur d'agent du cluster, accédez à **Opérateurs > Opérateurs installés**, puis sélectionnez **Désinstaller l'opérateur** dans la liste.



Mettre à niveau les agents

REMARQUE :

Assurez-vous que la version de l'agent est 14.1-38.x ou ultérieure.

À partir de la version 14.1–43.50, vous pouvez mettre à niveau les agents NetScaler (14.1-38.x ou version ultérieure) via l'interface graphique de NetScaler Console. Cette amélioration élimine le processus de mise à niveau manuel pour chaque agent et vous permet de mettre à niveau tous les agents en un seul processus ou de planifier les mises à niveau pour une date ultérieure.

Processus de mise à niveau

1. Accédez à **Infrastructure > Instances > Agents**.
2. Cliquez sur **Planifications de mise à niveau**.

   
3. Dans la page **Planifications de mise à niveau**, cliquez sur **Ajouter**.
4. Cliquez sur **Ajouter des agents**, sélectionnez les agents de la liste que vous souhaitez mettre à niveau, puis cliquez sur **Suivant**.

   REMARQUE :

   Seuls les agents exécutant la version 14.1-38.x ou ultérieure sont affichés.

   
5. Dans l'onglet **Sélectionner une image**, sélectionnez une image (.tgz) à partir de l'ordinateur local ou de l'appliance. Vous pouvez télécharger l'image depuis votre ordinateur local ou l'appliance. Lorsque vous sélectionnez **Appliance**, l'interface graphique de NetScaler Console affiche les images présentes dans `/var/mps/mas_agent_images`. Sélectionnez une image dans la liste.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Après avoir sélectionné l'image, cliquez sur **Suivant**.
7. Sous **Planification de la mise à niveau**, sélectionnez **Mettre à niveau maintenant** pour effectuer la mise à niveau immédiatement.

   Planification de la mise à niveau(/en-us/netscaler-application-delivery-management-software/media/upgrade-agent-scheduling.png)

   Si vous souhaitez planifier une mise à niveau, sélectionnez **Planifier ultérieurement**, puis fournissez les détails en sélectionnant le fuseau horaire, la date et l'heure (format 24 heures).

   Planifier ultérieurement(/en-us/netscaler-application-delivery-management-software/media/agent-upgrade-schedule-later.png)
8. Si vous souhaitez être informé du flux de travail de mise à niveau, cliquez sur **Configurer les notifications** sous **Notifications**, sélectionnez la catégorie `AgentMonitoring`, et sélectionnez les options de communication (Email, SMS, Slack, PagerDuty et ServiceNow) pour lesquelles vous souhaitez être informé.
9. Cliquez sur **Terminé**.

Migrer le déploiement de serveur unique NetScaler Console vers un déploiement haute disponibilité

Vous pouvez mettre à niveau votre serveur unique NetScaler Console vers un déploiement haute disponibilité de deux serveurs NetScaler Console. Une paire haute disponibilité de serveurs NetScaler Console est en mode actif-passif, et les deux serveurs ont la même configuration. Dans ce type de déploiement actif-passif, un serveur NetScaler Console est configuré comme nœud principal et l'autre comme nœud secondaire. Si, pour une raison quelconque, le nœud principal tombe en panne, le nœud secondaire prend le relais. Pour plus d'informations, consultez Configurer le déploiement haute disponibilité.

Pour migrer un serveur unique NetScaler Console vers une paire haute disponibilité, vous devez :

1. Connectez-vous au serveur unique NetScaler Console.
2. Accédez à **Paramètres > Administration** et cliquez sur **Configurer NetScaler® Console High Availability (HA)** sous **Paramètres de haute disponibilité**.

   
3. Dans la page **Configurer NetScaler Console High Availability (HA)** :

   a. Fournissez une adresse IP de serveur NetScaler Console secondaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Spécifiez le mot de passe du nœud secondaire.

c. Spécifiez l'adresse IP flottante.

d. Cliquez sur **Configurer**.

4. Dans la fenêtre de confirmation, cliquez sur **Oui**. Les instances NetScaler Console redémarrent pour former une paire HA.
5. Une fois la configuration de la paire HA terminée, connectez-vous au NetScaler Console principal et accédez à **Paramètres > Déploiement HA** pour valider les nœuds principal et secondaire.



Migrer de NetScaler Insight Center vers NetScaler Console

Vous pouvez désormais migrer votre déploiement NetScaler Insight Center vers NetScaler Console sans perdre la configuration, les paramètres ou les données existants. Avec NetScaler Console, vous pouvez non seulement afficher les différentes analyses générées par les instances NetScaler associées à une application, mais aussi gérer, surveiller et dépanner l'ensemble de l'infrastructure globale de livraison d'applications à partir d'une console unique et unifiée.

REMARQUE

La migration n'est actuellement prise en charge que sur les instances autonomes de NetScaler® Insight Center.

Prérequis

Avant de migrer l'appliance virtuelle NetScaler Insight Center vers NetScaler Console, vérifiez que les exigences suivantes sont remplies :

- NetScaler Insight Center 11.1 Build 47.14 ou version ultérieure est installé.
- Vous avez téléchargé le fichier image .tgz de NetScaler Console 12.0 build 57.24.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous devez installer NetScaler Console 12.0 build 57.24, puis effectuer la mise à niveau vers la dernière version de NetScaler Console 13.1. Pour plus d'informations, consultez Mise à niveau.

- Vous avez téléchargé le fichier image .tgz de la dernière version de NetScaler Console 13.1.

Exigences matérielles

COMPOSANT	EXIGENCE
RAM	32 Go
CPU virtuel	8 CPU
Espace de stockage	120 Go
	Remarque Nous vous recommandons d'utiliser **500 Go** pour de meilleures performances. De plus, Citrix recommande d'utiliser la technologie de disque SSD (Solid-State Drive) pour les déploiements NetScaler Console.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Exigences de l'hyperviseur	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Procédure d'installation

Pour migrer NetScaler Insight Center vers NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Connectez-vous à l'invite de commande shell de NetScaler Insight Center.
2. Téléchargez NetScaler Console 12.0 build 57.24 dans le dossier */var/mps/mps_images*.
3. Détarifier le fichier TGZ à l'aide de la commande **tar -zxvf build-mas-12.0-57.24.tgz**.

   
4. Installez NetScaler Console à l'aide de la commande **./installmas**.

   
5. Après avoir installé NetScaler Console 12.0 build 57.24, vous devez effectuer une mise à niveau vers la dernière version de NetScaler Console 13.1 en suivant les étapes ci-dessus.

Après la migration, toutes les instances NetScaler découvertes dans l'inventaire de NetScaler Insight Center apparaissent dans la section **Infrastructure > Instances** de NetScaler Console. Cependant, pour la première fois, vous devez interroger manuellement les serveurs virtuels hébergés dans les appliances découvertes.

REMARQUE

Dans NetScaler Console, par défaut, il n'y a pas de coût de licence pour gérer et surveiller deux serveurs virtuels créés au sein des instances NetScaler découvertes. Pour surveiller et gérer plus de deux serveurs virtuels, installez les licences NetScaler Console requises. Pour plus de détails, consultez Licences NetScaler Console.

Intégrer NetScaler Console avec Citrix Director

Director s'intègre à NetScaler Console pour l'analyse réseau et la gestion des performances.

- L'analyse réseau obtient des rapports HDX Insight de NetScaler Console et fournit une vue applicative et de bureau du réseau. Grâce à cette fonctionnalité, Director fournit une vue analytique avancée du trafic ICA dans votre déploiement.
- La gestion des performances fournit la rétention historique et les rapports de tendances. Grâce à la rétention historique des données par rapport à l'évaluation en temps réel, vous pouvez créer des rapports de tendances, y compris les tendances de capacité et de santé.

Après avoir intégré NetScaler Console à Director, les rapports HDX Insight vous fournissent les informations suivantes dans Director :

- L'onglet Réseau de la page Tendances affiche les effets de la latence et de la bande passante pour les applications, les bureaux et les utilisateurs dans l'ensemble de votre déploiement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La page Détails de l'utilisateur affiche les informations de latence et de bande passante spécifiques à une session utilisateur particulière.

Prérequis

Exigences matérielles pour la migration de HDX Insight vers NetScaler Console

COMPOSANT	EXIGENCE
RAM	32 Go
Processeur virtuel	8
Espace de stockage	500 Go. Nous recommandons l'utilisation de la technologie de disque SSD (Solid-State Drive) pour les déploiements NetScaler Console.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

Configuration minimale requise

Avant de configurer l'intégration réseau, assurez-vous de créer un utilisateur RBAC avec accès à HDX™ Insights.

Configuration logicielle requise

Avant de migrer vers l'appliance virtuelle NetScaler Console, vérifiez que les exigences suivantes ont été satisfaites :

- Director version 1811 est installé
- NetScaler HDX Insight version 10.1 ou ultérieure est installé
- HDX Insight et NetScaler Console prennent en charge Citrix VDA version 7.0 et ultérieure
- Citrix Workspace est pris en charge sur Citrix Virtual Apps and Desktops version 7.0 et ultérieure
- Assurez-vous que Citrix Workspace pour Mac version 11.8 et ultérieure, et Citrix Workspace pour Windows version 14.0 et ultérieure sont disponibles pour afficher des métriques ICA RTT précises.
- NetScaler Console version 11.0 et ultérieure est installée. Pour plus d'informations sur l'installation de NetScaler Console, consultez Déployer NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limitations

- La disponibilité de cette fonctionnalité dépend de la licence de votre organisation et de vos autorisations d'administrateur.
- Le temps d'aller-retour (RTT) de la session ICA affiche correctement les données pour Citrix Workspace pour Windows 3.4 ou version ultérieure et pour Citrix Workspace pour Mac 11.8 ou version ultérieure. Pour les versions antérieures de ces Workspaces, les données ne s'affichent pas correctement.
- Dans la vue Tendances, les données de connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées comme 0.
- Pour les déploiements qui disposent déjà d'un disque dur externe avec un espace de stockage inférieur à 500 Go, vous ne pouvez pas ajouter un autre disque dur.

REMARQUE

- Pour plus d'informations sur Director et pour les étapes d'intégration de NetScaler Console avec Director, consultez `<https://docs.citrix.com/fr-fr/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.html>`.
- Pour plus d'informations sur HDX Insight, consultez `<http://docs.citrix.com/fr-fr/xenapp-and-xendesktop/7-11/director/hdx-insight.html>`.

Attacher un disque supplémentaire à NetScaler Console

Les exigences de stockage de NetScaler Console sont déterminées en fonction de votre estimation de dimensionnement de NetScaler Console. Par défaut, NetScaler Console vous offre une capacité de stockage de 120 Go. Si vous avez besoin de plus de 120 Go pour stocker vos données, vous pouvez attacher un disque supplémentaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Estimez les besoins en stockage et attachez un disque supplémentaire au serveur.
- Pour un déploiement NetScaler Console à serveur unique, vous ne pouvez attacher qu'un seul disque au serveur en plus du disque par défaut.
- Pour un déploiement NetScaler Console à haute disponibilité, vous devez attacher un disque supplémentaire à chaque nœud. La taille des deux disques doit être identique.
- S'il existe un disque externe de capacité inférieure, vous devez le retirer avant d'attacher un nouveau disque.
- Nous recommandons l'utilisation de la technologie de disque SSD (Solid-State Drive) pour les déploiements NetScaler Console.

Ce document explique les scénarios suivants concernant l'attachement d'un nouveau disque supplémentaire, la création de partitions et le redimensionnement des disques additionnels :

1. Attacher un disque supplémentaire dans une NetScaler Console autonome
2. Lancer l'outil de partitionnement de disque
3. Créer des partitions dans le nouveau disque additionnel
4. Redimensionner les partitions dans le disque additionnel existant
5. Supprimer les partitions dans le disque additionnel

Attacher un disque supplémentaire dans une NetScaler Console autonome

1. Arrêtez la machine virtuelle NetScaler Console.
2. Dans l'hyperviseur, attachez un disque supplémentaire de la taille requise à la machine virtuelle NetScaler Console.

   Le nouveau disque plus grand attaché stocke les données de la base de données et les fichiers journaux de NetScaler Console. Le disque par défaut existant de 120 gigaoctets est maintenant utilisé pour stocker les fichiers core, les fichiers journaux du système d'exploitation, etc.
3. Démarrez la machine virtuelle NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lancer l'outil de partitionnement de disque

NetScaler Console fournit désormais **NetScaler Console disk partition tool**, un nouvel outil en ligne de commande.

1. À l'aide de l'outil, vous pouvez créer des partitions dans le disque supplémentaire nouvellement ajouté.
2. Vous pouvez également redimensionner les disques supplémentaires existants à l'aide de l'outil. Mais le disque externe existant ne doit pas être supérieur à 2 téraoctets.

   REMARQUE :

   - Le redimensionnement des disques existants au-delà de 2 téraoctets peut entraîner une perte de données. Cela est dû à une limitation connue de la plateforme.
   - Pour créer une capacité de stockage supérieure à 2 téraoctets, vous devez supprimer les partitions existantes et créer des partitions à l'aide de ce nouvel outil.

3. À l'aide de ce nouvel outil, vous pouvez effectuer explicitement toute action de partitionnement sur le disque. L'outil vous offre une visibilité et un contrôle clairs sur le disque et les données associées.

   REMARQUE :

   Vous ne pouvez utiliser cet outil que sur le disque supplémentaire que vous avez attaché au serveur NetScaler Console. Vous ne pouvez pas créer de partitions dans le disque principal (par défaut) à l'aide de cet outil.

Pour lancer l'outil de partitionnement de disque :

1. Ouvrez une connexion SSH à la NetScaler Console en utilisant un client SSH, tel que PuTTY.
2. Connectez-vous à la NetScaler Console en utilisant les informations d'identification `nsrecover/nsroot`.
3. Passez à l'invite de commande du shell et tapez :

   ```
   /mps/DiskPartitionTool.py
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour NetScaler Console en déploiement haute disponibilité, vous devez lancer l'outil sur les deux nœuds et créer ou redimensionner les partitions après avoir attaché les disques aux machines virtuelles respectives.

Créer des partitions sur le nouveau disque supplémentaire

La commande **create** est utilisée pour créer des partitions chaque fois qu'un nouveau disque secondaire est ajouté. Vous pouvez également utiliser cette commande pour créer des partitions sur un disque secondaire existant après la suppression des partitions existantes à l'aide de la commande « remove ».

REMARQUE :

Il n'y a pas de limitation de taille de 2 téraoctets lors de la création de partitions avec l'outil de partitionnement de disque. L'outil peut créer des partitions de plus de 2 téraoctets. Lorsque vous partitionnez le disque, une partition d'échange de 32 Go est automatiquement ajoutée. La partition principale utilise ensuite tout l'espace restant sur le disque.

Une fois la commande exécutée, un schéma de partitionnement de table de partition GUID (GPT) est créé. Une partition d'échange de 32 Go et une partition de données sont également créées pour utiliser le reste de l'espace. Un nouveau système de fichiers est ensuite créé sur la partition principale.

REMARQUE :

Ce processus peut prendre quelques secondes, et vous ne devez pas l'interrompre.

Une fois la commande de création terminée, la machine virtuelle est automatiquement redémarrée pour que la nouvelle partition soit montée.

Après le redémarrage, la nouvelle partition est montée sur /var/mps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La partition d'échange ajoutée apparaît comme espace d'échange dans la sortie de la commande « create ».



REMARQUE :

L'outil redémarre la machine virtuelle une fois la partition créée.

Redimensionner les partitions du disque supplémentaire existant

Vous pouvez utiliser la commande **resize** pour redimensionner le disque attaché (secondaire). Vous pouvez redimensionner un disque qui a un schéma `master boot record (MBR`) ou GPT. La taille du disque doit être inférieure à 2 téraoctets.

REMARQUE :

- La commande `resize` est conçue pour fonctionner sans perte de données existantes. Cependant, nous vous recommandons de sauvegarder les données critiques de ce disque sur un stockage externe avant de le redimensionner. La sauvegarde des données est utile dans les cas où les données du disque pourraient être corrompues pendant l'opération de redimensionnement.
- Assurez-vous d'augmenter l'espace disque par incréments de 100 Go lors du redimensionnement des partitions. Une augmentation incrémentielle de ce type garantit que vous n'aurez pas à redimensionner plus fréquemment.



La commande `resize` vérifie toutes les préconditions et procède si toutes les préconditions sont remplies et après que vous ayez donné votre consentement au redimensionnement. Elle arrête les processus accédant au disque, ce qui inclut les sous-systèmes NetScaler Console, les processus de la base de données PostgreSQL et le processus de surveillance de NetScaler Console. Une fois les processus arrêtés, le disque est démonté pour le préparer au redimensionnement. Le redimensionnement est effectué en étendant la partition pour occuper tout l'espace disponible, puis en augmentant le système de fichiers. Si une partition d'échange existe sur le disque, elle est supprimée et recréée à la fin du disque après le redimensionnement. La partition d'échange est abordée dans la section de la commande **Create** du document.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Le processus d'« augmentation du système de fichiers » peut prendre un certain temps. Veillez à ne pas interrompre le processus pendant son exécution. L'outil redémarre la machine virtuelle après que vous ayez redimensionné la partition.

Toutes les étapes intermédiaires du processus de redimensionnement (arrêt des applications, redimensionnement du disque, augmentation du système de fichiers) sont affichées sur la console. Une fois le processus terminé, le message suivant s'affiche.

Après le redémarrage, l'augmentation de la taille peut être observée à l'aide de la commande `df`. Voici les détails avant et après l'augmentation de la taille :

Supprimer les partitions du disque supplémentaire

Une partition existante sur le disque secondaire peut être redimensionnée jusqu'à 2 téraoctets. Ce problème est dû à une limitation connue de la partition. Si vous souhaitez un disque de plus de 2 téraoctets, attachez un nouveau disque et partitionnez-le à l'aide de l'outil de partitionnement de disque. Vous pouvez également supprimer la partition existante à l'aide de la commande `remove`, puis créer une partition.

REMARQUE :

La suppression de la partition existante efface toutes les données existantes. Par conséquent, toutes les données critiques doivent être sauvegardées sur un stockage externe avant d'utiliser cette commande.

L'exécution de la commande « remove » vous demande une confirmation et, une fois confirmée, elle arrête tous les processus (tels que les sous-systèmes NetScaler Console, les processus PostgreSQL et les moniteurs NetScaler Console) utilisant le disque secondaire. Si une partition d'échange existe et que l'échange est activé sur la partition, l'échange est désactivé.

Lorsque vous tapez « y », la commande démonte le disque et supprime toutes les partitions du disque.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



REMARQUE :

L'outil redémarre la machine virtuelle après que vous ayez supprimé la partition.

Redémarrer la machine virtuelle

Lorsqu'une partition est créée ou redimensionnée, ou lorsqu'un fichier d'échange est créé, redémarrez la machine virtuelle. Les modifications ne prennent effet qu'après le redémarrage. À cette fin, une commande **reboot** est fournie dans l'outil.



Une confirmation vous est demandée et après confirmation, tous les processus (tels que les sous-systèmes NetScaler Console, les processus PostgreSQL et les moniteurs NetScaler Console) sont arrêtés. La machine virtuelle est ensuite redémarrée.



Créer un fichier de sauvegarde des données du disque

REMARQUE :

La création d'un fichier de sauvegarde nécessite de l'espace disque. Assurez-vous qu'il y a suffisamment d'espace disque (50 % ou plus) avant d'exécuter les commandes de sauvegarde.

Pour sauvegarder les données de NetScaler Console avant de redimensionner ou de supprimer les partitions :

1. Arrêtez NetScaler Console.

   ```
   /mps/masd stop
   ```

2. Arrêter PostgreSQL.

   ```
   su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
   ```

3. Arrêter NetScaler Console Monitor.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
/mps/scripts/stop_mas_monit.sh
```

4. Créer une archive tar.

```
cd /var

tar cvfz /var/mps/mps_backup.tgz mps
```

REMARQUE :

L'opération prend du temps en fonction de la taille des données à sauvegarder.

5. Générer une somme de contrôle.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
```

6. Copier l'archive tar et les fichiers de somme de contrôle sur un serveur distant.
7. Valider l'exactitude de l'archive tar copiée. Générer une somme de contrôle du fichier transféré et comparer avec la somme de contrôle source.
8. Supprimer l'archive tar de la machine virtuelle NetScaler Console.

```
cd /var/mps/

rm mps_backup.tgz  mps_backup_checksum
```

Commandes supplémentaires

En plus des commandes listées précédemment, vous pouvez également utiliser les commandes suivantes dans l'outil :

Commande d'aide :

Pour lister les commandes prises en charge, tapez **help** ou **?** et appuyez sur Entrée. Pour obtenir de l'aide supplémentaire sur chacune des commandes, appuyez sur **help** ou **?** suivi du nom de la commande et appuyez sur la touche **Entrée**.

Commande d'informations :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La commande **info** fournit des informations sur le disque secondaire attaché si le disque existe. La commande fournit le nom du périphérique, le schéma de partition, la taille sous une forme lisible par l'homme et le nombre de blocs de disque. Le schéma peut être MBR ou GPT. Un schéma MBR signifie que le disque a été partitionné à l'aide d'une version antérieure de NetScaler Console. La partition basée sur MBR/GPT peut être redimensionnée mais pas au-delà de 2 téraoctets. Le schéma de partition GPT signifie que le disque a été partitionné à l'aide de NetScaler Console 12.1 ou version ultérieure.

REMARQUE :

Une partition GPT peut être supérieure à 2 téraoctets lors de sa création. Cependant, vous ne pouvez pas redimensionner le disque à une taille supérieure à 2 téraoctets après avoir créé un disque de taille inférieure. Ce problème est une limitation connue de la plateforme.

Commande Create_swapfile :

La partition de swap par défaut sur le disque principal de NetScaler Console est de 4 Go, et l'espace de swap par défaut est donc de 4 Go. Pour la configuration mémoire par défaut de NetScaler Console, qui est de 2 Go, cet espace de swap est suffisant. Cependant, lorsque vous exécutez NetScaler Console avec une configuration mémoire plus élevée, vous devez allouer plus d'espace de swap sur le disque.

REMARQUE :

Une partition de swap est généralement une partition dédiée créée sur un disque dur (HDD) lors de l'installation du système d'exploitation. Une telle partition est également appelée espace de swap. Une partition de swap est utilisée pour la mémoire virtuelle qui simule la mémoire principale supplémentaire.

Les disques secondaires ajoutés dans les versions antérieures de NetScaler Console n'ont pas de partition de swap créée par défaut. La commande « create_swapfile » est destinée aux disques secondaires créés à l'aide d'anciennes versions de NetScaler Console qui n'ont pas de partition de swap. La commande vérifie les éléments suivants :

- Présence d'un disque secondaire
- Disque monté
- Taille du disque (au moins 500 Go)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'existence du fichier de swap

La commande `create_swapfile` est utile uniquement lorsque la mémoire est supérieure ou égale à 16 Go et non lorsque la mémoire est faible. Par conséquent, cette commande vérifie également la mémoire avant de procéder à la création du fichier de swap.

Si toutes les conditions sont remplies et que l'utilisateur consent à continuer, un fichier d'échange de 32 Go est créé sur le disque secondaire. Le processus de création du fichier d'échange prend quelques minutes et veillez à ne pas interrompre le processus pendant qu'il est en cours. Une fois terminé avec succès, un redémarrage est effectué pour que le fichier d'échange prenne effet.

Après le redémarrage, l'augmentation de l'échange peut être observée à l'aide de la commande top.

Commande de sortie :

Pour quitter l'outil, tapez exit et appuyez sur la touche **Entrée**.

Attacher des disques supplémentaires à NetScaler Console déployé en haute disponibilité

Considérez que vous avez configuré une paire de serveurs NetScaler Console dans une configuration de haute disponibilité sans aucun disque secondaire. Considérez également que vous avez ajouté 2 instances NetScaler ou plus, vérifié et assuré que tous les processus sont en cours d'exécution. Vous pourriez vouloir ajouter des disques secondaires aux machines virtuelles dans cette configuration. Dans une configuration de haute disponibilité, vous devez ajouter des disques supplémentaires aux deux nœuds, comme détaillé dans cette tâche :

1. Arrêtez le nœud secondaire.
2. Ajoutez un disque via l'hyperviseur.

   REMARQUE :

   Assurez-vous de ne pas étendre le disque principal du nœud secondaire.

3. Démarrez le nœud secondaire.
4. Exécutez l'outil de partitionnement sur le nœud secondaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Une fois le disque ajouté, le nœud secondaire redémarre.
6. Arrêtez le nœud secondaire après son redémarrage.
7. Arrêtez le nœud principal.
8. Ajoutez un disque via l'hyperviseur.

   REMARQUE :

   Assurez-vous de ne pas étendre le disque principal du nœud principal.

9. Démarrez le nœud principal.
10. Exécutez l'outil de partitionnement sur le nœud principal.
11. Une fois le disque ajouté, le nœud principal redémarre.
12. Une fois le nœud principal opérationnel, démarrez le nœud secondaire.
13. Assurez-vous que le nœud secondaire est opérationnel et que les bases de données sont synchronisées.
14. Confirmez que toutes les données existent toujours.

Pour augmenter la capacité de la RAM sur les deux nœuds :

1. Arrêtez Console_Secondary et augmentez la taille de la RAM selon les besoins. Ne redémarrez pas le nœud.
2. Arrêtez Console_Primary et augmentez la taille de la RAM selon les besoins.

   Assurez-vous d'augmenter la taille de la RAM de manière égale sur les deux nœuds. Par exemple, si vous augmentez la taille de la RAM sur le nœud principal à 16 Go, faites de même sur le nœud secondaire.
3. Redémarrez la Console_Primary.
4. Une fois que la Console_Primary a redémarré, vérifiez s'il s'agit du nœud principal.
5. Démarrez le nœud Console_Secondary. Après son redémarrage, assurez-vous qu'il est passé en mode secondaire et que la synchronisation de la base de données fonctionne.
6. Confirmez que toutes les données existent toujours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Après avoir ajouté le disque secondaire, le nœud principal met un certain temps à démarrer. De plus, l'ensemble du processus d'ajout de disques secondaires aux deux nœuds et d'augmentation de la capacité de la RAM nécessite que les deux nœuds soient hors service pendant un certain temps. Tenez compte de cette période d'indisponibilité lors de la planification de cette activité de maintenance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Chiffrement de disque NetScaler MPX™ via NetScaler Console

REMARQUES :

- Le chiffrement de disque est pris en charge uniquement sur les instances NetScaler MPX 9100.
- Le chiffrement de disque pour les instances NetScaler MPX 9100 ne peut être activé que dans une console NetScaler autonome.
- À partir de la version 14.1-56.x, le chiffrement de disque est pris en charge sur les instances NetScaler MPX 9100, 16000 et MPX 15000-50G fabriquées après May 20, 2025.

Le chiffrement de disque est essentiel pour sécuriser les données sensibles stockées sur un disque de stockage. Il garantit que même si le périphérique de stockage physique est compromis, les données restent inaccessibles. Pour NetScaler MPX, le chiffrement de disque offre une couche de sécurité supplémentaire, en particulier pour les répertoires critiques tels que `/var/core`, `/var/crash`, `/var/log`, `/var/nslog`, `/flash/nsconfig`, `/var/nstrace` et `/var/temp`.

Voici quelques-uns des avantages du chiffrement de disque :

- **Protection des données au repos** : Empêche l'accès non autorisé aux données sensibles lorsque le système est éteint.
- **Conformité** : Aide à respecter les exigences réglementaires et de conformité en matière de sécurité des données.
- **Atténuation des risques de vol physique** : Garantit que les données sensibles et propriétaires sur les périphériques de stockage volés ou égarés ne peuvent pas être consultées.
- **Processus de démarrage sécurisé** : Nécessite des informations d'identification authentifiées lors du démarrage, garantissant que seuls les utilisateurs autorisés peuvent accéder au système.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Sécurité renforcée pour les données critiques** : Protège les journaux, les configurations et les données de plantage contre tout accès non autorisé.

Le chiffrement de disque sur NetScaler MPX 9100 est pris en charge uniquement dans la version 14.1-47.x livrée après **May 20, 2025** et peut être activé via NetScaler Console exécutant la version 14.1-47.x. Le chiffrement de disque de chaque instance NetScaler MPX nécessite une clé gérée par le serveur Hardware Security Module (HSM), qui est le Thales CipherTrust Manager. Les instances NetScaler MPX utilisent NetScaler Console pour récupérer la clé du serveur HSM.

Le chiffrement de disque sur NetScaler MPX 9100, 16000 et MPX 15000-50G est pris en charge uniquement dans la version 14.1-56.x livrée avant **May 20, 2025** et peut être activé via NetScaler Console exécutant la version 14.1-56.x. Pour activer la fonctionnalité, consultez Chiffrement de disque d'instance via NetScaler Console.

REMARQUE :

NetScaler Console prend en charge Thales CipherTrust Manager en tant que serveur HSM.

Pour un chiffrement réussi, vous devez (#add-the-instance-serial-number-in-the-hsm-thales-ciphertrust-manager-server). Après avoir ajouté le numéro de série de l'instance NetScaler MPX, NetScaler Console récupère la clé à l'aide du numéro de série de l'instance à partir du serveur HSM.

Une fois le chiffrement du disque terminé :

- Si le disque de l'instance NetScaler MPX est retiré, les données ne sont pas accessibles.
- Si vous redémarrez l'instance NetScaler MPX, le redémarrage n'est réussi qu'après que NetScaler Console a authentifié l'instance NetScaler MPX à l'aide de son numéro de série depuis le serveur HSM.

Conditions préalables

Assurez-vous que :

- Pour les 9100, les instances NetScaler MPX exécutent la version 14.1-47.x et sont gérées sur NetScaler Console sur site exécutant la version 14.1-47.x.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Le chiffrement de disque n'est pas pris en charge sur le service NetScaler Console.

- Vous avez ajouté le numéro de série de l'instance NetScaler MPX dans le serveur HSM (Thales CipherTrust Manager) pour que NetScaler Console partage la clé après avoir authentifié l'instance à l'aide de son numéro de série.
- L'instance NetScaler MPX est sauvegardée via NetScaler Console. Pour plus d'informations, consultez (/fr-fr/netscaler-application-delivery-management-software/current-release/analytics/security/backup-restore-netscaler-instances.html).
- Pour les MPX 16000 et MPX 15000-50G, NetScaler Console sur site est en version 14.1 build 56.x.

Ajouter le numéro de série de l'instance dans le serveur HSM (Thales CipherTrust Manager)

Avant de chiffrer l'instance NetScaler MPX, vous devez ajouter le numéro de série de l'instance NetScaler MPX dans le serveur HSM.

1. Connectez-vous au serveur Thales CipherTrust Manager.
2. Dans le volet gauche, sélectionnez **Clés** et cliquez sur **Ajouter une clé**.
3. Sous **Étiquettes de clé**, ajoutez une étiquette avec le nom `serialnumber`, spécifiez le numéro de série de l'instance dans la zone de texte **Valeur de l'étiquette**, cliquez sur le bouton **+** pour ajouter les détails de la clé, puis cliquez sur **Ajouter une clé**.

   
4. Dans la page des détails de la clé, vous devez activer le bouton bascule Exportable pour cette clé.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- La taille de clé maximale prise en charge est de 511 octets. Par exemple : AES-128 et AES-256 sont pris en charge. Les clés RSA entre 512 et 4096 ne sont pas prises en charge.
- Nous vous recommandons d'utiliser uniquement la taille de clé prise en charge. L'instance NetScaler® échoue si vous configurez une taille de clé non prise en charge.
- Assurez-vous de spécifier le numéro de série correct. S'il y a une non-concordance dans le numéro de série, le processus de chiffrement ne démarre pas.
- Nous vous recommandons de copier le numéro de série de l'instance depuis NetScaler Console. Dans l'interface graphique de NetScaler Console, accédez à **Infrastructure > Instance > MPX**, sélectionnez l'instance NetScaler MPX, et dans la liste **Sélectionner une action**, cliquez sur **Obtenir le numéro de série**.

Chiffrement du disque d'instance via NetScaler Console

Avant de commencer le chiffrement du disque, assurez-vous de sauvegarder l'instance MPX via NetScaler Console. Pour plus d'informations, consultez Configurer la sauvegarde de l'instance.

Après avoir effectué la sauvegarde :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Dans l'onglet **NetScaler MPX**, vous pouvez voir les détails des instances gérées. L'instance que vous souhaitez chiffrer affiche **Texte brut** sous **État du chiffrement du disque**.

   
3. Dans la liste **Sélectionner une action**, cliquez sur **Paramètres de chiffrement du disque**.

   
4. Dans la liste **Sélectionner une action**, cliquez sur **Promouvoir l'appareil**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

La sélection de l'option **Promouvoir l'appareil** est obligatoire pour activer la fonctionnalité de chiffrement de disque spécifiquement pour les appliances MPX fabriquées avant May 20, 2025. Prévoyez environ 30 minutes pour que l'appliance MPX termine sa conversion en un appareil compatible avec le chiffrement de disque.

5. Dans la page **Paramètres de chiffrement du disque** :

   a. Spécifiez l'adresse IP, le nom d'utilisateur et le mot de passe du serveur HSM à partir duquel NetScaler Console peut récupérer la clé de chiffrement à l'aide du numéro de série.

   b. Activez le **proxy du gestionnaire de clés**. Vous devez activer cette option pour poursuivre le processus de chiffrement du disque.

   REMARQUE :

   Assurez-vous que le **proxy du gestionnaire de clés** est toujours activé, même après la fin du chiffrement. Si vous désactivez cette option, l'instance chiffrée ne redémarrera pas correctement dans des scénarios tels qu'après une mise à niveau de l'instance ou un redémarrage forcé de l'instance.

   c. Cliquez sur **Enregistrer**.

6. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, cliquez sur **Chiffrer le système de fichiers**.

   Une fenêtre de confirmation apparaît. Cliquez sur **Oui** pour continuer.

7. Un message de confirmation apparaît dans NetScaler Console indiquant que le chiffrement a démarré et que l'instance sera en état **Hors service** pendant environ 30 minutes.

   L'état de l'instance apparaît comme **Chiffrement en cours**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validation après le chiffrement

Le chiffrement de l'instance est terminé en environ 30 minutes. Une fois le chiffrement terminé :

- Vous pouvez vous connecter à l'instance NetScaler MPX à l'aide d'un client SSH, puis vérifier si le chiffrement a réussi en utilisant la commande suivante :

  `show filesystemencryption`

AVANT LE CHIFFREMENT	APRÈS LE CHIFFREMENT
	

- Vous pouvez redémarrer votre instance NetScaler MPX et vérifier si le redémarrage est terminé après le chiffrement, comme illustré dans l'exemple suivant :

  

- Vous pouvez utiliser la commande suivante pour vérifier si le **proxy du gestionnaire de clés** est correctement configuré et accessible depuis NetScaler :

  `show keymanagerproxy`

  

  REMARQUE :

  Après le chiffrement, NetScaler Console utilise `mpx_disk_encryption_default_profile` pour accéder à l'instance NetScaler MPX. Le `mpx_disk_encryption_default_profile` contient les informations d'identification par défaut (`nsroot` / `nsroot`).

  

Restaurer l'instance NetScaler MPX après le chiffrement

Si vous avez modifié le mot de passe par défaut (nsroot) avant d'effectuer la sauvegarde, assurez-vous que le profil utilisé lors de la sauvegarde est disponible dans NetScaler Console après le chiffrement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comportement de la paire HA NetScaler MPX™ après le chiffrement

Les nœuds principal et secondaire doivent avoir le même état de chiffrement. S'il existe une non-concordance entre l'état de chiffrement des nœuds principal et secondaire, la synchronisation entre les deux nœuds est désactivée. Connectez-vous à l'instance NetScaler® MPX principale à l'aide d'un client SSH et utilisez la commande suivante pour vérifier si les deux nœuds affichent le même état de chiffrement :

```
sh ha node
```



Si l'état de chiffrement des deux nœuds est différent :

- La sortie suivante apparaît en cas de non-concordance du chiffrement de disque :

  

- Une erreur de non-concordance du chiffrement de disque apparaît pour l'activation de la synchronisation HA, l'activation de la propagation HA et la synchronisation HA forcée :

  - `set ha node -haprop enabled`

    

  - `set ha node -hasync enabled`

    

  - `force ha sync`

    

Comportement du cluster NetScaler MPX™ après chiffrement

Pour une formation de cluster réussie, tous les nœuds doivent avoir le même statut de chiffrement. S'il y a une incohérence dans le statut de chiffrement d'un nœud :

- Le statut de santé du nœud non concordant est affiché comme **HORS SERVICE** et le nœud ne traite pas le trafic.

  

- La synchronisation du nœud non concordant dans le cluster est désactivée.

  

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le nœud ne peut pas être ajouté au cluster. Le message d'échec de la commande de jonction apparaît :

  

- La propagation des commandes du cluster est désactivée.

  

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console Cloud Connect

NetScaler Console Cloud Connect établit une connexion sécurisée et sortante de NetScaler Console sur site vers le service NetScaler Console via Citrix Cloud™ pour activer les fonctionnalités fournies par le cloud sur NetScaler Console sur site.

Vous pouvez configurer Cloud Connect pour utiliser la fonctionnalité suivante dans NetScaler Console sur site :

- **Licences basées sur LAS (Livraison des droits)** - Lorsque Cloud Connect est activé sur NetScaler Console sur site et que le déploiement exécute des versions compatibles LAS, LAS est automatiquement activé. Les droits de licence sont récupérés et renouvelés automatiquement. Pour plus d'informations, consultez Service d'activation de licence.
- **Livraison d'actifs** - La livraison d'actifs fournit des mises à jour de signature chiffrées et des mises à jour de schéma chiffrées pour les profils WAF intégrés définis pour sécuriser les requêtes entrantes pour l'authentification, l'autorisation, l'audit, le VPN et les composants GUI. La livraison d'actifs est activée par défaut lorsque Cloud Connect est activé et, si nécessaire, les administrateurs peuvent la désactiver. Pour plus d'informations, consultez Protection du pare-feu d'applications Web pour les serveurs virtuels VPN et les serveurs virtuels d'authentification.
- **Conseil de mise à niveau** - Pour utiliser le conseil de mise à niveau sur NetScaler Console sur site, Cloud Connect doit être activé. L'activation de Cloud Connect permet à NetScaler Console de récupérer les dernières informations de build et de les comparer avec les builds des instances NetScaler gérées, aidant ainsi à identifier les instances EOL, EOM et les instances exécutant des builds plus anciennes de NetScaler sur NetScaler Console sur site. Le conseil de mise à niveau est activé par défaut lorsque Cloud Connect est activé. Si nécessaire, les administrateurs peuvent le désactiver. Pour plus d'informations, consultez Conseil de mise à niveau.
- **Intégration ServiceNow** - Cette intégration utilise le connecteur Citrix ITSM pour communiquer entre NetScaler Console et l'instance ServiceNow. L'intégration ServiceNow avec NetScaler Console utilise le service d'adaptateur ITSM pour l'authentification basée sur des jetons. Pour plus d'informations, consultez Intégrer NetScaler Console à l'instance ServiceNow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prérequis

Avant de configurer Cloud Connect, assurez-vous de disposer des prérequis suivants :

- Assurez-vous de disposer d'une connexion Internet ou d'un serveur proxy configuré dans NetScaler Console sur site pour l'accessibilité à Citrix Cloud.
- L'ordinateur portable ou la machine utilisée pour accéder à NetScaler Console pour la configuration de Cloud Connect doit disposer d'une connectivité Internet pendant la configuration initiale. Pour plus d'informations, consultez FAQ.
- Assurez-vous que le compte de service NetScaler Console est disponible.
  - Étape 1 : Créez un compte Citrix Cloud ou connectez-vous à l'aide d'un compte Citrix Cloud existant. Pour plus d'informations sur la création d'un compte Citrix Cloud, consultez Créer un compte Citrix Cloud.
  - Étape 2 : Créez un locataire de service NetScaler Console en gérant le service NetScaler Console. Pour plus d'informations sur la gestion du service NetScaler Console, consultez Démarrage rapide.
- Assurez-vous d'avoir autorisé l'accès aux URL de point de terminaison suivantes :

SERVICE	URL POUR LE CLOUD GOUVERNEMENTAL	URL POUR LES RÉGIONS APAC, UE ET ÉTATS-UNIS	URL POUR LE JAPON	POURQUOI EST-CE NÉCESSAIRE ?
Service de confiance	`*.citrixnetworkapi.us`	-	-	Utilisé pour établir la confiance entre NetScaler Console sur site et les services Citrix Cloud.
	`trust.citrixnetworkapi.us`	`trust.citrixnetworkapi.net`	`trust.citrixnetworkapi.jp`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVICE	URL POUR LE CLOUD GOUVERNEMENTAL	URL POUR LES RÉGIONS APAC, UE ET ÉTATS-UNIS	URL POUR LE JAPON	POURQUOI EST-CE NÉCESSAIRE ?
URL de service	`*.agent.adm.cloud.us`	`*.agent.adm.cloud.com`	`*.agent.adm.citrixcloud.jp`	Ce sont les points de terminaison de service NetScaler Console utilisés pour les opérations Cloud Connect. NetScaler Console sur site initie une communication sortante vers ces points de terminaison pour les fonctionnalités fournies via le cloud.
	`*.adm.cloud.us`	`*.adm.cloud.com`	`*.citrixnetworkapi.jp`	
	`adm.cloud.us`	`adm.cloud.com`	`*.adm.citrixcloud.jp`	
	-	`netscalermas.cloud.com`	`adm.citrixcloud.jp`	Utilisé pour récupérer les détails du client tels que le point de terminaison, le nom du POP.
Connectivité Citrix Cloud™	`citrix.cloud.us`	`Citrix.cloud.com`	`citrix.citrixcloud.jp`	Requis pour l'authentificatio

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVICE	URL POUR LE CLOUD GOUVERNEMENTAL	URL POUR LES RÉGIONS APAC, UE ET ÉTATS-UNIS	URL POUR LE JAPON	POURQUOI EST-CE NÉCESSAIRE ?
				n et la sélection du locataire lors de l'intégration de Cloud Connect.
	`accounts.cloud.us`	`Accounts.cloud.com`	`accounts.citrixcloud.jp`	

- Assurez-vous de désactiver le bloqueur de fenêtres contextuelles dans le navigateur à partir duquel vous accédez à l'interface graphique de NetScaler Console sur site.
- (Applicable uniquement au Government Cloud) Effectuez les étapes suivantes sur NetScaler Console sur site pour vous connecter aux points de terminaison de la région Government Cloud.
  - Sur le shell de NetScaler Console sur site, exécutez les commandes suivantes :

```
cd /mps/python/util/



python consoleService.py --region gov
```

REMARQUES :

Ces commandes redémarrent les processus NetScaler Console.

- (Applicable uniquement aux utilisateurs de Japan Cloud) Effectuez les étapes suivantes sur NetScaler Console sur site pour vous connecter aux points de terminaison de la région Japan.
  - Sur le shell de NetScaler Console sur site, exécutez les commandes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
cd /mps/python/util/



python consoleService.py --region japan
```

REMARQUES :

La commande redémarre les processus NetScaler Console.

- Configurez les ports suivants :

```
-  443 (NetScaler Console on-prem/proxy to Cloud)

-  80 (NetScaler Console on-prem to proxy)
```

- Désactivez le bloqueur de fenêtres contextuelles du navigateur pour l'hôte de l'interface graphique de NetScaler Console utilisé pour configurer Cloud Connect.

Configurer Cloud Connect

Flux de travail 1 – Nouvel utilisateur (pas de compte Citrix Cloud et pas de locataire de service NetScaler Console)

1. Créez un compte Citrix Cloud. Pour plus d'informations, consultez Créer un compte Citrix Cloud.
2. Connectez-vous à votre compte Citrix Cloud et cliquez sur la vignette **service NetScaler Console**. Après une connexion réussie, la page redirige vers les étapes de création du locataire de service NetScaler Console.

   a. Sélectionnez une **région** qui correspond à vos besoins commerciaux et cliquez sur **Terminé**.

   b. Sélectionnez un **rôle** et terminez la configuration. Pour plus d'informations, consultez Démarrage.

3. Connectez-vous à NetScaler Console sur site, cliquez sur l'icône **Cloud** > **Démarrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez sur **Connecter au service NetScaler Console**.



   a. Connectez-vous à votre compte Citrix Cloud.
   b. Sélectionnez le nom de votre compte pour terminer la connexion.
   c. Un message « Connexion réussie » s'affiche.

La configuration de Cloud Connect est terminée, Cloud Connect affiche un statut **Connecté**. Vous pouvez ensuite activer des intégrations telles que **ServiceNow** à partir de la page de configuration de **Cloud Connect**.

Flux de travail 2 – Un compte Citrix Cloud existe mais le locataire du service NetScaler Console n'existe pas

1. Connectez-vous à votre compte Citrix Cloud et cliquez sur la vignette **Service NetScaler Console**. Une fois la connexion réussie, la page redirige vers les étapes de création du locataire du service NetScaler Console.

   a. Sélectionnez une **région** qui correspond à vos besoins commerciaux et cliquez sur **Terminé**.
   b. Sélectionnez un **rôle** et terminez la configuration. Pour plus d'informations, consultez Démarrage.

2. Dans NetScaler Console, cliquez sur l'icône **Cloud** > **Démarrer**.



3. Cliquez sur **Connecter au service NetScaler Console**.



   a. Connectez-vous à votre compte Citrix Cloud.
   b. Sélectionnez le nom de votre compte pour terminer la connexion.
   c. Un message « Connexion réussie » vous accueille.

La configuration de Cloud Connect est terminée, Cloud Connect affiche l'état **Connecté**. Vous pouvez ensuite activer des intégrations telles que **ServiceNow** à partir de la page de configuration de **Cloud Connect**.

Flux de travail 3 - Le compte Citrix Cloud et le locataire du service NetScaler Console existent

1. Dans NetScaler Console, cliquez sur l'icône **Cloud** > **Démarrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Cliquez sur **Connecter au service NetScaler Console**.



   a. Connectez-vous à votre compte Citrix Cloud.
   b. Sélectionnez le nom de votre compte pour terminer la connexion.
   c. Un message « Connexion réussie » vous accueille.

La configuration de Cloud Connect est terminée, Cloud Connect affiche un statut **Connecté**. Vous pouvez ensuite activer des intégrations telles que **ServiceNow** à partir de la page de configuration de **Cloud Connect**.

Prise en charge de la configuration du proxy pour Cloud Connect

Cloud Connect prend en charge les serveurs proxy non authentifiés et authentifiés. La configuration du serveur proxy est facultative.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- À partir de la version 14.1-66.x de NetScaler Console, Cloud Connect prend en charge l'interception SSL pour les déploiements de proxy explicites. Téléchargez le certificat CA du proxy pour établir une communication fiable. Pour plus d'informations sur la gestion des certificats pour les configurations activées par proxy avec inspection SSL, consultez Gérer le certificat CA.
- Le type d'authentification de base est pris en charge.
- Les types de configuration de proxy suivants sont pris en charge :
  - Proxy explicite direct (non-interception)
  - Proxy explicite d'interception SSL
  - Proxy transparent d'interception SSL

  Pour plus d'informations sur les types de configuration de proxy, consultez Prise en charge de la configuration du proxy.
- Assurez-vous que le proxy est configuré pour autoriser les connexions WebSocket, car Cloud Connect nécessite une communication WebSocket pour certaines opérations de service.

1. Sur la page de configuration de Cloud Connect, cliquez sur **Cliquer pour configurer le serveur proxy**.

   

2. Activez le proxy et saisissez l'adresse IP/FQDN et le port.
3. Si nécessaire, ajoutez un `Username` et un `Password`.

   

État de Cloud Connect et comportement d'actualisation

État de Cloud Connect

L'état de Cloud Connect reflète la santé actuelle de la connexion entre NetScaler Console sur site et Citrix Cloud. Les états pris en charge sont :

- **Connecté** – La connexion est saine et fonctionne normalement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Déconnecté** – La connexion est intentionnellement déconnectée.
- **En attente** – Cloud Connect est en cours d'établissement.
- **Erreur** – Un problème est détecté avec la connexion Cloud Connect.

Actualiser l'état de Cloud Connect

L'état de Cloud Connect est automatiquement actualisé toutes les six heures. Les administrateurs peuvent également utiliser **Actualiser l'état de Cloud Connect** pour déclencher une mise à jour immédiate de l'état.

L'action d'actualisation vérifie l'accessibilité des URL de service cloud requises.

REMARQUE :

À partir de la version 14.1-73.x de NetScaler Console, l'actualisation est fusionnée avec **Vérifier la connectivité**.

Diagnostics de Cloud Connect

L'outil de diagnostic **Vérifier la connectivité** aide les administrateurs à résoudre les problèmes de connectivité entre NetScaler Console sur site et le service NetScaler Console.

L'outil **Vérifier la connectivité** effectue les vérifications suivantes :

- Vérifications de l'accessibilité pour tous les points de terminaison de service Cloud Connect requis.
- Validation de la connectivité via les paramètres de proxy configurés, le cas échéant.
- **Validation de la connectivité WebSocket :** Vérifie la communication WebSocket que Cloud Connect utilise pour maintenir une connectivité persistante avec les services cloud. Dans NetScaler Console version 14.1-72.x et antérieures, cette vérification était effectuée dans le cadre de l'action Actualiser.
- **Validation du téléchargement et du téléversement de fichiers factices :** Vérifie la communication de bout en bout pour toutes les fonctionnalités de Cloud Connect, telles que la licence basée sur LAS. Dans NetScaler Console version 14.1-72.x et antérieures, cette vérification était effectuée dans le cadre de l'action Actualiser.

Les résultats du diagnostic incluent les informations suivantes :

- Chaque URL de service est affichée comme « Accessible » ou « Non accessible ».

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Toutes les défaillances sont affichées directement dans l'interface utilisateur avec des messages d'erreur descriptifs.

Après avoir résolu les problèmes de réseau ou de proxy, les administrateurs doivent effectuer les actions suivantes :

- Réexécuter **Vérifier la connectivité**.
- Utiliser **Actualiser l'état de Cloud Connect** pour mettre à jour l'état global de la connexion.

Vous pouvez exécuter **Vérifier la connectivité** en saisissant le CCID, même si Cloud Connect n'est pas encore entièrement établi ou connecté. Cette étape permet de confirmer que toutes les conditions préalables sont remplies avant de se connecter à Cloud Connect.

Cliquez sur **Vérifier la connectivité** pour vérifier la connexion à votre CCID en saisissant le CCID et assurez-vous que toutes les conditions préalables sont remplies, même avant que Cloud Connect ne soit entièrement établi.

Cliquez sur **Afficher les prérequis** pour afficher tous les prérequis pour Cloud Connect.

Gestion des erreurs et messagerie

En fonction des diagnostics et de la validation du proxy, les erreurs suivantes peuvent être observées :

- **Échec de la vérification du certificat SSL** – Indique un certificat d'autorité de certification proxy manquant ou non valide. Cette erreur se produit lorsqu'un proxy d'interception SSL est utilisé et que le certificat d'autorité de certification proxy n'est pas téléchargé sur la console.
- **URL de service requise inaccessible** – Indique que la configuration du proxy ne fonctionne pas correctement ou que les URL requises ne sont pas autorisées sur le réseau.

Notifications pour l'état de Cloud Connect

NetScaler Console génère des notifications pour informer les administrateurs des changements d'état de Cloud Connect. Ces notifications alertent les administrateurs sur les problèmes de connectivité de Cloud Connect qui pourraient avoir un impact sur les fonctionnalités dépendantes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de Cloud Connect, telles que les avis de mise à niveau, la livraison d'actifs, les services basés sur la télémétrie et les intégrations.

Les notifications Cloud Connect sont déclenchées lorsqu'il y a un changement dans l'état de la connexion entre NetScaler Console sur site et Citrix Cloud, notamment :

- Lorsque Cloud Connect passe de Connecté à Déconnecté ou Erreur
- Lorsque Cloud Connect passe de Déconnecté ou Erreur à Connecté

Vous pouvez également consulter les événements d'état de Cloud Connect sous **Paramètres > Événements système**.



Fréquence des notifications

Si Cloud Connect reste dans un état `Disconnected` ou `Error`, des notifications sont envoyées toutes les six heures. Lorsque la connectivité Cloud Connect est rétablie, une seule notification est envoyée pour indiquer la récupération.

Canaux de notification

Les notifications Cloud Connect sont transmises via le cadre de notification standard de NetScaler Console et peuvent être configurées à l'aide de **Notifications d'événements système**. Les canaux de notification pris en charge incluent :

- E-mail
- Slack
- PagerDuty
- ServiceNow

Gestion des notifications

Les notifications d'état Cloud Connect sont activées par défaut. Vous pouvez désactiver les notifications par e-mail si nécessaire. Pour désactiver les notifications par e-mail :

1. Accédez à **Paramètres > Administration > Configurer la notification et le résumé des événements**.
2. Sous **Notification d'événements > Configurer les notifications système**, recherchez **CloudConnectStatus**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Supprimez la catégorie d'événement système **CloudConnectStatus** et cliquez sur **Enregistrer**.



Données collectées via Cloud Connect

IMPORTANT :

Cloud Connect n'est pas le canal du programme de télémétrie NetScaler. La télémétrie est collectée à l'aide d'un canal activé automatiquement. Pour plus d'informations sur la télémétrie, consultez Programme de télémétrie NetScaler.

Lorsque Cloud Connect est activé sur NetScaler Console sur site et que vous utilisez des versions compatibles LAS, LAS est automatiquement activé. Pour plus de détails sur les informations collectées dans le cadre du workflow lié à LAS, consultez Service d'activation de licence.

Dépannage des problèmes de connectivité Cloud Connect

- Problème : Fenêtre contextuelle bloquée lors de la connexion

  Solution : Désactivez le bloqueur de fenêtres contextuelles du navigateur et réessayez l'intégration de Cloud Connect.

- Problème : Points de terminaison bloqués

  Solution : Vérifiez la liste d'autorisation pour les domaines Download/Trust/Service et Citrix Cloud (ou les équivalents de la région Japon).

- Problème : Avertissements de période de grâce LAS

  Assurez-vous que NetScaler Console sur site peut atteindre Citrix Cloud (directement ou via un proxy). Le blob d'autorisation se rafraîchit automatiquement ; des échecs répétés déclenchent la période de grâce et des alertes.

Autres options

Après avoir activé Cloud Connect, vous pouvez utiliser les options suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Modifier le locataire** : vous permet de modifier le locataire existant. Lorsque vous cliquez sur **Modifier le locataire**, vous êtes redirigé vers un nouvel onglet et vous devez vous connecter à Citrix Cloud. Après une connexion réussie, vous pouvez sélectionner un autre locataire.

  

- **Modifier le proxy** - Permet de configurer les paramètres de proxy dans NetScaler Console sur site. Cette action est requise lorsque NetScaler Console n'a pas d'accès direct à Internet via le réseau de gestion. Cliquez sur **Modifier le proxy** dans la liste, mettez à jour les détails, puis cliquez sur **Enregistrer**.

  

- **Déconnecter** - Désactive la fonctionnalité Cloud Connect. Si vous choisissez de désactiver, toutes les fonctionnalités activées dans le cadre de Cloud Connect cessent de fonctionner.

  Pour désactiver, cliquez sur **Déconnecter** dans la liste.

  

- **Paramètres de connectivité** - La désactivation de ce paramètre désactive les vérifications de validation de téléchargement et de téléversement de fichiers d'échantillon. Par conséquent, les problèmes qui pourraient affecter des fonctionnalités telles que la licence LAS pourraient ne pas être détectés de manière proactive.

  

Comportement des fonctionnalités spécifiques à la version

Le tableau suivant présente la disponibilité des fonctionnalités via Cloud Connect dans les différentes versions sur site de NetScaler Console :

VERSION	FONCTIONNALITÉ DISPONIBLE DANS CLOUD CONNECT	ACTION REQUISE	COLLECTE DE DONNÉES VIA CLOUD CONNECT
14.1-66.x et versions ultérieures	Licences basées sur LAS	Configurer Cloud Connect	Non
	Intégration ServiceNow		
	Livraison d'actifs		

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERSION	FONCTIONNALITÉ DISPONIBLE DANS CLOUD CONNECT	ACTION REQUISE	COLLECTE DE DONNÉES VIA CLOUD CONNECT
	Avis de mise à niveau		
14.1-56.x et versions ultérieures	Licences basées sur LAS	Configurer Cloud Connect	Non
	Intégration ServiceNow		
	Livraison d'actifs		
14.1-51.x et versions ultérieures	Licences basées sur LAS	Configurer Cloud Connect	Non
	Intégration ServiceNow		
14.1-25.x et versions ultérieures	Intégration ServiceNow	Configurez Cloud Connect et activez l'intégration ServiceNow.	Non
Entre 14.1-8.x et 14.1-21.x	Avis de sécurité et intégration ServiceNow	Configurez Cloud Connect et activez la fonctionnalité	Oui. Après avoir configuré Cloud Connect. Pour plus d'informations, consultez Gouvernance des données pour Cloud Connect
14.1-4.x ou version antérieure	N/A	NA	NA

FAQ

1. Quelles sont les URL exactes qui doivent être ajoutées à la liste verte sur l'ordinateur portable ?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour garantir une connectivité appropriée, ajoutez les URL suivantes à la liste verte de votre navigateur en fonction de votre environnement de compte de service NetScaler Console :

- Cloud commercial
  - Service de confiance
  - Citrix Cloud
  - Comptes Citrix Cloud
- Cloud Japon
  - Service de confiance
  - Citrix Cloud
  - Comptes Citrix Cloud
- Cloud gouvernemental
  - Service de confiance
  - Citrix Cloud

2. Cloud Connect pousse-t-il la configuration vers mes instances NetScaler ?

   Non. Cloud Connect ne pousse pas la configuration vers les instances NetScaler ; il active uniquement les services fournis via le cloud pour NetScaler Console sur site et facilite la livraison des licences ou des actifs.

3. Existe-t-il une connectivité entrante depuis Citrix Cloud vers mon environnement ?

   Non. Cloud Connect utilise une communication uniquement sortante initiée depuis NetScaler Console sur site.

4. Est-il nécessaire de migrer les instances NetScaler vers le service NetScaler Console ?

   Non. Vous n'avez pas besoin de migrer les instances vers le service NetScaler Console pour utiliser les fonctionnalités de Cloud Connect.

5. Quels types d'authentification proxy sont pris en charge ?

   Cloud Connect peut être utilisé via un proxy. Nous prenons en charge l'intégration de proxy avec authentification de base ou sans authentification.

6. Le Security Advisory est-il toujours activé via Cloud Connect ?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Uniquement sur certaines versions plus anciennes de 14.1 (8.x à 21.x). Dans les versions ultérieures, Cloud Connect active principalement les fonctionnalités décrites dans cette rubrique. À partir de la version 14.1-25.x, Security Advisory peut être utilisé via un canal activé automatiquement. Pour plus d'informations, consultez Mode de collecte de télémétrie automatisée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer

Vous pouvez accéder à un serveur NetScaler Console uniquement en utilisant l'interface graphique. Vous devez accéder à l'interface graphique pour ajouter des instances, gérer et surveiller vos instances et applications, afficher les analyses et configurer le serveur NetScaler Console.

Votre poste de travail doit disposer d'un navigateur web pris en charge pour accéder à l'utilitaire de configuration et au tableau de bord.

Les navigateurs suivants sont pris en charge.

NAVIGATEUR WEB	VERSION
Internet Explorer	11.0 et versions ultérieures
Google Chrome	Chrome 19 et versions ultérieures
Safari	Safari 5.1.1 et versions ultérieures
Mozilla Firefox	Firefox 3.6.25 et versions ultérieures

Pour accéder à l'interface graphique de NetScaler Console :

Connectez-vous à NetScaler Console en utilisant les informations d'identification de l'administrateur.

Après vous être connecté à NetScaler Console, vous devez effectuer les opérations suivantes pour commencer :

- Ajouter des instances à NetScaler Console. Vous devez ajouter des instances au serveur NetScaler Console si vous souhaitez gérer et surveiller ces instances.
- Activer l'analyse sur les serveurs virtuels. Pour afficher les données d'analyse du flux de trafic de votre application, vous devez activer la fonctionnalité d'analyse sur les serveurs virtuels qui reçoivent le trafic pour les applications spécifiques.
- Configurer le serveur NTP sur NetScaler Console. Vous devez configurer un serveur NTP (Network Time Protocol) dans NetScaler Console pour synchroniser son horloge avec le serveur NTP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Configurer les paramètres système pour des performances optimales de NetScaler Console. Avant de commencer à utiliser NetScaler Console pour gérer et surveiller vos instances et applications, il est recommandé de configurer quelques paramètres système qui garantissent des performances optimales de votre serveur NetScaler Console.

Ajouter des instances à NetScaler Console

Les instances sont des appliances NetScaler ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller depuis NetScaler Console. Vous devez ajouter des instances au serveur NetScaler Console si vous souhaitez gérer et surveiller ces instances. Vous pouvez ajouter les appliances NetScaler et les appliances virtuelles suivantes à NetScaler Console :

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler Console ou ultérieurement. Vous devez ensuite spécifier un profil d'instance que NetScaler Console peut utiliser pour accéder à l'instance.

REMARQUE :

- NetScaler Console utilise l'adresse IP NetScaler (NSIP) des instances NetScaler pour la communication. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances NetScaler et NetScaler Console, consultez Ports.
- Pour savoir comment NetScaler Console découvre les instances, consultez Découvrir les instances.

Comment créer un profil NetScaler

Le profil NetScaler inclut les informations d'identification, les ports et les types d'authentification pour l'ajout d'instances à NetScaler Console. Pour chaque type d'instance, un profil par défaut est disponible. Par exemple, `nsroot` est le profil par défaut pour les instances NetScaler. Le profil par défaut est défini à l'aide des informations d'identification de l'administrateur NetScaler par

© 1997–2026 Citrix Systems, Inc. All rights reserved.

défaut. Si vous avez modifié les informations d'identification d'administrateur par défaut de vos instances, vous pouvez définir des profils d'instance personnalisés pour ces instances. Si vous modifiez les informations d'identification d'une instance après sa découverte, vous devez modifier le profil d'instance ou créer un profil, puis redécouvrir l'instance.

Vous pouvez créer un profil NetScaler à partir de la page **Instance** ou lors de l'ajout ou de la modification d'une instance.

REMARQUE :

Assurez-vous d'utiliser le compte super administrateur pour créer un profil d'instance.

Pour créer un profil NetScaler à partir de la page Instance :

1. Accédez à **Infrastructure > Instances**.
2. Sélectionnez une instance. Par exemple, NetScaler.
3. Sur la page NetScaler, sous **Sélectionner une action**, sélectionnez **Profils**.

   
4. Sur la page **Profils d'administration**, sélectionnez **Ajouter**.

   
5. Sur la page **Créer un profil NetScaler**, effectuez les opérations suivantes :

   
   a. **Nom du profil** : Spécifiez un nom de profil pour l'instance NetScaler.
   b. **Nom d'utilisateur** : Spécifiez un nom d'utilisateur pour vous connecter à l'instance NetScaler.
   c. **Mot de passe** : Spécifiez un mot de passe pour vous connecter à l'instance NetScaler.
   d. **Port SSH** : Spécifiez le port pour la communication SSH entre NetScaler Console et l'instance NetScaler.
   e. **Port HTTP** : Spécifiez le port pour la communication HTTP entre NetScaler Console et l'instance NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Le port HTTP par défaut est 80. Vous pouvez également spécifier le port HTTP non par défaut ou personnalisé que vous avez peut-être configuré dans votre instance NetScaler CPX. Le port HTTP personnalisé ne peut être utilisé que pour la communication entre NetScaler Console et NetScaler CPX.

f. **Port HTTPS** : Spécifiez le port pour la communication HTTPS entre NetScaler Console et l'instance NetScaler.

REMARQUE

Le port HTTPS par défaut est 443. Vous pouvez également spécifier le port HTTPS non par défaut ou personnalisé que vous avez peut-être configuré dans votre instance NetScaler CPX. Le port HTTPS personnalisé ne peut être utilisé que pour la communication entre NetScaler Console et NetScaler CPX.

g. **Utiliser les paramètres globaux pour la communication NetScaler** : Sélectionnez cette option si vous souhaitez utiliser les paramètres système pour la communication entre NetScaler Console et l'instance NetScaler, sinon sélectionnez HTTP ou HTTPS.

h. **Version SNMP** : Sélectionnez **SNMPv2** ou **SNMPv3** et effectuez les opérations suivantes :

   i. Si vous sélectionnez SNMPv2, spécifiez le nom de la **communauté** pour l'authentification.

   ii. Si vous sélectionnez SNMPv3, spécifiez le **nom de sécurité** et le **niveau de sécurité**. En fonction du niveau de sécurité, sélectionnez le **type d'authentification** et le **type de confidentialité**.

REMARQUE

Pour NetScaler SDX, seul **SNMPv2** est pris en charge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. **Paramètres de délai d'expiration** : Spécifiez le temps que NetScaler Console doit attendre avant d'envoyer une demande de connexion à l'instance NetScaler après un redémarrage.

j. Sélectionnez **Créer**.

Ajouter des instances NetScaler à NetScaler Console

Vous pouvez ajouter des instances soit lors de la première configuration du serveur NetScaler Console, soit ultérieurement.

Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance NetScaler, ou une plage d'adresses IP.

REMARQUE :

- Pour ajouter des instances NetScaler configurées dans un cluster, vous devez spécifier l'adresse IP du cluster ou l'un des nœuds individuels de la configuration du cluster. Cependant, sur NetScaler Console, le cluster est représenté uniquement par l'adresse IP du cluster.
- Pour les instances NetScaler configurées en paire HA, lorsque vous ajoutez une instance, l'autre instance de la paire est automatiquement ajoutée.

Lorsque vous ajoutez une instance à partir de données distantes configurées avec un agent, la source du trafic passe par l'agent.

Pour ajouter une instance à NetScaler Console :

1. Connectez-vous à NetScaler Console avec les informations d'identification de l'administrateur.
2. Accédez à **Infrastructure > Instances > NetScaler**. Sélectionnez le type d'instance que vous souhaitez ajouter (par exemple, NetScaler VPX) et cliquez sur **Ajouter**.

   

3. Sélectionnez l'une des options suivantes :

   - **Entrer l'adresse IP du périphérique** - Pour les instances NetScaler, spécifiez l'un des éléments suivants :

     - Nom d'hôte
     - Adresse IP ou IP NAT de chaque instance NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Plage d'adresses IP

  Par exemple, saisissez un ou plusieurs noms d'hôte, adresses IP ou IP NAT, et/ou une plage d'adresses IP (par exemple, 10.10.20.10-10.10.20.45) en utilisant un séparateur virgule. Le format d'entrée pour la découverte des instances NAT HA est `10.10.20.10#10.10.20.32` (adresse IP NAT des deux instances NetScaler HA)

  Si vous souhaitez découvrir une paire HA NetScaler à l'aide de SNIP, assurez-vous que le mode de configuration réseau indépendant (INC) est activé. Et, spécifiez les adresses SNIP au format suivant :

```
<SNIP of primary instance>#<SNIP of secondary instance>
```

- **Importer depuis un fichier** - Depuis votre système local, téléchargez un fichier texte contenant les adresses IP de toutes les instances que vous souhaitez ajouter.

4. Dans **Nom du profil**, sélectionnez le profil d'instance approprié, ou créez un profil en cliquant sur l'icône +.
5. Dans **Site**, sélectionnez l'emplacement où vous souhaitez ajouter l'instance, ou créez un emplacement en cliquant sur l'icône **+**.
6. Cliquez sur **OK** pour démarrer le processus d'ajout d'instances à NetScaler Console.

REMARQUE :

Si vous souhaitez redécouvrir une instance, accédez à **Infrastructure > Instances > NetScaler**. Sélectionnez le type d'instance (par exemple, VPX) et sélectionnez l'instance que vous souhaitez redécouvrir, puis, dans la liste **Sélectionner une action**, cliquez sur **Redécouvrir**.

Ajouter des instances NetScaler CPX à NetScaler Console

NetScaler Console a été amélioré pour prendre en charge les améliorations apportées aux fonctionnalités de CPX. L'instance NetScaler CPX est désormais ajoutée dans NetScaler Console en fournissant une adresse IP pour le CPX ainsi qu'un profil de périphérique. Le processus d'ajout d'une instance CPX est désormais similaire à la façon dont d'autres types de NetScaler, tels que VPX ou MPX, sont ajoutés dans NetScaler Console. De plus, l'enregistrement de CPX dans NetScaler Console a été amélioré. Lorsqu'un CPX démarre, NetScaler Console découvre et

© 1997–2026 Citrix Systems, Inc. All rights reserved.

enregistre automatiquement l'instance CPX. Une instance CPX n'est plus découverte via l'hôte Docker.

1. Accédez à **Infrastructure > Instances > NetScaler** et cliquez sur **CPX**.
2. Cliquez sur **Ajouter** pour ajouter de nouvelles instances CPX dans NetScaler Console.
3. La page **Ajouter NetScaler CPX** s'ouvre. Saisissez les valeurs pour les paramètres suivants :

   a. Vous pouvez ajouter des instances CPX en fournissant soit l'adresse IP accessible de l'instance CPX, soit l'adresse IP du conteneur Docker où l'instance CPX est hébergée.

   b. Sélectionnez le profil de l'instance CPX.

   c. Sélectionnez le site où les instances doivent être déployées.

   d. Sélectionnez l'agent.

   e. En option, vous pouvez saisir la paire clé-valeur pour l'instance. L'ajout d'une paire clé-valeur vous permet de rechercher facilement l'instance ultérieurement.

   Ajouter NetScaler CPX(/en-us/netscaler-application-delivery-management-software/media/add-cpx-instances.png)

   REMARQUE :

   Pour les instances NetScaler CPX, vous devez spécifier les détails des ports **HTTP, HTTPS, SSH** et **SNMP** de l'hôte lors de la création du profil d'instance CPX. Vous pouvez également spécifier la plage de ports publiés par l'hôte dans les champs **Port de début** et **Nombre de ports**.

4. Cliquez sur **OK**.

Ajouter une instance NetScaler BLX autonome dans NetScaler Console

Une instance NetScaler BLX autonome est une instance unique qui s'exécute sur le serveur Linux hôte dédié.

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Dans l'onglet **BLX**, cliquez sur **Ajouter**.
3. Sélectionnez l'option **Autonome** dans la liste **Type d'instance**.
4. Dans le champ **Adresse IP**, spécifiez l'adresse IP de l'instance BLX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Dans le champ **Adresse IP de l'hôte**, spécifiez l'adresse IP du serveur Linux où l'instance BLX est hébergée.
6. Dans la liste **Nom du profil**, sélectionnez le profil approprié pour une instance BLX, ou créez un profil.

   Pour créer un profil, cliquez sur **Ajouter**.

   IMPORTANT :

   Assurez-vous d'avoir spécifié le nom d'utilisateur et le mot de passe corrects de l'hôte du serveur Linux dans le profil.

7. Dans la liste **Site**, sélectionnez le site où vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.
8. Dans la liste **Agent**, sélectionnez l'agent NetScaler auquel vous souhaitez associer l'instance.

   Si un seul agent est configuré sur votre NetScaler Console, cet agent est sélectionné par défaut.
9. Cliquez sur **OK**.

Ajouter des instances NetScaler BLX haute disponibilité dans NetScaler Console

Les instances NetScaler BLX haute disponibilité qui s'exécutent sur différents serveurs hôtes Linux. Un serveur Linux ne peut pas héberger plus d'une instance BLX.

1. Dans l'onglet **BLX**, cliquez sur **Ajouter**.
2. Sélectionnez l'option **Haute disponibilité** dans la liste **Type d'instance**.
3. Dans le champ **Adresse IP**, spécifiez l'adresse IP de l'instance BLX.
4. Dans le champ **Adresse IP de l'hôte**, spécifiez l'adresse IP du serveur Linux où l'instance BLX est hébergée.
5. Dans le champ **Adresse IP du pair**, spécifiez l'adresse IP de l'instance BLX paire.
6. Dans le champ **Adresse IP de l'hôte pair**, spécifiez l'adresse IP du serveur Linux où l'instance BLX paire est hébergée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Dans la liste **Nom du profil**, sélectionnez le profil approprié pour une instance BLX, ou créez un profil.

   Pour créer un profil, cliquez sur **Ajouter**.

   IMPORTANT :

   Assurez-vous de spécifier le nom d'utilisateur et le mot de passe corrects de l'hôte du serveur Linux dans le profil.

8. Dans la liste **Site**, sélectionnez le site où vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.

9. Dans la liste **Agent**, sélectionnez l'agent NetScaler auquel vous souhaitez associer l'instance.

   S'il n'y a qu'un seul agent configuré sur votre NetScaler Console, cet agent est sélectionné par défaut.

10. Cliquez sur **OK**.



Accéder à l'interface graphique d'une instance depuis la NetScaler Console

1. Accédez à **Infrastructure > Instances** > **NetScaler**.
2. Sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, VPX, MPX, CPX, SDX ou BLX).
3. Cliquez sur l'adresse IP ou le nom d'hôte NetScaler requis.



L'interface graphique de l'instance sélectionnée s'affiche dans une fenêtre contextuelle.

Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler Console

Vous pouvez utiliser NetScaler Console pour gérer et surveiller les instances NetScaler VPX déployées sur un cloud public tel qu'Amazon Web Services (AWS), Microsoft Azure ou Google Cloud. Vous devez établir une connectivité de couche 3 entre NetScaler Console et les instances NetScaler VPX déployées sur le cloud public. Pour établir la connectivité de couche 3, vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pouvez utiliser des solutions telles que Direct Connect vers AWS, VPN dans Azure, ou des connecteurs tiers tels qu'Equinix, etc.

La topologie d'exemple suivante utilise Citrix CloudBridge Connector pour la connectivité de couche 3 entre NetScaler Console et les instances NetScaler VPX déployées dans le cloud.



Un tunnel Citrix CloudBridge Connector est configuré entre l'appliance NetScaler NS_Appliance-DC, dans un centre de données DC, et l'appliance virtuelle NetScaler (VPX) NS_VPX_CBC dans le cloud public. NS_Appliance-DC et NS_VPX_CBC permettent la communication entre NetScaler Console et l'instance NetScaler VPX, NS_VPX_1, déployée dans le cloud public. Une fois la communication établie, vous pouvez découvrir NS_VPX_1 dans NetScaler Console.

Pour configurer cette topologie :

1. Installez, configurez et démarrez une instance NetScaler VPX dans le cloud public.
    - Pour obtenir des instructions, consultez Installer NetScaler VPX sur AWS.
    - Pour obtenir des instructions, consultez Installer NetScaler VPX sur Microsoft Azure.
    - Pour obtenir des instructions, consultez Installer NetScaler VPX sur Google Cloud.
2. Déployez et configurez une appliance physique NetScaler, ou provisionnez et configurez une appliance virtuelle NetScaler (VPX) sur une plateforme de virtualisation dans le centre de données.
    - Pour obtenir des instructions, consultez Installer une instance NetScaler VPX sur Citrix Hypervisor.
    - Pour obtenir des instructions, consultez Installer les appliances virtuelles Citrix sur VMware ESXi.
    - Pour obtenir des instructions, consultez Installer les appliances virtuelles NetScaler sur Microsoft Hyper-V.
3. Configurez le Citrix CloudBridge Connector entre le centre de données et le cloud public. Pour obtenir des instructions, consultez Configuration de Citrix CloudBridge Connector.
4. Configurez la route statique pour établir la connexion entre NetScaler Console et les instances NetScaler VPX déployées sur le cloud, comme suit :
    a. Connectez-vous à NetScaler Console.
    b. Accédez à **Système \> Routes statiques** et cliquez sur **Ajouter**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Dans le champ **Adresse réseau**, saisissez l'adresse du réseau pour lequel vous souhaitez établir une route statique depuis NetScaler Console via le connecteur.

d. Dans le champ **Masque de sous-réseau**, saisissez le masque de sous-réseau du réseau.

e. Dans le champ **Passerelle**, saisissez l'adresse de la passerelle.

5. Ajoutez les instances cloud NetScaler VPX à NetScaler Console en spécifiant la plage d'adresses IP des instances NetScaler VPX dans le cloud public. Pour des instructions détaillées, Ajouter des instances à NetScaler Console.

Configurer les analyses

- Pour les versions jusqu'à 14.1-17.x(/fr-fr/netscaler-application-delivery-management-software/current-release/configure/enable-analytics-on-virtual-servers.html)
- Pour les versions 14.1-21.x ou ultérieures(/fr-fr/netscaler-application-delivery-management-software/current-release/configure/enable-analytics-for-flexed-license.html)

Gérer les licences et activer l'analyse sur les serveurs virtuels

REMARQUE

- Par défaut, l'option **Serveurs virtuels sous licence automatique** est activée. Vous devez vous assurer de disposer de licences suffisantes pour les serveurs virtuels. Si vous disposez de licences limitées et que vous souhaitez n'attribuer des licences qu'à certains serveurs virtuels en fonction de vos besoins, désactivez l'option **Serveurs virtuels sous licence automatique**. Accédez à **Paramètres > Configuration des licences et de l'analyse** et désactivez l'option **Serveurs virtuels sous licence automatique** sous **Attribution de licences de serveurs virtuels**.

Le processus d'activation de l'analyse est simplifié. Vous pouvez attribuer une licence au serveur virtuel et activer l'analyse en un seul flux de travail.

Accédez à **Paramètres > Configuration des licences et de l'analyse** pour :

- Afficher le **Résumé des licences de serveurs virtuels**
- Afficher le **Résumé de l'analyse des serveurs virtuels**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque vous cliquez sur **Configurer la licence** ou **Configurer l'analyse**, la page **Tous les serveurs virtuels** s'affiche.



Sur la page **Tous les serveurs virtuels**, vous pouvez :

- Appliquer une licence pour les serveurs virtuels sans licence
- Supprimer la licence pour les serveurs virtuels sous licence
- Activer l'analyse sur les serveurs virtuels sous licence
- Modifier l'analyse
- Désactiver l'analyse

REMARQUE

Les serveurs virtuels pris en charge pour activer l'analyse sont l'équilibrage de charge, la commutation de contenu et NetScaler Gateway.

Gérer les licences sur les serveurs virtuels

Pour attribuer une licence aux serveurs virtuels, depuis la page **Tous les serveurs virtuels** :

1. Cliquez sur la barre de recherche, sélectionnez **Sous licence**, puis sélectionnez **Non**.

   

   Le filtre est maintenant appliqué et seuls les serveurs virtuels sans licence sont affichés.
2. Sélectionnez les serveurs virtuels, puis cliquez sur **Licence**.

   

Pour retirer la licence des serveurs virtuels, depuis la page **Tous les serveurs virtuels** :

1. Cliquez sur la barre de recherche, sélectionnez **Sous licence**, puis sélectionnez **Oui**.
2. Sélectionnez les serveurs virtuels et cliquez sur **Retirer la licence**.

Activer l'analyse

Voici les prérequis pour activer l'analyse pour les serveurs virtuels :

- Assurez-vous que les serveurs virtuels sont **sous licence**
- Assurez-vous que l'état de l'analyse est **Désactivé**
- Assurez-vous que les serveurs virtuels sont à l'état **UP**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez filtrer les résultats pour identifier les serveurs virtuels mentionnés dans les prérequis.

1. Cliquez sur la barre de recherche, sélectionnez **État**, puis sélectionnez **UP**.
2. Cliquez sur la barre de recherche, sélectionnez **Sous licence**, puis sélectionnez **Oui**.
3. Cliquez sur la barre de recherche, sélectionnez **État de l'analyse**, puis sélectionnez **Désactivé**.
4. Après avoir appliqué les filtres, sélectionnez les serveurs virtuels, puis cliquez sur **Activer l'analyse**.

   REMARQUE

   Vous pouvez également activer l'analyse pour une instance particulière :

   a. Accédez à **Infrastructure > Instances > NetScaler**, puis sélectionnez le type d'instance. Par exemple, VPX.
   b. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.
   c. Sur la page Configurer l'analyse sur les serveurs virtuels, sélectionnez le serveur virtuel et cliquez sur **Activer l'analyse**.

5. Dans la fenêtre **Activer l'analyse** :

   a. Sélectionnez les types d'informations (Web Insight ou Violations de sécurité WAF)
   b. Sélectionnez **Logstream** comme mode de transport

      REMARQUE

      Pour NetScaler 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour NetScaler 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.

      Pour plus d'informations sur IPFIX et Logstream, consultez Présentation de Logstream.

   c. Sous **Options au niveau de l'instance** :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Activer HTTP X-Forwarded-For** - Sélectionnez cette option pour identifier l'adresse IP de la connexion entre le client et l'application, via un proxy HTTP ou un équilibreur de charge.
- **NetScaler Gateway** - Sélectionnez cette option pour afficher les analyses pour NetScaler Gateway.

d. L'expression est vraie par défaut

e. Cliquez sur **OK**

REMARQUE

- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, NetScaler Console attribue d'abord une licence à ces serveurs virtuels, puis active les analyses.
- Pour les partitions d'administration, seul **Web Insight** est pris en charge.
- Pour les serveurs virtuels tels que la redirection de cache, l'authentification et GSLB, vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, NetScaler Console traite l'activation des analyses sur les serveurs virtuels sélectionnés.

REMARQUE

NetScaler Console utilise NetScaler SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre l'agent NetScaler et l'instance NetScaler, assurez-vous d'ouvrir le port suivant pour permettre à NetScaler Console de collecter le trafic AppFlow :

MODE DE TRANSPORT	IP SOURCE	TYPE	PORT
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modifier les analyses

Pour modifier les analyses sur les serveurs virtuels :

1. Sélectionnez les serveurs virtuels

   Remarque

   Vous pouvez également modifier les analyses pour une instance particulière :

   a. Accédez à **Infrastructure > Instances > NetScaler**, puis sélectionnez le type d'instance. Par exemple, VPX.

   b. Sélectionnez l'instance et cliquez sur **Modifier les analyses**.

2. Cliquez sur **Modifier les analyses**
3. Modifiez les paramètres que vous souhaitez appliquer dans la fenêtre **Modifier la configuration des analyses**
4. Cliquez sur **OK**.

Désactiver les analyses

Pour désactiver les analyses sur les serveurs virtuels sélectionnés :

1. Sélectionnez les serveurs virtuels
2. Cliquez sur **Désactiver les analyses**

NetScaler Console désactive les analyses sur les serveurs virtuels sélectionnés

Le tableau suivant décrit les fonctionnalités de NetScaler Console qui prennent en charge IPFIX et Logstream comme mode de transport :

FONCTIONNALITÉ	IPFIX	LOGSTREAM
Web Insight	•	•
Violations de sécurité WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉ	IPFIX	LOGSTREAM
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Configurer l'analyse globalement

Outre le processus existant pour activer l'analyse, vous pouvez également utiliser un flux de travail à volet unique pour configurer l'analyse sur :

- Tous les serveurs virtuels sous licence existants
- Les serveurs virtuels sous licence ultérieurs

Après la configuration, cette fonctionnalité élimine la nécessité d'activer manuellement l'analyse sur les serveurs virtuels existants et ultérieurs.

Points à noter :

Avant de configurer l'analyse, vous devez comprendre les comportements suivants de NetScaler Console :

- Lorsque vous configurez cette fonctionnalité pour la première fois, vous devez vous assurer que les prérequis mentionnés dans ce document sont remplis.
- Modifier les paramètres d'analyse ultérieurement.

  Considérez que vous avez configuré les paramètres d'analyse pour la première fois en sélectionnant Web Insight, HDX™ Insight et Gateway Insight. Si vous souhaitez modifier les paramètres d'analyse ultérieurement et désélectionner Gateway Insight, les modifications n'affectent pas les serveurs virtuels déjà activés avec l'analyse.
- Les serveurs virtuels déjà activés avec l'analyse.

  Supposons que vous ayez 10 serveurs virtuels sous licence et que deux d'entre eux soient déjà activés avec l'analyse. Dans ce scénario, cette fonctionnalité active l'analyse uniquement pour les huit serveurs virtuels restants.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Les serveurs virtuels qui sont désactivés manuellement avec l'analyse.

  Supposons que vous ayez 10 serveurs virtuels sous licence et que vous ayez désactivé manuellement l'analyse pour deux serveurs virtuels. Dans ce scénario, cette fonctionnalité active l'analyse uniquement pour les huit serveurs virtuels restants et ignore les serveurs virtuels qui sont désactivés manuellement avec l'analyse.
- **Violations de sécurité des bots** et **Violations de sécurité WAF** sont prises en charge uniquement sur les serveurs virtuels sous licence premium. Si les serveurs virtuels ne sont pas sous licence premium, alors **Violations de sécurité des bots** et **Violations de sécurité WAF** ne sont pas activées.

Prérequis

Assurez-vous que :

- Tous les serveurs virtuels existants sont sous licence.
- L'option de licence automatique est activée pour attribuer une licence à tous les serveurs virtuels ultérieurs. Accédez à **Paramètres > Configuration des licences et de l'analyse** et, sous **Allocation de licence de serveur virtuel**, activez l'option **Serveurs virtuels sous licence automatique**.

Activer l'analyse

1. Accédez à **Paramètres > Configuration des licences et de l'analyse**.
2. Sous **Résumé de l'analyse**, cliquez sur **Configuration globale de l'analyse**.

   
3. Sélectionnez les fonctionnalités d'analyse que vous souhaitez activer sur les serveurs virtuels.
4. Pour activer l'analyse sur les serveurs virtuels ultérieurs, cochez la case **Appliquer ces paramètres d'analyse aux serveurs virtuels sous licence ultérieurs**.
5. Cliquez sur **Soumettre**.

   

Configurer l'analyse sur les serveurs virtuels

La condition préalable pour activer l'analyse est que les serveurs virtuels doivent être sous licence. Si vous utilisez une licence flexible, tous les serveurs virtuels existants et les serveurs virtuels ultérieurs sont automatiquement sous licence. Vous pouvez alors procéder à la configuration de l'analyse.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez configurer l'analyse de deux manières. Accédez à **Paramètres > Configuration de l'analyse** pour afficher :

- **Résumé de l'analyse des serveurs virtuels** - Vous permet de configurer l'analyse sur les serveurs virtuels existants.
- **Résumé de l'analyse globale** - Vous permet de configurer l'analyse sur les serveurs virtuels existants et ultérieurs.



Configurer l'analyse sur les serveurs virtuels existants

REMARQUE :

Assurez-vous que les serveurs virtuels pour lesquels vous souhaitez activer l'analyse sont en état **UP**.

1. Sous **Résumé de l'analyse des serveurs virtuels**, cliquez sur **Configurer l'analyse**.

   La page **Tous les serveurs virtuels** s'affiche. Vous pouvez :

   - Activer l'analyse
   - Modifier l'analyse
   - Désactiver l'analyse

   REMARQUE :

   Les serveurs virtuels pris en charge pour l'activation des analyses sont l'équilibrage de charge, la commutation de contenu et NetScaler Gateway.

2. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer les analyses**.

   

   REMARQUE

   Vous pouvez également activer les analyses pour une instance :

   a. Accédez à **Infrastructure > Instances > NetScaler**, puis sélectionnez le type d'instance. Par exemple, VPX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Configurer les analyses**.

c. Sur la page Configurer les analyses sur les serveurs virtuels, sélectionnez le serveur virtuel et cliquez sur **Activer les analyses**.

3. Dans la fenêtre **Activer les analyses** :

a. Sélectionnez les types d'informations.

b. Sélectionnez **Logstream** comme mode de transport.

> **REMARQUE :**
>
> Pour NetScaler 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour NetScaler 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.

Pour plus d'informations sur IPFIX et Logstream, consultez Présentation de Logstream.

c. Sous **Options au niveau de l'instance** :

- **Activer HTTP X-Forwarded-For** - Sélectionnez cette option pour identifier l'adresse IP de la connexion entre le client et l'application, via un proxy HTTP ou un équilibreur de charge.
- **En-tête personnalisé** - Définissez un en-tête personnalisé tel que X-Real-IP, X-Client-IP ou tout autre en-tête personnalisé pour récupérer l'adresse IP réelle du client au lieu de l'adresse IP du proxy. Assurez-vous que l'instance NetScaler gérée est la version 14.1–38.24 ou ultérieure.
- **NetScaler Gateway** - Sélectionnez cette option pour afficher les analyses pour NetScaler Gateway.

d. L'expression est vraie par défaut.

e. Cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Pour les partitions d'administration, seul **Web Insight** est pris en charge.
- Pour les serveurs virtuels tels que la redirection de cache, l'authentification et le GSLB, vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, NetScaler Console procède à l'activation des analyses sur les serveurs virtuels sélectionnés.

REMARQUE

NetScaler Console utilise NetScaler SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre l'agent NetScaler et l'instance NetScaler, assurez-vous d'ouvrir le port suivant pour permettre à NetScaler Console de collecter le trafic AppFlow :

MODE DE TRANSPORT	IP SOURCE	TYPE	PORT
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Modifier l'analyse

Pour modifier l'analyse sur les serveurs virtuels :

1. Sélectionnez les serveurs virtuels.

   REMARQUE :

   Vous pouvez également modifier l'analyse pour une instance :

   a. Accédez à **Infrastructure > Instances > NetScaler**, puis sélectionnez le type d'instance. Par exemple, VPX.

   b. Sélectionnez l'instance et cliquez sur **Modifier l'analyse**.

2. Cliquez sur **Modifier l'analyse**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Modifiez les paramètres que vous souhaitez appliquer dans la fenêtre **Configuration de l'analyse**.
4. Cliquez sur **OK**.

Désactiver l'analyse

Pour désactiver l'analyse sur les serveurs virtuels sélectionnés :

1. Sélectionnez les serveurs virtuels.
2. Cliquez sur **Désactiver l'analyse**.

NetScaler Console désactive l'analyse sur les serveurs virtuels sélectionnés.

Le tableau suivant décrit les fonctionnalités de NetScaler Console qui prennent en charge IPFIX et Logstream comme mode de transport :

FONCTIONNALITÉ	IPFIX	LOGSTREAM
Web Insight	•	•
Violations de sécurité WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Configurer l'analyse globale

Vous pouvez activer l'analyse globale en créant une politique personnalisée ou une politique globale.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Vous pouvez créer jusqu'à 10 stratégies. Les stratégies peuvent être une combinaison de neuf stratégies personnalisées et d'une stratégie globale, ou de 10 stratégies personnalisées.
- Si vous avez les deux types de stratégies (personnalisée et globale), les informations sélectionnées dans les deux stratégies sont appliquées aux serveurs virtuels. Si vous souhaitez supprimer des informations, vous devez les supprimer manuellement.

Stratégie personnalisée

À l'aide d'une stratégie personnalisée, vous pouvez contrôler les instances ou les serveurs virtuels qui ne nécessitent que des informations spécifiques. Vous pouvez avoir des centaines de serveurs virtuels configurés via diverses instances NetScaler gérées dans votre NetScaler Console. Dans certains scénarios, vous pouvez souhaiter appliquer des informations sélectives (par exemple, les violations de sécurité des bots et les violations de sécurité WAF) uniquement à certains serveurs virtuels ou instances. Pour de tels scénarios, vous pouvez configurer une stratégie personnalisée, sélectionner des fonctionnalités d'analyse spécifiques et l'appliquer aux instances et serveurs virtuels pertinents.

Pour configurer une stratégie personnalisée :

1. Sous **Résumé de l'analyse globale**, cliquez sur **Configuration de l'analyse globale**.

   

2. Sous **Détails de la stratégie**, sélectionnez **Stratégie personnalisée** et spécifiez un nom de stratégie de votre choix.

   REMARQUE :

   Vous ne pouvez pas modifier le nom de la stratégie ultérieurement.

   

3. Sous **Définir les conditions**, créez des conditions en sélectionnant l'ensemble des adresses IP d'instance ou des instances spécifiques ou le nom du serveur virtuel ou les deux.

   

4. Sous **Activer l'analyse**, sélectionnez le type de fonctionnalité d'analyse.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Si vous activez **Appliquer ces paramètres d'analyse aux serveurs virtuels suivants**, l'analyse sera appliquée aux serveurs virtuels suivants en fonction des fonctionnalités d'analyse définies.

5. Cliquez sur **Enregistrer**.

Points à noter :

- Si vous modifiez la stratégie en supprimant une information existante et en ajoutant une autre information, la stratégie mise à jour est appliquée avec la nouvelle information. Si vous souhaitez supprimer une information, vous devez supprimer manuellement les informations déjà configurées.

  Considérez que vous avez créé une stratégie personnalisée avec HDX Insight et Web Insight. Si vous mettez à jour la stratégie pour supprimer HDX Insight et ajouter des violations de sécurité des bots, les serveurs virtuels/instances sont mis à jour avec HDX Insight, Web Insight et les violations de sécurité des bots. Si vous souhaitez supprimer HDX Insight, vous devez le supprimer manuellement à l'aide de l'option modifier l'analyse.
- La même logique est également applicable si vous supprimez une stratégie existante et en créez une autre en ajoutant les mêmes instances ou serveurs virtuels.

Stratégie globale

À l'aide de la stratégie globale, vous pouvez activer l'analyse sur les serveurs virtuels découverts et suivants. Pour créer une stratégie globale :

1. Sous **Résumé de l'analyse globale**, cliquez sur **Configuration de l'analyse globale**.
2. Sous **Détails de la stratégie**, sélectionnez **Stratégie globale**.
3. Sous **Activer l'analyse**, sélectionnez le type de fonctionnalité d'analyse.

REMARQUE :

Si vous activez **Appliquer ces paramètres d'analyse aux serveurs virtuels suivants**, l'analyse sera appliquée aux serveurs virtuels suivants en fonction de la catégorie définie.

4. Cliquez sur **Enregistrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après la configuration, l'analyse est activée sur les serveurs virtuels découverts et les serveurs virtuels ultérieurs.

Points à noter

- Considérez que vous avez configuré la politique globale pour la première fois en sélectionnant **Web Insight**, **HDX™ Insight** et **Gateway Insight**. Si vous modifiez à nouveau les paramètres d'analyse ultérieurement et désélectionnez **Gateway Insight**, les modifications n'affectent pas les serveurs virtuels déjà activés avec l'analyse. Vous devez supprimer manuellement Gateway Insight sur les serveurs virtuels.
- Considérez que vous avez 10 serveurs virtuels et que deux d'entre eux sont déjà activés avec l'analyse à l'aide de l'option **Configurer l'analyse**. Dans ce scénario, lorsque vous configurez la politique globale, l'analyse est appliquée uniquement sur les huit serveurs virtuels restants.
- Considérez que vous avez 10 serveurs virtuels et que vous avez désactivé manuellement l'analyse pour deux serveurs virtuels. Dans ce scénario, lorsque vous configurez la politique globale, l'analyse est appliquée uniquement sur les huit serveurs virtuels restants et elle ignore les serveurs virtuels qui sont manuellement désactivés avec l'analyse.

Migrer l'analyse

À partir de la version **14.1-43.x**, lorsque vous activez l'analyse sur les serveurs virtuels, l'analyse est appliquée via une configuration basée sur des profils. Auparavant, l'analyse était configurée via une politique AppFlow. La configuration basée sur des profils présente les avantages suivants :

- Performances et flexibilité améliorées
- Configuration et gestion plus faciles

REMARQUE :

Les améliorations liées aux configurations d'analyse ne sont prises en charge que par la configuration basée sur des profils. Nous vous recommandons de migrer tous vos serveurs virtuels existants activés pour l'analyse vers une configuration basée sur des profils.

1. Accédez à **Paramètres > Configuration de l'analyse**, puis sélectionnez **Migrer l'analyse**.

   

2. Dans la page **Migrer l'analyse**, vous pouvez afficher les instances qui ont un ou plusieurs serveurs virtuels configurés via la politique AppFlow®.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Une fenêtre de confirmation apparaît. Cliquez sur **Oui** pour terminer la migration.

Attribuer un profil réseau à l'instance NetScaler gérée

Lorsque vous activez l'analyse ou le collecteur de métriques pour les serveurs virtuels dans NetScaler Console, les données AppFlow ou métriques du NetScaler sont exportées vers NetScaler Console via l'adresse IP de sous-réseau NetScaler (SNIP). Dans certains scénarios, le SNIP peut être bloqué en raison du pare-feu dans le réseau. Dans de tels scénarios, vous devrez peut-être utiliser une adresse IP différente de celle du SNIP. Pour plus d'informations sur le profil réseau, consultez (/fr-fr/citrix-adc/current-release/load-balancing/load-balancing-manage-clienttraffic/use-specified-srcip.html) .

Vous pouvez attribuer un profil réseau à une instance NetScaler via NetScaler Console pour exporter les données AppFlow de NetScaler vers NetScaler Console.

Conditions préalables

Assurez-vous que :

- La version de l'instance NetScaler est **13.0-48.4 ou ultérieure**.
- Le profil réseau est configuré dans les instances NetScaler.

Pour attribuer un profil réseau dans NetScaler Console :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Sélectionnez l'instance, et dans la liste **Sélectionner une action** :
   - Cliquez sur **Configurer les profils réseau** pour attribuer un profil réseau pour AppFlow.
   - Cliquez sur **Configurer les profils réseau pour le collecteur de métriques** pour attribuer un profil réseau pour le collecteur de métriques.
3. Sélectionnez un profil réseau dans la liste et cliquez sur **Appliquer**.

REMARQUE :

- Pour AppFlow, assurez-vous de désactiver l'analyse pour tous les serveurs virtuels avant d'attribuer des profils réseau à l'instance.
- Pour le collecteur de métriques, assurez-vous de désactiver les métriques pour tous les serveurs virtuels avant d'attribuer des profils réseau à l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer le serveur NTP

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans NetScaler Console pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge de NetScaler Console a les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

Pour configurer un serveur NTP sur NetScaler Console :

1. Depuis l'interface graphique de NetScaler Console, accédez à **Paramètres > Administration**. Dans la page **Administration du système**, sous **Configurations réseau**, cliquez sur **Serveurs NTP**. Cliquez ensuite sur **Ajouter**.
2. Sur la page **Créer un serveur NTP**, saisissez les détails suivants :

    - **Nom du serveur/Adresse IP** – Saisissez le nom de domaine ou l'adresse IP du serveur NTP. Le nom ou l'adresse IP ne peut pas être modifié après l'ajout du serveur NTP.
    - **Intervalle d'interrogation minimal** – Spécifiez la valeur minimale de l'intervalle entre les messages NTP transmis, en secondes, sous forme de puissance de 2. Par exemple, si vous souhaitez que l'intervalle d'interrogation minimal soit de 64 secondes, ce qui peut être exprimé comme 2\^6, saisissez 6
    - **Intervalle d'interrogation maximal** – Spécifiez la valeur maximale de l'intervalle entre les messages NTP transmis, en secondes, sous forme de puissance de 2. Par exemple, si vous souhaitez que l'intervalle d'interrogation maximal soit de 256 secondes, ce qui peut être exprimé comme 2\^8, saisissez 8.
    - **Identifiant de clé** - Saisissez l'identifiant de clé qui peut être utilisé pour l'authentification par clé symétrique avec le serveur NTP. N'ajoutez pas d'identifiant de clé si vous choisissez de sélectionner Autokey. Pour trouver l'identifiant de clé, consultez la documentation de votre serveur NTP.
    - **Autokey** - Sélectionnez **Autokey** si vous souhaitez utiliser l'authentification par clé publique avec le serveur NTP. Ne sélectionnez pas si vous souhaitez ajouter un identifiant de clé.
    - **Préféré** – Sélectionnez cette option si vous souhaitez spécifier ce serveur NTP comme serveur préféré pour la synchronisation de l'horloge. Cela s'applique uniquement si plusieurs serveurs sont configurés.

3. Cliquez sur **Créer**.

Pour activer la synchronisation NTP sur NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à la page d'accueil **Serveurs NTP**.
2. Cliquez sur **Synchronisation NTP** et cochez la case **Activer la synchronisation NTP**.
3. Cliquez sur **OK**.

   Une fenêtre de confirmation apparaît pour redémarrer NetScaler Console. Cliquez sur **Oui** pour continuer.

Configurer les paramètres système

Avant de commencer à utiliser NetScaler Console pour gérer et surveiller vos instances et applications, il est recommandé de configurer quelques paramètres système afin d'assurer des performances optimales de votre serveur NetScaler Console.

Configurer les alarmes système

Configurez les alarmes système pour vous assurer d'être informé de tout problème système critique ou majeur. Par exemple, vous pourriez vouloir être averti si l'utilisation du CPU est élevée ou s'il y a plusieurs échecs de connexion au serveur. Pour certaines catégories d'alarmes, telles que cpuUsageHigh ou memoryUsageHigh, vous pouvez définir des seuils et la gravité (par exemple, Critique ou Majeur) pour chacune. Pour certaines catégories, telles que inventoryFailed ou loginFailure, vous ne pouvez définir que la gravité. Lorsque le seuil est dépassé pour une catégorie d'alarme (par exemple, memoryUsageHigh) ou lorsqu'un événement correspondant à la catégorie d'alarme se produit (par exemple, loginFailure), un message est enregistré dans le système et vous pouvez le consulter en tant que message syslog.

Pour configurer les alarmes système :

1. Accédez à **Paramètres > SNMP**, puis cliquez sur l'onglet **Alarmes** dans le coin supérieur droit.
2. Sélectionnez l'alarme que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Sur la page **Configurer l'alarme**, sélectionnez la gravité de l'alarme et définissez le seuil.
4. Pour afficher les alarmes qui ont dépassé le seuil ou pour lesquelles un événement s'est produit, accédez à **Paramètres > Audit** et cliquez sur **Messages Syslog**.

Configurer les notifications système

Vous pouvez envoyer des notifications à des groupes d'utilisateurs sélectionnés pour diverses fonctions liées au système. Vous pouvez configurer un serveur de notification dans NetScaler Console, et vous pouvez configurer des serveurs de messagerie électronique et de passerelle de service de messages courts (SMS) pour envoyer des notifications par e-mail et par SMS aux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

utilisateurs. La configuration des notifications garantit que vous êtes informé de toute activité au niveau du système, telle que la connexion d'un utilisateur ou le redémarrage du système.

Pour configurer les notifications système :

1. Accédez à **Paramètres > Administration**. Dans la page **Administration système**, sous **Notifications d'événements**, cliquez sur **Configurer la notification d'événements et le résumé > Notification d'événements**.
2. Sur la page **Configurer les paramètres de notification système**, sélectionnez la ou les catégories d'événements générés par NetScaler Console.
3. Ensuite, configurez le serveur de messagerie ou le serveur SMS pour recevoir des notifications par e-mail ou par SMS, ou les deux.

Configurer les paramètres de sauvegarde du système

NetScaler Console sauvegarde automatiquement le système tous les jours à 00h30. Par défaut, il enregistre trois fichiers de sauvegarde. Vous pouvez souhaiter conserver un plus grand nombre de sauvegardes du système. Vous pouvez également chiffrer le fichier de sauvegarde. Vous pouvez également choisir d'enregistrer la sauvegarde sur un serveur externe.

Pour configurer les paramètres de sauvegarde du système :

1. Accédez à **Paramètres > Administration**.
2. Sous **Sauvegarde**, cliquez sur **Configurer la sauvegarde du système et des instances**.
3. Cliquez sur **Système** et, sur la page **Configurer les paramètres de sauvegarde du système**, spécifiez les valeurs requises.

Configurer les paramètres de sauvegarde des instances

Si vous sauvegardez l'état actuel d'une instance NetScaler, vous pouvez utiliser les fichiers de sauvegarde pour restaurer la stabilité si l'instance devient instable. Cela est particulièrement important avant d'effectuer une mise à niveau. Par défaut, une sauvegarde est effectuée toutes les 12 heures et trois fichiers de sauvegarde sont conservés dans le système.

Pour configurer les paramètres de sauvegarde des instances :

1. Accédez à **Paramètres > Administration**.
2. Sous **Sauvegarde**, cliquez sur **Configurer la sauvegarde du système et des instances**.
3. Cliquez sur **Instance**, sous **Configurer les paramètres de sauvegarde des instances**, et spécifiez les valeurs requises.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activer l'authentification de base

L'authentification de base doit être temporairement activée pour :

- Terminer l'enregistrement initial des agents et des nœuds de reprise après sinistre.
- Lancez le processus de validation du système d'activation des licences (LAS) depuis l'interface graphique de NetScaler.

REMARQUE :

L'authentification de base n'est requise que pour l'enregistrement initial.

Configurer l'authentification de base

1. Accédez à **Paramètres > Administration > Configurations système > Système, fuseau horaire, URL autorisées et paramètres de l'agent**.
2. Cliquez sur **Paramètres de base**.
3. Sélectionnez **Activer l'authentification de base**.
4. Cliquez sur **OK**.

Activer ou désactiver les fonctionnalités de NetScaler Console

En tant qu'administrateur, vous pouvez activer ou désactiver les fonctionnalités suivantes sur la page **Paramètres > Administration > Fonctionnalités configurables** :

- **Basculement de l'agent** - Le basculement de l'agent peut se produire sur un site comportant au moins deux agents actifs. Lorsqu'un agent devient inactif (état DOWN) sur le site, le service NetScaler Console redistribue les instances NetScaler de l'agent inactif avec d'autres agents actifs. Pour plus d'informations, consultez Configurer les agents sur site pour un déploiement multisite.
- **Fonction réseau d'interrogation d'entités** - Une entité est une stratégie, un serveur virtuel, un service ou une action attaché à une instance NetScaler. Par défaut, NetScaler Console interroge automatiquement les entités de fonction réseau configurées toutes les 60 minutes. Pour plus d'informations, consultez Présentation de l'interrogation.
- **Sauvegarde d'instance** - Sauvegardez l'état actuel d'une instance NetScaler et utilisez ultérieurement les fichiers de sauvegarde pour restaurer l'instance NetScaler au même état. Pour plus d'informations, consultez Sauvegarder et restaurer les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Audit de configuration d'instance** - Surveillez les modifications de configuration sur les instances NetScaler gérées, dépannez les erreurs de configuration et récupérez les configurations non enregistrées.
- **Événements d'instance** - Les événements représentent des occurrences d'événements ou d'erreurs sur une instance NetScaler gérée. Les événements reçus dans NetScaler Console sont affichés sur la page **Résumé des événements** (**Infrastructure > Événements**), et tous les événements actifs sont affichés sur la page Messages d'événements (**Infrastructure > Événements > Messages d'événements**). Pour plus d'informations, consultez Événements.
- **Rapports réseau d'instance** - Vous pouvez générer des rapports pour les instances au niveau global. Également pour des entités telles que les serveurs virtuels et les interfaces réseau. Pour plus d'informations, consultez Rapports réseau.
- **Certificats SSL d'instance** - NetScaler Console offre une vue centralisée des certificats SSL installés sur toutes les instances NetScaler gérées. Pour plus d'informations, consultez Tableau de bord SSL.
- **Syslog d'instance** - Vous pouvez surveiller les événements syslog générés sur vos instances NetScaler si vous avez configuré votre appareil pour rediriger tous les messages syslog vers NetScaler Console.

Pour activer une fonctionnalité, procédez comme suit :

1. Sélectionnez la fonctionnalité que vous souhaitez activer dans la liste.
2. Cliquez sur **Activer**.

IMPORTANT

Si une fonctionnalité est désactivée, l'utilisateur ne peut pas effectuer les opérations associées à cette fonctionnalité.

Intégrer NetScaler Console à l'instance ServiceNow

Lorsque vous souhaitez activer les notifications ServiceNow pour les événements NetScaler et NetScaler Console, intégrez NetScaler Console à l'instance ServiceNow. Cette intégration utilise le connecteur Citrix ITSM pour communiquer entre NetScaler Console et l'instance ServiceNow.

L'intégration de ServiceNow à NetScaler Console utilise le service ITSM Adapter pour l'authentification basée sur les jetons. Pour ce faire, elle crée une instance de point de terminaison dans ServiceNow. Pour plus d'informations, consultez Fonctionnement de l'adaptateur ITSM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour connecter votre déploiement NetScaler Console sur site à un adaptateur ITSM, assurez-vous d'avoir configuré Cloud Connect. Pour plus d'informations, consultez Cloud Connect.

Pour l'intégration de ServiceNow avec NetScaler Console version 14.1-4.x ou antérieure, assurez-vous de configurer l'identité du client. Pour plus d'informations, consultez Configurer l'identité du client.

Conditions préalables

Avant d'intégrer NetScaler Console à ServiceNow, assurez-vous des points suivants :

1. Inscrivez-vous à Citrix Cloud. Assurez-vous d'avoir accès à la gestion des administrateurs Citrix Cloud. Pour plus d'informations, consultez Gérer les administrateurs Citrix Cloud.

Comment intégrer NetScaler Console à ServiceNow ?

Effectuez les étapes suivantes pour intégrer NetScaler Console à ServiceNow à l'aide du connecteur ITSM :

1. Abonnez-vous au service ITSM Adapter dans Citrix Cloud™.
2. Créer un accès de point de terminaison dans l'instance ServiceNow.
3. Ajouter une instance ServiceNow.
4. Tester la génération automatique de tickets ServiceNow dans NetScaler Console.

Étape 1 - S'abonner au service ITSM Adapter dans Citrix Cloud

1. Sur la vignette **ITSM Adapter**, cliquez sur **Demander un essai**.
2. Accédez à **Identity Access and Management** > **API Access** et notez les informations **Client ID** et **Client Secret**.

Étape 2 - Créer un accès de point de terminaison dans l'instance ServiceNow

1. Connectez-vous à votre instance ServiceNow avec des informations d'identification d'administrateur.
2. Accédez au magasin ServiceNow. Téléchargez et installez le **connecteur Citrix ITSM**.
3. Dans le volet **Citrix ITSM Connector**, sélectionnez **Accueil** puis cliquez sur **Authentifier**. Saisissez l'ID client et le secret que vous avez notés depuis Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Testez la connexion.
5. Enregistrez la configuration. Un accusé de réception de ServiceNow apparaît, indiquant que la connexion est active.
6. Créez un point de terminaison pour accéder à une instance ServiceNow. Voir Créer un point de terminaison pour que les clients accèdent à l'instance.
7. Obtenez les jetons d'accès et d'actualisation à l'aide de l'ID client et du secret client. Voir Jetons OAuth.

Étape 3 - Ajouter une instance ServiceNow

1. Dans l'onglet **Gérer**, sélectionnez Ajouter une instance ServiceNow.
2. Spécifiez le **Nom de l'instance**, l'**ID client**, le **Secret client**, le **Jeton d'actualisation** et le **Jeton d'accès**.
3. Cliquez sur **Tester**.

   L'instance ServiceNow est maintenant connectée au service d'adaptateur ITSM.
4. Après avoir testé la connexion avec succès, cliquez sur **Enregistrer** pour ajouter une instance ServiceNow.

Étape 4 - Tester la génération automatique de tickets ServiceNow dans NetScaler Console

1. Connectez-vous à NetScaler Console.
2. Accédez à **Compte > Notifications** et sélectionnez **ServiceNow**.
3. Sélectionnez le profil ServiceNow dans la liste.
4. Cliquez sur **Tester** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

   Si vous souhaitez afficher les tickets ServiceNow dans l'interface graphique de NetScaler Console, sélectionnez **Tickets ServiceNow**.

Définir les notifications ServiceNow dans NetScaler Console

Une fois l'instance ServiceNow enregistrée sur l'adaptateur ITSM, vous pouvez configurer les notifications ServiceNow pour les événements suivants dans l'interface graphique de NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

Cette fonctionnalité est prise en charge sur ServiceNow Cloud.

- **Événements NetScaler** : NetScaler Console peut générer des incidents ServiceNow pour l'ensemble sélectionné d'événements NetScaler à partir des instances NetScaler gérées sélectionnées.

  Pour envoyer des notifications ServiceNow pour les événements NetScaler à partir des instances gérées, vous devez configurer une règle d'événement et attribuer l'action de la règle comme **Envoyer des notifications ServiceNow**.

  Créez une règle d'événement sur NetScaler Console en accédant à **Infrastructure > Événements > Règles**. Pour plus d'informations, consultez Envoyer des notifications ServiceNow.

- **Analyse des applications** : NetScaler Console peut générer des incidents ServiceNow pour les applications qui dépassent le seuil spécifié.

  

  Dans cet exemple, un incident ServiceNow est généré lorsque le score d'application des applications tombe en dessous de 90.

- **Événements de certificat SSL et de licence NetScaler Console** : NetScaler Console peut générer des incidents ServiceNow pour l'expiration du certificat SSL et l'expiration de la licence NetScaler Console.

  Pour envoyer des notifications ServiceNow pour l'expiration d'un certificat SSL, consultez L'expiration du certificat SSL.

  Pour envoyer des notifications ServiceNow pour l'expiration d'une licence NetScaler Console, consultez L'expiration de la licence NetScaler Console.

Exporter ou planifier l'exportation de rapports

Dans NetScaler Console, vous pouvez exporter un rapport complet pour la fonctionnalité NetScaler Console sélectionnée. Ce rapport vous donne un aperçu du mappage entre les instances, les partitions et les détails correspondants.

NetScaler Console affiche les rapports d'exportation planifiés spécifiques aux fonctionnalités sous les fonctionnalités individuelles de NetScaler Console, que vous pouvez afficher, modifier ou supprimer. Par exemple, pour afficher les rapports d'exportation des instances NetScaler, accédez

© 1997–2026 Citrix Systems, Inc. All rights reserved.

à **Réseau > Instances > NetScaler** et cliquez sur l'icône d'exportation. Vous pouvez exporter ces rapports aux formats de fichier PDF, JPEG, PNG et CSV.

Dans **Exporter les rapports**, vous pouvez effectuer les actions suivantes :

- Exporter un rapport vers un ordinateur local
- Planifier l'exportation de rapports
- Afficher, modifier ou supprimer les rapports d'exportation planifiés

Exporter un rapport

Pour exporter un rapport de NetScaler Console vers l'ordinateur local, procédez comme suit :

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.
2. Sélectionnez **Exporter maintenant**.
3. Sélectionnez l'une des options d'exportation suivantes :

    - **Instantané** - Cette option exporte les rapports NetScaler Console sous forme d'instantané.
    - **Tabulaire** - Cette option exporte les rapports NetScaler Console dans un format tabulaire. Vous pouvez également choisir le nombre d'enregistrements de données à exporter dans un format tabulaire.

    

4. Sélectionnez le format de fichier dans lequel vous souhaitez enregistrer le rapport sur votre ordinateur local.
5. Cliquez sur **Exporter**.

Planifier l'exportation du rapport

Pour planifier l'exportation du rapport à intervalles réguliers, spécifiez l'intervalle de récurrence. NetScaler Console envoie le rapport exporté au profil de messagerie ou Slack configuré.

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.
2. Sélectionnez **Planifier l'exportation** et spécifiez les éléments suivants :

    - **Objet** - Par défaut, ce champ est automatiquement renseigné avec le nom de la fonctionnalité sélectionnée. Cependant, vous pouvez le modifier avec un titre significatif.
    - **Option d'exportation** - Exportez les rapports NetScaler Console au format instantané ou tabulaire. Vous pouvez également choisir le nombre d'enregistrements de données à exporter au format tabulaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Format** - Sélectionnez le format de fichier dans lequel vous souhaitez recevoir le rapport sur le profil de messagerie ou Slack configuré.
- **Récurrence** - Sélectionnez **Quotidien**, **Hebdomadaire** ou **Mensuel** dans la liste.
- **Description** - Spécifiez une description significative pour un rapport.
- **Heure d'exportation** - Spécifiez l'heure à laquelle vous souhaitez exporter le rapport.
- **E-mail** - Cochez la case et sélectionnez le profil dans la liste déroulante. Si vous souhaitez ajouter un profil, cliquez sur **Ajouter**.
- **Slack** - Cochez la case et sélectionnez le profil dans la liste déroulante. Si vous souhaitez ajouter un profil, cliquez sur **Ajouter**.

3. Cliquez sur **Planifier**.

Planifier l'exportation des rapports NetScaler Console(/en-us/netscaler-application-delivery-management-software/media/schedule-export-adm-reports.png)

Afficher et modifier les rapports d'exportation planifiés

Pour afficher les rapports d'exportation, procédez comme suit :

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.

   La page **Rapport d'exportation** affiche tous les rapports d'exportation spécifiques aux fonctionnalités.

2. Sélectionnez le rapport que vous souhaitez modifier et cliquez sur **Modifier**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mise à niveau

Chaque version de NetScaler Console offre des fonctionnalités nouvelles et mises à jour avec une fonctionnalité accrue. Nous vous recommandons de mettre à niveau NetScaler Console vers la dernière version pour bénéficier des nouvelles fonctionnalités et des corrections de bogues. Une liste complète des améliorations, des problèmes connus et des corrections de bogues est incluse dans les notes de publication accompagnant chaque annonce de version. Il est également important de comprendre le cadre de licence et les types de licences qui peuvent être utilisés avant de commencer la mise à niveau. Pour plus d'informations sur les licences NetScaler Console, consultez Licences.

Avant la mise à niveau

Téléchargez le package de mise à niveau depuis la page de téléchargements de NetScaler Console et suivez les instructions de cet article pour mettre à niveau votre système vers la dernière version 14.1. Une fois le processus de mise à niveau commencé, NetScaler Console redémarre et les connexions existantes sont terminées puis rétablies une fois la mise à niveau terminée. La configuration existante est conservée, mais NetScaler Console ne traite aucune donnée tant que la mise à niveau n'est pas terminée.

IMPORTANT

La version et la build de NetScaler Console doivent être **égales ou supérieures** à la version et à la build de votre NetScaler. Par exemple, si vous avez installé NetScaler Console 12.1 Build 50.39, assurez-vous d'avoir installé NetScaler 12.1 Build 50.28/50.31 ou une version antérieure.

Points à noter avant la mise à niveau vers la version 14.1 :

- Si vous effectuez une mise à niveau depuis la version 11.1 ou la version 12.0 56.x et les builds précédentes, suivez les étapes suivantes :

  a. Mettez à niveau de la version existante vers la build 12.0 57.24.

  b. Mettez à niveau vers la dernière build de la version 12.1.

  c. Mettez à niveau vers la version 13.1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Mettez à niveau vers la version 14.1.

- Si vous effectuez une mise à niveau depuis la build 12.0 57.24 ou supérieure, mettez d'abord à niveau vers la version 12.1, puis vers la 13.1, et enfin vers la 14.1.
- Si vous effectuez une mise à niveau depuis la version 12.1, vous devez d'abord mettre à niveau vers la version 13.0 64.xx, puis directement vers la 14.1.
- Si vous effectuez une mise à niveau depuis des versions inférieures à la 13.0 64.xx, pour une meilleure expérience utilisateur, mettez d'abord à niveau vers la 13.0 64.xx, puis vers la 14.1.
- Pour passer de la version 13.1 à la version 14.1, effectuez d'abord la mise à niveau vers la dernière version de la version 13.1, puis vers la version 14.1.
- Après la mise à niveau réussie vers la version 14.1 et votre connexion à l'interface graphique, il vous est recommandé de modifier le mot de passe si vous utilisez le mot de passe par défaut.

Points importants à noter avant de passer à la version 14.1-xx.xx et ultérieure

Lorsque vous mettez à niveau NetScaler Console vers la version 14.1-xx.xx, votre base de données NetScaler Console est également migrée. Cette migration de données se produit car NetScaler Console utilise désormais PostgreSQL version 10.11.

REMARQUE :

La rétrogradation de NetScaler Console n'est pas prise en charge. N'essayez pas de rétrograder.

Précautions recommandées :

- Prenez un instantané du serveur NetScaler Console pour chaque mise à niveau, si vous effectuez une mise à niveau vers la version 14.1-xx.xx et ultérieure.
- Sauvegardez le serveur NetScaler Console avant de procéder à la mise à niveau.
- Après la mise à niveau, vous devrez peut-être rétablir les connexions entre le serveur NetScaler Console et les instances gérées. Une invite de confirmation vous avertit que les connexions peuvent échouer si vous continuez.
- Pour les serveurs NetScaler Console configurés en haute disponibilité, lors de la mise à niveau, n'apportez aucune modification de configuration sur l'un ou l'autre des nœuds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AVERTISSEMENT :

Ne rafraîchissez pas le navigateur tant que le processus de mise à niveau n'est pas terminé avec succès. Vérifiez l'interface graphique pour connaître le temps approximatif nécessaire à la fin de la mise à niveau.

Mettre à niveau un seul serveur NetScaler Console vers la version 14.1-xx.xx

1. Connectez-vous à NetScaler Console avec les informations d'identification de l'administrateur.
2. Naviguez vers **Paramètres** \> **Administration**. Sous **Maintenance du système**, cliquez sur **Mettre à niveau NetScaler Console**.

   
3. Sur la page **Mettre à niveau NetScaler Console**, cochez la case **Nettoyer l'image logicielle après une mise à niveau réussie** pour supprimer les fichiers image après la mise à niveau. La sélection de cette option supprime automatiquement les fichiers image de NetScaler Console après la mise à niveau.

   REMARQUE :

   Cette option est sélectionnée par défaut. Si vous ne cochez pas cette case avant de démarrer le processus de mise à niveau, vous devez supprimer manuellement les images.
4. Vous pouvez ensuite télécharger un nouveau fichier image en sélectionnant **Local** (votre machine locale) ou **Appliance**. Le fichier de build doit être présent sur l'appliance virtuelle NetScaler Console.

   
5. Cliquez sur **OK**. La boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui**.

   Le processus de mise à niveau démarre.

Une fois votre configuration migrée, vous pouvez vous connecter à l'interface graphique de NetScaler Console. Lors de la connexion, les données historiques commencent à migrer en arrière-plan pendant que vous pouvez continuer à travailler sur NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pendant la migration des données historiques, certaines des anciennes données peuvent ne pas être disponibles. Le temps nécessaire pour migrer votre base de données dépend de la taille des données et du nombre de tables.

Vous pouvez surveiller la migration de la base de données à l'aide de l'interface graphique de NetScaler Console. Cliquez sur **Afficher la progression de la mise à niveau** et le **Statut de la migration de la base de données** apparaît.

Mettre à niveau une paire haute disponibilité vers la version 14.1

Pour les serveurs NetScaler Console en mode haute disponibilité, vous pouvez effectuer la mise à niveau en accédant au nœud actif ou à l'adresse IP flottante. Les deux serveurs NetScaler Console sont automatiquement mis à niveau vers la dernière version une fois que vous avez lancé le processus de mise à niveau sur l'un ou l'autre des serveurs.

Mettre à niveau le déploiement de reprise après sinistre de NetScaler Console

REMARQUE :

- Assurez-vous que le mot de passe est le même pour la paire HA et le nœud de reprise après sinistre.
- Mettez à niveau le nœud de reprise après sinistre uniquement après avoir mis à niveau le nœud autonome ou le nœud HA. Si vous mettez à niveau le nœud de reprise après sinistre avant de mettre à niveau le nœud principal ou le nœud HA, vous pourriez observer des problèmes de synchronisation de base de données.

La mise à niveau du déploiement de reprise après sinistre de NetScaler Console est un processus en deux étapes :

- Mettez à niveau les nœuds NetScaler Console configurés en mode haute disponibilité sur le site principal. Ensuite, vous devez mettre à niveau le nœud de reprise après sinistre.
- Assurez-vous d'avoir mis à niveau les serveurs NetScaler Console déployés en haute disponibilité avant de mettre à niveau le nœud de reprise après sinistre.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mettre à niveau le nœud de reprise après sinistre de NetScaler Console

1. Téléchargez le fichier image de mise à niveau de NetScaler Console depuis le site NetScaler.
2. Téléchargez ce fichier sur le nœud de reprise après sinistre à l'aide des informations d'identification `nsrecover`.
3. Connectez-vous au nœud de reprise après sinistre à l'aide des informations d'identification `nsrecover`.
4. Accédez au dossier où vous avez placé le fichier image et décompressez le fichier.
5. Exécutez le script suivant :

   ./installmas

   

Mettre à niveau les agents sur site pour un déploiement multisite

La mise à niveau du déploiement de l'agent NetScaler est un processus en trois étapes. Assurez-vous d'avoir effectué les tâches suivantes avant de mettre à niveau les agents sur site :

1. Mettez à niveau les serveurs NetScaler Console qui sont déployés en haute disponibilité.
2. Mettez à niveau le nœud de reprise après sinistre de NetScaler Console.

   Pour plus d'informations, consultez Mettre à niveau le déploiement de reprise après sinistre de NetScaler Console.

Mettre à niveau l'agent sur site

1. Téléchargez le fichier image de mise à niveau de l'agent NetScaler depuis le site NetScaler.
2. Téléchargez ce fichier sur le nœud de l'agent à l'aide des informations d'identification `nsrecover`.
3. Assurez-vous de télécharger la bonne image de mise à niveau de l'agent.
4. Connectez-vous à l'agent sur site à l'aide des informations d'identification `nsrecover`.
5. Accédez au dossier où vous avez placé le fichier image et décompressez le fichier.

   

6. Exécutez le script suivant :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./installmasagent
```

- [ ]

Ajouter un disque supplémentaire au serveur NetScaler Console

Si votre besoin en stockage NetScaler Console dépasse l'espace disque par défaut (120 Go), vous pouvez attacher un disque supplémentaire. Vous pouvez attacher plus de disques dans les déploiements à serveur unique et à haute disponibilité.

Lorsque vous mettez à niveau NetScaler Console depuis la version 12.1–13.10, les partitions que vous aviez créées sur le disque supplémentaire dans la version précédente restent les mêmes. Les partitions ne sont ni supprimées ni redimensionnées.

La procédure pour attacher plus de disques reste la même dans la version mise à niveau. Vous pouvez maintenant utiliser le nouvel outil de partitionnement de disque dans NetScaler Console pour créer des partitions sur le disque nouvellement ajouté. Vous pouvez également utiliser l'outil pour redimensionner les partitions sur le disque supplémentaire existant. Pour plus d'informations sur la façon d'attacher plus de disques et d'utiliser le nouvel outil de partitionnement de disque, consultez Comment attacher un disque supplémentaire à NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentification

Les utilisateurs peuvent être authentifiés soit en interne par NetScaler Console, soit en externe par un serveur d'authentification, soit les deux. Si l'authentification locale est utilisée, l'utilisateur doit figurer dans la base de données de sécurité de NetScaler Console. Si l'utilisateur est authentifié en externe, le « nom externe » de l'utilisateur doit correspondre à l'identité de l'utilisateur externe enregistrée auprès du serveur d'authentification, en fonction du protocole d'authentification sélectionné.

NetScaler Console prend en charge l'authentification externe par les serveurs RADIUS, LDAP et TACACS. Ce support unifié fournit une interface commune pour authentifier et autoriser tous les utilisateurs des serveurs d'authentification, d'autorisation et de comptabilité locaux et externes qui accèdent au système. NetScaler Console peut authentifier les utilisateurs quels que soient les protocoles réels qu'ils utilisent pour communiquer avec le système. Lorsqu'un utilisateur tente d'accéder à une implémentation de NetScaler Console configurée pour l'authentification externe, le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au serveur RADIUS, LDAP ou TACACS pour authentification. Si l'authentification est réussie, l'utilisateur est autorisé à accéder à NetScaler Console.

Serveurs d'authentification externes

NetScaler Console envoie toutes les requêtes de service d'authentification, d'autorisation et d'audit au serveur RADIUS, LDAP ou TACACS distant. Le serveur d'authentification, d'autorisation et d'audit distant reçoit la requête, la valide et envoie une réponse à NetScaler Console. Lorsqu'il est configuré pour utiliser un serveur RADIUS, TACACS ou LDAP distant pour l'authentification, NetScaler Console devient un client RADIUS, TACACS ou LDAP. Dans toutes ces configurations, les enregistrements d'authentification sont stockés dans la base de données du serveur hôte distant. Le nom de compte, les autorisations attribuées et les enregistrements de comptabilité horaire sont également stockés sur le serveur d'authentification, d'autorisation et d'audit pour chaque utilisateur.

Vous pouvez également utiliser la base de données interne de NetScaler Console pour authentifier les utilisateurs localement. Vous créez des entrées dans la base de données pour les utilisateurs, leurs mots de passe et leurs rôles par défaut. Vous pouvez également sélectionner l'ordre d'authentification pour des types d'authentification spécifiques. La liste des serveurs d'un groupe de serveurs est une liste ordonnée. Le premier serveur de la liste est toujours utilisé, sauf s'il est

© 1997–2026 Citrix Systems, Inc. All rights reserved.

indisponible, auquel cas le serveur suivant de la liste est utilisé. Vous pouvez configurer les serveurs pour inclure la base de données interne comme sauvegarde d'authentification de secours à la liste configurée de serveurs d'authentification, d'autorisation et d'audit.

Vous pouvez configurer et ajouter les serveurs suivants dans NetScaler Console :

- Serveur d'authentification LDAP
- Serveur d'authentification RADIUS
- Serveur d'authentification TACACS
- Activer les serveurs d'authentification externes et les options de secours
- Prise en charge de l'authentification à deux facteurs (2FA) avec LDAP, RADIUS et TACACS

Authentifier les utilisateurs dans NetScaler Console

Vous pouvez authentifier vos utilisateurs dans NetScaler Console de deux manières :

- Utilisateurs locaux configurés dans NetScaler Console

  Authentification des utilisateurs locaux(/en-us/netscaler-application-delivery-management-software/media/auth-local-users-console.png)

  Après la configuration, voici le flux de travail pour l'authentification des utilisateurs sur le serveur local.

  Authentification des utilisateurs locaux(/en-us/netscaler-application-delivery-management-software/media/auth-local-users1-console.png)

  1 – L'utilisateur se connecte à NetScaler Console

  2 – NetScaler Console invite les utilisateurs à saisir leurs informations d'identification pour l'authentification et vérifie si les informations d'identification correspondent dans la base de données NetScaler Console.
- Utilisation de serveurs d'authentification externes

  Authentification des utilisateurs externes(/en-us/netscaler-application-delivery-management-software/media/auth-external-console.png)

  Après la configuration, voici le flux de travail pour l'authentification des utilisateurs sur le serveur externe d'authentification, d'autorisation et d'audit :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentification des utilisateurs externes(/en-us/netscaler-application-delivery-management-software/media/auth-external1-console.png)

1 – L'utilisateur se connecte à NetScaler Console

2 – NetScaler Console invite l'utilisateur à saisir ses informations d'identification

3 – NetScaler Console valide les informations d'identification de l'utilisateur auprès du serveur externe d'authentification, d'autorisation et d'audit. Si la validation est réussie, l'utilisateur peut continuer à se connecter

Ajouter un serveur d'authentification LDAP

Lorsque vous intégrez le protocole LDAP avec les serveurs d'authentification RADIUS et TACAS, vous pouvez utiliser NetScaler Console pour rechercher et authentifier les informations d'identification des utilisateurs à partir de répertoires distribués.

1. Accédez à **Paramètres > Authentification**.
2. Sélectionnez l'onglet **LDAP**, puis cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur LDAP**, spécifiez les paramètres suivants :
    a. **Nom** – Spécifiez le nom du serveur LDAP
    b. **Nom du serveur/adresse IP** – Spécifiez l'adresse IP ou le nom du serveur LDAP
    c. **Type de sécurité** – Type de communication requis entre le système et le serveur LDAP. Sélectionnez dans la liste. Si la communication en texte clair est inadéquate, vous pouvez choisir une communication chiffrée en sélectionnant Transport Layer Security (TLS) ou SSL.
    d. **Port** – Par défaut, le port 389 est utilisé pour PLAINTEXT. Vous pouvez également spécifier le port 636 pour SSL/TLS.
    e. **Type de serveur** – Sélectionnez Active Directory (AD) ou Novell Directory Service (NDS) comme type de serveur LDAP.
    f. **Délai d'expiration (secondes)** – Temps en secondes pendant lequel le système NetScaler Console attend une réponse du serveur LDAP.
    g. **Nom d'hôte LDAP** – Cochez la case Valider le certificat LDAP et spécifiez le nom d'hôte à saisir sur le certificat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Désactivez l'option **Authentification** et spécifiez la clé publique SSH. Avec l'authentification par clé, vous pouvez désormais récupérer la liste des clés publiques stockées sur l'objet utilisateur dans le serveur LDAP via SSH.

Sous Paramètres de connexion, spécifiez les paramètres suivants :

i. **DN de base** – Le nœud de base pour le serveur LDAP à partir duquel démarrer la recherche

ii. **DN de liaison administrateur** – Nom d'utilisateur pour se lier au serveur LDAP. Par exemple, admin@aaa.local.

iii. **Mot de passe du DN de liaison** – Sélectionnez cette option pour fournir un mot de passe pour l'authentification

iv. **Activer le changement de mot de passe** – Sélectionnez cette option pour activer le changement de mot de passe

Sous **Autres paramètres**, spécifiez les paramètres suivants

i. **Attribut de nom de connexion au serveur** – Attribut de nom utilisé par le système pour interroger le serveur LDAP externe ou un Active Directory. Sélectionnez **samAccountname** dans la liste.

ii. **Filtre de recherche** – Configurez les utilisateurs externes pour l'authentification à deux facteurs en fonction du filtre de recherche configuré dans le serveur LDAP. Par exemple, vpnallowed=true avec ldaploginame `samaccount` et le nom d'utilisateur fourni par l'utilisateur bob donneraient une chaîne de recherche LDAP de : `&(vpnallowed=true)(samaccount=bob)`.

   Remarque

   Par défaut, les valeurs du filtre de recherche sont entre crochets.

iii. **Attribut de groupe** – Sélectionnez memberOf dans la liste.

iv. **Nom du sous-attribut** – Le nom du sous-attribut pour l'extraction de groupe du serveur LDAP.

v. **Groupe d'authentification par défaut** – Groupe par défaut à choisir lorsque l'authentification réussit en plus des groupes extraits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Cliquez sur **Créer**.

   Le serveur LDAP est maintenant configuré.

   REMARQUE

   .

   Si les utilisateurs sont membres d'un groupe Active Directory, le groupe et les noms d'utilisateur sur NetScaler Console doivent être identiques aux noms des membres du groupe Active Directory.

5. Activez les serveurs d'authentification externes.

   Pour plus d'informations sur l'activation des serveurs d'authentification externes, consultez Activer les serveurs d'authentification externes et les options de secours.

Ajouter un serveur d'authentification RADIUS

1. Accédez à **Paramètres > Authentification**.
2. Sélectionnez l'onglet **RADIUS**, puis cliquez sur **Ajouter**.

   Sur la page **Créer un serveur RADIUS**, spécifiez les paramètres suivants :

   a. **Nom** – Spécifiez un nom de serveur RADIUS
   b. **Nom du serveur / Adresse IP** – Spécifiez l'adresse IP du serveur RADIUS
   c. **Port** – Spécifiez le numéro de port sur lequel le serveur RADIUS est hébergé. Le port par défaut est 1812
   d. **Délai d'expiration (secondes)** – Durée en secondes pendant laquelle le système NetScaler Console attend une réponse du serveur RADIUS
   e. **Clé secrète** – Spécifiez la clé secrète RADIUS pour l'authentification
   f. **Confirmer la clé secrète** – Spécifiez à nouveau la clé pour confirmation

      

      Sous **Détails**, spécifiez les paramètres suivants :

      i. **ID NAS** – Spécifiez l'ID pour envoyer l'identifiant au serveur RADIUS
      ii. **Identifiant du fournisseur de groupe** – Spécifiez l'ID du fournisseur pour l'extraction de groupe RADIUS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iii. **Préfixe de groupe** - Une chaîne qui précède les noms de groupe dans un attribut RADIUS pour l'extraction de groupe RADIUS

iv. **Type d'attribut de groupe** – Spécifiez le type d'attribut pour l'extraction de groupe RADIUS

v. **Séparateur de groupe** – Une chaîne qui délimite les noms de groupe au sein d'un attribut RADIUS pour l'extraction de groupe RADIUS

vi. **Identifiant du fournisseur d'adresse IP** – L'ID du fournisseur dans RADIUS indique l'adresse IP de l'intranet. Une valeur de 0 indique que l'attribut n'est pas encodé par le fournisseur

vii. **Identifiant du fournisseur de mot de passe** – Mot de passe de l'ID du fournisseur dans la réponse RADIUS pour extraire le mot de passe de l'utilisateur

viii. **Type d'attribut d'adresse IP** – Attribut d'adresse IP distante pour que le RADIUS réponde

ix. **Type d'attribut de mot de passe** – L'attribut de mot de passe pour que le RADIUS réponde

x. **Encodage du mot de passe** – Sélectionnez pap, chap, mschapv1 ou mschapv2 dans la liste. Cela indique comment les mots de passe doivent être encodés dans les paquets RADIUS circulant du système vers le serveur RADIUS.

xi. **Groupe d'authentification par défaut** – Groupe par défaut à choisir lorsque l'authentification réussit en plus des groupes extraits

Sélectionnez Comptabilité si vous souhaitez que l'appliance enregistre les informations d'audit avec le serveur RADIUS.

3. Cliquez sur **Créer**.

Le serveur RADIUS est maintenant configuré.

4. Activez les serveurs d'authentification externes.

Pour plus d'informations sur l'activation des serveurs d'authentification externes, consultez Activer les serveurs d'authentification externes et les options de secours.

Ajouter un serveur d'authentification TACACS

1. Accédez à **Paramètres > Authentification**.
2. Sélectionnez l'onglet **TACACS**, puis cliquez sur **Ajouter**.
3. Sur la page **Créer TACACS**, spécifiez les paramètres suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Nom** – Spécifiez un nom de serveur TACACS

b. **Adresse IP** – Spécifiez l'adresse IP TACACS

c. **Port** – Spécifiez le numéro de port sur lequel le serveur TACACS est hébergé. Le port par défaut est 49

d. **Délai d'expiration (secondes)** – Temps en secondes pendant lequel le système NetScaler Console attend une réponse du serveur LDAP

e. **Clé TACACS** – Spécifiez la clé TACACS pour l'authentification

f. **Confirmer la clé TACACS** – Spécifiez à nouveau la clé TACACS pour confirmation

g. **Nom de l'attribut de groupe** – Spécifiez le nom du groupe

Sélectionnez **Comptabilité** si vous souhaitez que l'appliance enregistre les informations d'audit avec le serveur TACACS.

4. Cliquez sur **Créer**.



5. Activez les serveurs d'authentification externes.

Pour plus d'informations sur l'activation des serveurs d'authentification externes, consultez Activer les serveurs d'authentification externes et les options de secours.

Utilisateurs dans NetScaler Console

Vous pouvez créer des comptes utilisateur localement sur NetScaler Console pour compléter les utilisateurs des serveurs d'authentification. Par exemple, vous pourriez vouloir créer des comptes utilisateur locaux pour des utilisateurs temporaires, tels que des consultants ou des visiteurs, sans créer d'entrée pour ces utilisateurs sur le serveur d'authentification.

Pour plus d'informations sur la configuration des utilisateurs, consultez Configurer les utilisateurs.

Remarque

Si les utilisateurs se trouvent sur Active Directory, assurez-vous que le nom du groupe dans NetScaler Console est le même que celui du groupe Active Directory sur le serveur externe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Groupes d'utilisateurs dans NetScaler Console

NetScaler Console vous permet d'authentifier et d'autoriser vos utilisateurs en créant des groupes et en y ajoutant les utilisateurs. Un groupe peut avoir des autorisations « admin » ou « lecture seule », et tous les utilisateurs de ce groupe recevront des autorisations égales.

Dans NetScaler Console :

- Un groupe est défini comme une collection d'utilisateurs ayant des autorisations similaires
- Un groupe peut avoir un ou plusieurs rôles
- Un utilisateur est défini comme une entité pouvant avoir accès en fonction des autorisations attribuées
- Un utilisateur peut appartenir à un ou plusieurs groupes

Vous pouvez créer des groupes locaux dans NetScaler Console et utiliser l'authentification locale pour les utilisateurs de ces groupes. Si vous utilisez des serveurs externes pour l'authentification, configurez les groupes sur NetScaler Console pour qu'ils correspondent aux groupes configurés sur les serveurs d'authentification du réseau interne. Lorsqu'un utilisateur se connecte et est authentifié, si un nom de groupe correspond à un groupe sur un serveur d'authentification, l'utilisateur hérite des paramètres du groupe sur NetScaler Console. Si vous utilisez l'authentification locale, créez des utilisateurs et ajoutez-les aux groupes configurés sur NetScaler Console. Les utilisateurs héritent alors des paramètres de ces groupes.

Pour plus d'informations sur la configuration des groupes et l'attribution des autorisations de groupe, consultez Configurer les groupes.

Extraire un groupe de serveurs d'authentification

REMARQUE

L'extraction du serveur TACACS est prise en charge à partir de **NetScaler Console 13.0**.

NetScaler Console vous permet de :

- Extraire la liste des groupes auxquels un utilisateur appartient sur le serveur d'authentification externe.
- Les attribuer aux paramètres de groupe qui correspondent aux groupes configurés sur le serveur externe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Avantages :

- Vous n'avez pas à créer d'utilisateurs dans NetScaler Console, car ils sont gérés sur le serveur externe.
- NetScaler Console effectue l'autorisation des utilisateurs en attribuant des autorisations de groupe pour accéder à des serveurs virtuels d'équilibrage de charge spécifiques et à des applications spécifiques sur le système.

Activer les serveurs d'authentification externes et les options de secours

L'option de secours permet à l'authentification locale de prendre le relais si l'authentification du serveur externe échoue. Un utilisateur configuré à la fois sur NetScaler Console et sur le serveur d'authentification externe peut se connecter à NetScaler Console, même si les serveurs d'authentification externes configurés sont hors service ou inaccessibles. Pour que l'authentification de secours fonctionne :

- Les utilisateurs non-nsroot doivent pouvoir accéder à NetScaler Console si le serveur externe est hors service ou inaccessible
- Vous devez ajouter au moins un serveur externe

NetScaler Console prend également en charge un système unifié de protocoles d'authentification, d'autorisation et de comptabilité (AAA) (LDAP, RADIUS et TACACS), ainsi que l'authentification locale. Ce support unifié fournit une interface commune pour authentifier et autoriser tous les utilisateurs et clients AAA externes accédant au système.

NetScaler Console peut authentifier les utilisateurs quels que soient les protocoles réels qu'ils utilisent pour communiquer avec le système. La mise en cascade des serveurs d'authentification externes offre un processus continu et sans échec pour l'authentification et l'autorisation des utilisateurs externes. Si l'authentification échoue sur le premier serveur d'authentification, NetScaler Console tente d'authentifier l'utilisateur en utilisant le deuxième serveur d'authentification externe, et ainsi de suite. Pour activer l'authentification en cascade, vous devez ajouter les serveurs d'authentification externes dans NetScaler Console. Vous pouvez ajouter n'importe quel type de serveurs d'authentification externes pris en charge (RADIUS, LDAP et TACACS).

Par exemple, supposons que vous souhaitiez ajouter quatre serveurs d'authentification externes et que vous ayez configuré deux serveurs RADIUS, un serveur LDAP et un serveur TACACS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console tente de s'authentifier auprès des serveurs externes, en fonction des configurations. Dans ce scénario d'exemple, NetScaler Console tente de :

- Se connecter au premier serveur RADIUS
- Se connecter au deuxième serveur RADIUS, si l'authentification a échoué avec le premier serveur RADIUS
- Se connecter au serveur LDAP, si l'authentification a échoué avec les deux serveurs RADIUS
- Se connecter au serveur TACACS, si l'authentification a échoué avec les deux serveurs RADIUS et le serveur LDAP.

Remarque

> Vous pouvez configurer jusqu'à 32 serveurs d'authentification externes dans NetScaler Console.

Configurer les serveurs externes de secours et en cascade

1. Accédez à **Paramètres > Authentification > Paramètres d'authentification**.
2. Sur la page **Paramètres d'authentification**, sous **Authentification du serveur externe**, cliquez sur **Activer l'authentification à facteur unique**.
3. Sur la page **Activer l'authentification à facteur unique**, cliquez sur **Sélectionner les serveurs**. Sélectionnez un ou plusieurs serveurs d'authentification et cliquez sur **Ajouter**.
4. Sélectionnez **Revenir à l'authentification locale si l'authentification externe échoue** si vous souhaitez que l'authentification locale prenne le relais en cas d'échec de l'authentification externe.
5. Sélectionnez **Enregistrer les informations du groupe d'utilisateurs externes dans les journaux système** si vous souhaitez capturer les informations du groupe d'utilisateurs externes dans le journal d'audit du système.
6. Cliquez sur **Soumettre** pour fermer la page.

   Les serveurs sélectionnés sont affichés sur la page **Paramètres d'authentification**.

   

Vous pouvez également spécifier l'ordre d'authentification en utilisant l'icône à côté des noms de serveur pour déplacer les serveurs vers le haut ou vers le bas de la liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prise en charge de l'authentification à deux facteurs (2FA) avec LDAP, RADIUS et TACACS

L'authentification multifacteur est aujourd'hui une bonne pratique en matière de sécurité, et la plupart des organisations exigent au moins deux facteurs d'authentification pour les appliances réseau afin de respecter les normes de conformité. L'authentification à deux facteurs est un mécanisme de sécurité par lequel un produit authentifie un utilisateur à deux niveaux. L'accès n'est accordé qu'après une validation réussie aux deux niveaux.

À partir de NetScaler Console 14.1-43.x et versions ultérieures, l'authentification à deux facteurs (2FA) est prise en charge sur NetScaler Console sur site. Vous pouvez utiliser LDAP, RADIUS et TACACS comme facteurs d'authentification pour NetScaler Console sur site.

REMARQUE :

La prise en charge de l'authentification à deux facteurs est disponible uniquement pour l'authentification de serveur externe.

Lorsqu'un utilisateur tente de se connecter à une NetScaler Console avec l'authentification à deux facteurs activée, il est invité à saisir son nom d'utilisateur et son mot de passe pour l'authentification externe initiale. Une fois l'authentification initiale réussie, l'utilisateur est invité à procéder au deuxième niveau d'authentification.

L'utilisateur n'est entièrement authentifié qu'après la validation réussie des deux mots de passe. Si l'authentification échoue, la raison de l'échec est affichée à l'utilisateur.

Si un utilisateur est authentifié localement, le profil utilisateur doit être créé dans la base de données NetScaler Console. Si l'utilisateur est authentifié en externe, le nom d'utilisateur et le mot de passe doivent correspondre à l'identité de l'utilisateur enregistrée dans le serveur d'authentification externe.



Configurer l'authentification à deux facteurs

1. Connectez-vous à NetScaler Console sur site et accédez à **Paramètres > Authentification > Paramètres d'authentification**.

   

2. Dans la section **Authentification du serveur externe**, cliquez sur **Activer l'authentification à deux facteurs** sous **Modes d'authentification**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Sur la page **Activer l'authentification à deux facteurs**, sous **Étape 1 : Serveurs principaux**, cliquez sur **Ajouter des serveurs**.

   

4. Cliquez sur **Sélectionner des serveurs** et sélectionnez les serveurs requis. Cliquez sur **Ajouter**, puis sur **Terminé**.

   

5. Sur la page **Activer l'authentification à deux facteurs**, sous **Étape 2 : Serveurs secondaires**, cliquez sur **Ajouter des serveurs**.
6. Dans **Étiquette pour le champ d'authentification à deux facteurs**, saisissez une étiquette qui sera utilisée pour l'authentification auprès des serveurs configurés pour l'authentification du second facteur.
7. Cliquez sur **Sélectionner des serveurs** et sélectionnez les serveurs requis. Cliquez sur **Ajouter**, puis sur **Terminé**.

   

8. Cliquez sur **Soumettre**.

Accès utilisateur à NetScaler® Console avec authentification à deux facteurs

1. Dans un navigateur web, saisissez l'adresse IP de la NetScaler Console. La page de connexion apparaît.

   

2. Saisissez le nom d'utilisateur et le mot de passe dans les champs **Nom d'utilisateur** et **Mot de passe**. Cette étape correspond à l'authentification du premier facteur.
3. Après une authentification réussie du premier facteur, l'utilisateur est invité à procéder à l'authentification du second facteur. Saisissez l'étiquette configurée pour l'authentification du second facteur.

   

4. Après une authentification réussie du second facteur, l'utilisateur est connecté à l'interface graphique de NetScaler Console.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Contrôle d'accès

L'authentification est un processus par lequel vous vérifiez qu'une personne est bien celle qu'elle prétend être. Pour effectuer l'authentification, un utilisateur doit déjà avoir un compte créé dans un système qui peut être interrogé par le mécanisme d'authentification, ou un compte doit être créé dans le cadre du processus de la première authentification. NetScaler fournit une méthode pour authentifier les utilisateurs locaux et les utilisateurs externes. Alors que les utilisateurs locaux sont authentifiés en interne, NetScaler Console prend en charge l'authentification externe avec les protocoles RADIUS, LDAP et TACACS. Lorsqu'un utilisateur tente d'accéder à NetScaler Console configuré pour l'authentification externe, le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au serveur RADIUS, LDAP ou TACACS pour authentification. Une fois authentifié, le protocole requis est utilisé pour identifier l'utilisateur sur NetScaler Console.

Le contrôle d'accès est le processus d'application de la sécurité requise pour une ressource particulière. C'est une technique de sécurité qui peut être utilisée pour réguler qui peut visualiser ou utiliser des ressources dans un environnement informatique. Son objectif est de limiter les actions ou opérations qu'un utilisateur légitime d'un système informatique peut effectuer. Il restreint ce qu'un utilisateur peut faire directement, et ce que les programmes exécutés au nom des utilisateurs sont autorisés à faire. De cette manière, il vise à prévenir les activités pouvant entraîner une violation de la sécurité. Le contrôle d'accès suppose que l'authentification de l'utilisateur a été vérifiée avec succès avant son application via un moniteur de référence. NetScaler Console permet un contrôle d'accès basé sur les rôles (RBAC) granulaire, par lequel les administrateurs peuvent accorder des autorisations d'accès aux utilisateurs en fonction des rôles des utilisateurs individuels au sein d'une entreprise. Le RBAC dans NetScaler Console est mis en œuvre en créant des stratégies d'accès, des rôles, des groupes et des utilisateurs.

Contrôle d'accès basé sur les rôles

NetScaler Console offre un contrôle d'accès basé sur les rôles (RBAC) granulaire, avec lequel vous pouvez accorder des autorisations d'accès en fonction des rôles des utilisateurs individuels au sein de votre entreprise. Dans ce contexte, l'accès est la capacité d'effectuer une tâche spécifique, telle que l'affichage, la création, la modification ou la suppression d'un fichier. Les rôles sont définis en fonction de l'autorité et de la responsabilité des utilisateurs au sein de l'entreprise. Par exemple, un utilisateur peut être autorisé à effectuer toutes les opérations réseau, tandis qu'un

© 1997–2026 Citrix Systems, Inc. All rights reserved.

autre utilisateur peut observer le flux de trafic dans les applications et aider à créer des modèles de configuration.

Les rôles sont déterminés par des stratégies. Après avoir créé des stratégies, vous créez des rôles, liez chaque rôle à une ou plusieurs stratégies, et attribuez des rôles aux utilisateurs. Vous pouvez également attribuer des rôles à des groupes d'utilisateurs.

Un groupe est une collection d'utilisateurs qui ont des autorisations en commun. Par exemple, les utilisateurs qui gèrent un centre de données particulier peuvent être affectés à un groupe. Un rôle est une identité accordée aux utilisateurs ou aux groupes en fonction de conditions spécifiques. Dans NetScaler Console, la création de rôles et de stratégies est spécifique à la fonctionnalité RBAC de NetScaler. Les rôles et les stratégies peuvent être facilement créés, modifiés ou supprimés à mesure que les besoins de l'entreprise évoluent, sans avoir à mettre à jour individuellement les privilèges de chaque utilisateur.

Les rôles peuvent être basés sur les fonctionnalités ou sur les ressources. Par exemple, considérons un administrateur SSL/sécurité et un administrateur d'applications. Un administrateur SSL/sécurité doit avoir un accès complet aux fonctionnalités de gestion et de surveillance des certificats SSL, mais doit avoir un accès en lecture seule pour les opérations d'administration système. Un administrateur d'applications ne doit pouvoir accéder qu'aux ressources relevant de son périmètre.

Exemple :

Chris, le chef de groupe NetScaler, est le super administrateur de NetScaler Console dans son organisation. Chris crée trois rôles d'administrateur : administrateur de sécurité, administrateur d'applications et administrateur réseau.

David, l'administrateur de sécurité, doit avoir un accès complet à la gestion et à la surveillance des certificats SSL, mais aussi un accès en lecture seule pour les opérations d'administration système.

Steve, un administrateur d'applications, n'a besoin d'accéder qu'à des applications spécifiques et à des modèles de configuration spécifiques.

Greg, un administrateur réseau, a besoin d'accéder à l'administration système et réseau.

Chris doit également fournir le RBAC pour tous les utilisateurs, qu'ils soient locaux ou externes.

Les utilisateurs de NetScaler Console peuvent être authentifiés localement ou via un serveur externe (RADIUS/LDAP/TACACS). Les paramètres RBAC doivent être applicables à tous les utilisateurs, quelle que soit la méthode d'authentification adoptée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'image suivante montre les autorisations dont disposent les administrateurs et les autres utilisateurs, ainsi que leurs rôles dans l'organisation.



Limitations

Le RBAC n'est pas entièrement pris en charge pour les fonctionnalités suivantes de NetScaler Console :

- **Analyse** - Le RBAC n'est pas entièrement pris en charge dans les modules d'analyse. La prise en charge du RBAC est limitée au niveau de l'instance et n'est pas applicable au niveau de l'application dans les modules d'analyse Web Insight, SSL Insight, Gateway Insight, HDX™ Insight et WAF Security Violations. Par exemple :

Exemple 1 : RBAC basé sur l'instance (pris en charge)

Un administrateur auquel quelques instances ont été attribuées peut voir uniquement ces instances sous **Web Insight** \> **Instances**, et uniquement les serveurs virtuels correspondants sous **Web Insight** \> **Applications**, car le RBAC est pris en charge au niveau de l'instance.

Exemple 2 : RBAC basé sur l'application (non pris en charge)

Un administrateur auquel quelques applications ont été attribuées peut voir tous les serveurs virtuels sous **Web Insight** \> **Applications** mais ne peut pas y accéder, car le RBAC n'est pas pris en charge au niveau des applications.

- **Orchestration** - Le RBAC n'est pas pris en charge pour l'orchestration.

Configurer les stratégies d'accès

Les stratégies d'accès définissent les autorisations. Une stratégie peut être appliquée à un seul utilisateur ou groupe, ou à plusieurs utilisateurs et plusieurs groupes. NetScaler Console fournit quatre stratégies d'accès prédéfinies :

1. **adminpolicy**. Accorde l'accès à toutes les fonctionnalités de NetScaler Console. L'utilisateur dispose des autorisations d'affichage et de modification, peut afficher tout le contenu de NetScaler Console et peut effectuer toutes les opérations de modification. C'est-à-dire que l'utilisateur peut effectuer des opérations d'ajout, de modification et de suppression sur les ressources.
2. **readonlypolicy**. Accorde des autorisations en lecture seule. L'utilisateur peut afficher tout le contenu de NetScaler Console, mais n'est pas autorisé à effectuer d'opérations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **appAdminPolicy**. Accorde des autorisations administratives pour l'accès aux fonctionnalités d'application dans NetScaler Console. Un utilisateur lié à cette stratégie peut ajouter, modifier et supprimer des applications personnalisées, et peut activer ou désactiver les services, les groupes de services et les différents serveurs virtuels, tels que la commutation de contenu, la redirection de cache et les serveurs virtuels HAProxy.
4. **appReadOnlyPolicy**. Accorde une autorisation en lecture seule pour les fonctionnalités d'application. Un utilisateur lié à cette stratégie peut afficher les applications, mais ne peut effectuer aucune opération d'ajout, de modification, de suppression, d'activation ou de désactivation.

REMARQUE :

Les stratégies prédéfinies ne peuvent pas être modifiées.

Vous pouvez également créer vos propres stratégies (définies par l'utilisateur).

Pour créer des stratégies d'accès définies par l'utilisateur :

1. Dans NetScaler Console, accédez à **Paramètres > Utilisateurs et rôles > Stratégies d'accès**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom de la stratégie**, entrez le nom de la stratégie, et entrez la description dans le champ **Description de la stratégie**.

   La section **Autorisations** répertorie toutes les fonctionnalités de NetScaler Console, avec des options pour spécifier l'accès en lecture seule, l'activation-désactivation ou la modification.
4. Cliquez sur l'icône (+) pour développer chaque groupe de fonctionnalités en plusieurs fonctionnalités.

   a. Sélectionnez la case à cocher d'autorisation à côté du nom de la fonctionnalité pour accorder des autorisations aux utilisateurs.

   - **Afficher :** Cette option permet à l'utilisateur d'afficher la fonctionnalité dans NetScaler Console.
   - **Activer-Désactiver :** Cette option est disponible uniquement pour les fonctionnalités **Fonctions réseau** qui permettent l'activation ou la désactivation dans NetScaler Console. L'utilisateur peut activer ou désactiver la fonctionnalité. Et l'utilisateur peut également effectuer l'action **Interroger maintenant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque vous accordez l'autorisation **Activer-Désactiver** à un utilisateur, l'autorisation **Afficher** est également accordée. Vous ne pouvez pas désélectionner cette option.

- **Modifier :** Cette option accorde un accès complet à l'utilisateur. L'utilisateur peut modifier la fonctionnalité et ses fonctions.

  Si vous accordez l'autorisation **Modifier**, les autorisations **Afficher** et **Activer-Désactiver** sont toutes deux accordées. Vous ne pouvez pas désélectionner les options sélectionnées automatiquement.

Si vous cochez la case de la fonctionnalité, toutes les autorisations pour cette fonctionnalité sont sélectionnées.

REMARQUE :

Développez Équilibrage de charge et GSLB pour afficher plus d'options de configuration.

Dans l'image suivante, les options de configuration de la fonctionnalité d'équilibrage de charge ont des autorisations différentes :



L'autorisation **Afficher** est accordée à un utilisateur pour la fonctionnalité **Serveurs virtuels**. L'utilisateur peut afficher les serveurs virtuels d'équilibrage de charge dans NetScaler Console. Pour afficher les serveurs virtuels, accédez à **Infrastructure > Fonctions réseau > Équilibrage de charge** et sélectionnez l'onglet **Serveurs virtuels**.

L'autorisation **Activer-Désactiver** est accordée à un utilisateur pour la fonctionnalité **Services**. Cette autorisation accorde également l'autorisation **Afficher**. L'utilisateur peut activer ou désactiver les services liés à un serveur virtuel d'équilibrage de charge. De plus, l'utilisateur peut effectuer l'action **Interroger maintenant** sur les services. Pour activer ou désactiver les services, accédez à **Infrastructure > Fonctions réseau > Équilibrage de charge** et sélectionnez l'onglet **Services**.

REMARQUE :

Si un utilisateur dispose de l'autorisation **Activer-Désactiver**, l'action d'activation ou de désactivation d'un service est restreinte dans la page suivante :

a. Accédez à **Infrastructure > Fonctions réseau**.

b. Sélectionnez un serveur virtuel et cliquez sur **Configurer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Sélectionnez la page **Liaison de service de serveur virtuel d'équilibrage de charge**. Cette page affiche un message d'erreur si vous sélectionnez **Activer** ou **Désactiver**.

L'autorisation **Modifier** est accordée à un utilisateur pour la fonctionnalité **Groupes de services**. Cette autorisation accorde un accès complet lorsque les autorisations **Afficher** et **Activer-Désactiver** sont accordées. L'utilisateur peut modifier les groupes de services liés à un serveur virtuel d'équilibrage de charge. Pour modifier les groupes de services, accédez à **Infrastructure > Fonctions réseau > Équilibrage de charge** et sélectionnez l'onglet **Groupes de services**.

5. Cliquez sur **Créer**.

Accorder des autorisations StyleBook aux utilisateurs

Vous pouvez créer une stratégie d'accès pour accorder des autorisations StyleBook telles que l'importation, la suppression, le téléchargement, et plus encore.

REMARQUE :

L'autorisation Afficher est automatiquement activée lorsque vous accordez d'autres autorisations StyleBook.

Configurer les groupes

Dans NetScaler Console, un groupe peut avoir un accès au niveau des fonctionnalités et au niveau des ressources. Par exemple, un groupe d'utilisateurs peut avoir accès uniquement à certaines instances NetScaler sélectionnées ; un autre groupe à seulement quelques applications sélectionnées, et ainsi de suite.

Lorsque vous créez un groupe, vous pouvez lui attribuer des rôles, lui fournir un accès au niveau de l'application et lui affecter des utilisateurs. Tous les utilisateurs de ce groupe se voient attribuer les mêmes droits d'accès dans NetScaler Console.

Vous pouvez gérer l'accès d'un utilisateur dans NetScaler Console au niveau individuel des entités de fonction réseau. Vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou au groupe au niveau de l'entité.

NetScaler Console traite les serveurs virtuels, les services, les groupes de services et les serveurs comme des entités de fonction réseau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Serveur virtuel (Applications)** - Équilibrage de charge (lb), GSLB, commutation de contexte (CS), redirection de cache (CR), authentification (`Auth`) et NetScaler Gateway (VPN)
- **Services** - Services d'équilibrage de charge et GSLB
- **Groupe de services** - Groupes de services d'équilibrage de charge et GSLB
- **Serveurs** - Serveurs d'équilibrage de charge

Créer un groupe d'utilisateurs

1. Dans NetScaler Console, accédez à **Paramètres > Utilisateurs et rôles > Groupes**.
2. Cliquez sur **Ajouter**.

   La page **Créer un groupe système** s'affiche.
3. Dans le champ **Nom du groupe**, saisissez le nom du groupe. La longueur maximale autorisée est de 64 caractères.
4. Dans le champ **Description du groupe**, saisissez une description de votre groupe. Fournir une bonne description du groupe vous aide à mieux comprendre le rôle et la fonction du groupe ultérieurement.
5. Dans la section **Rôles**, ajoutez ou déplacez un ou plusieurs rôles vers la liste **Configuré**.

   REMARQUE :

   Sous la liste **Disponible**, vous pouvez cliquer sur **Nouveau** ou **Modifier** et créer ou modifier des rôles. Vous pouvez également accéder à **Paramètres > Utilisateurs et rôles > Utilisateurs** et créer ou modifier des utilisateurs.
6. Sélectionnez **Configurer le délai d'expiration de la session utilisateur** pour configurer la période pendant laquelle un utilisateur doit rester actif.

   Lorsqu'elle est activée, spécifiez les paramètres suivants :

   - **Délai d'expiration de la session** : Saisissez la durée pendant laquelle une session utilisateur doit rester active. La valeur par défaut est 15.
   - **Unité de délai d'expiration de la session** : Sélectionnez l'unité de délai d'expiration dans la liste, en minutes ou en heures. La valeur par défaut est les minutes.
7. Dans le champ **Limite de sessions utilisateur**, saisissez le nombre maximal de sessions autorisées par utilisateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous pouvez configurer jusqu'à 40 sessions utilisateur. Par défaut, 20 sessions utilisateur vous sont attribuées. Cependant, si vous appartenez aux groupes d'utilisateurs administrateurs et en lecture seule, 40 sessions utilisateur vous sont attribuées par défaut et cette valeur ne peut pas être modifiée.

1. Cliquez sur **Suivant**. Sous l'onglet **Paramètres d'autorisation**, vous pouvez fournir des paramètres d'autorisation pour les ressources suivantes :

   - Groupes Autoscale™
   - Instances
   - Applications
   - Modèles de configuration
   - StyleBooks
   - Packs de configuration
   - Noms de domaine

   Vous pouvez sélectionner des ressources spécifiques parmi les catégories auxquelles les utilisateurs peuvent avoir accès.

   Groupes de mise à l'échelle automatique :

   Si vous souhaitez sélectionner les groupes de mise à l'échelle automatique spécifiques qu'un utilisateur peut afficher ou gérer, procédez comme suit :

   a. Décochez la case **Tous les groupes de mise à l'échelle automatique** et cliquez sur **Ajouter des groupes de mise à l'échelle automatique**.
   b. Sélectionnez les groupes de mise à l'échelle automatique requis dans la liste et cliquez sur **OK**.

   Instances :

   Si vous souhaitez sélectionner les instances spécifiques qu'un utilisateur peut afficher ou gérer, procédez comme suit :

   a. Décochez la case **Toutes les instances** et cliquez sur **Sélectionner des instances**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Sélectionnez les instances requises dans la liste et cliquez sur **OK**.



Balises :

Pour autoriser les utilisateurs à afficher ou à gérer des instances spécifiques en fonction des balises associées :

a. Désactivez la case à cocher **Toutes les instances** et cliquez sur **Sélectionner les balises**.
b. Sélectionnez les balises requises dans la liste et cliquez sur **OK**.



Plus tard, à mesure que vous associerez davantage d'instances aux balises sélectionnées, les utilisateurs autorisés auront automatiquement accès aux nouvelles instances.

Pour plus d'informations sur les balises et l'association de balises aux instances, consultez Comment créer des balises et les attribuer à des instances.

Applications :

La liste **Choisir les applications** vous permet d'accorder l'accès à un utilisateur pour les applications requises.

Vous pouvez accorder l'accès aux applications sans sélectionner leurs instances. Lorsque vous accordez à un utilisateur l'accès à une application, l'utilisateur est autorisé à accéder uniquement à cette application, quelle que soit la sélection de l'instance.

Les options suivantes sont disponibles :

- **Toutes les applications** : Cette option est sélectionnée par défaut. Elle ajoute toutes les applications présentes dans NetScaler Console.
- **Toutes les applications des instances sélectionnées** : Cette option apparaît uniquement si vous sélectionnez des instances dans la catégorie **Toutes les instances**. Elle ajoute toutes les applications présentes sur l'instance sélectionnée.
- **Applications spécifiques** : Cette option vous permet d'ajouter les applications requises auxquelles vous souhaitez que les utilisateurs aient accès. Cliquez sur **Ajouter des applications** et sélectionnez les applications requises dans la liste.
- **Sélectionner un type d'entité individuelle** : Cette option vous permet de sélectionner un type spécifique d'entité de fonction réseau et les entités correspondantes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez soit ajouter des entités individuelles, soit sélectionner toutes les entités sous le type d'entité requis pour accorder l'accès à un utilisateur.

L'option **Appliquer également aux entités liées** autorise les entités qui sont liées au type d'entité sélectionné. Par exemple, si vous sélectionnez une application et l'option **Appliquer également aux entités liées**, NetScaler Console autorise toutes les entités qui sont liées à l'application sélectionnée.

REMARQUE :

Pour autoriser les entités liées, sélectionnez un seul type d'entité.

Vous pouvez utiliser des expressions régulières pour rechercher et ajouter les entités de fonction réseau qui répondent aux critères d'expression régulière pour les groupes. L'expression régulière spécifiée est conservée dans NetScaler Console. Pour ajouter une expression régulière, procédez comme suit :

a. Cliquez sur **Ajouter une expression régulière**.
b. Spécifiez l'expression régulière dans la zone de texte.

L'image suivante explique comment utiliser une expression régulière pour ajouter une application lorsque vous sélectionnez l'option **Applications spécifiques** :



L'image suivante explique comment utiliser une expression régulière pour ajouter des entités de fonction réseau lorsque vous choisissez l'option **Sélectionner le type d'entité individuelle** :



Si vous souhaitez ajouter d'autres expressions régulières, cliquez sur l'icône **+**.

REMARQUE :

L'expression régulière ne correspond qu'au nom du serveur pour le type d'entité **Serveurs** et non à l'adresse IP du serveur.

Si vous sélectionnez l'option **Appliquer également aux entités liées** pour une entité découverte, un utilisateur peut accéder automatiquement aux entités qui sont liées à l'entité découverte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'expression régulière est stockée dans le système pour mettre à jour la portée d'autorisation. Lorsque les nouvelles entités correspondent à l'expression régulière de leur type d'entité, NetScaler Console met à jour la portée d'autorisation pour les nouvelles entités.

Modèles de configuration :

Si vous souhaitez sélectionner le modèle de configuration spécifique qu'un utilisateur peut afficher ou gérer, effectuez les étapes suivantes :

a. Décochez la case **Tous les modèles de configuration** et cliquez sur **Ajouter un modèle de configuration**.
b. Sélectionnez le modèle requis dans la liste et cliquez sur **OK**.

StyleBooks :

Si vous souhaitez sélectionner le StyleBook spécifique qu'un utilisateur peut afficher ou gérer, effectuez les étapes suivantes :

a. Décochez la case **Tous les StyleBooks** et cliquez sur **Ajouter un StyleBook au groupe**. Vous pouvez soit sélectionner des StyleBooks individuels, soit spécifier une requête de filtre pour autoriser les StyleBooks.

   Si vous souhaitez sélectionner les StyleBooks individuels, sélectionnez les StyleBooks dans le volet **StyleBooks individuels** et cliquez sur **Enregistrer la sélection**.

   Si vous souhaitez utiliser une requête pour rechercher des StyleBooks, sélectionnez le volet **Filtres personnalisés**. Une requête est une chaîne de paires clé-valeur où les clés sont `name`, `namespace` et `version`.

   Vous pouvez également utiliser des expressions régulières comme valeurs pour rechercher et ajouter des StyleBooks qui répondent aux critères d'expression régulière pour les groupes. Une requête de filtre personnalisée pour rechercher des StyleBooks prend en charge les opérations `And` et `Or`.

   Exemple :

   ```
   name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
   version=1.0
   ```

   Cette requête répertorie les StyleBooks qui remplissent les conditions suivantes :

   - Le nom du StyleBook est `lb-mon` ou `lb`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'espace de noms du StyleBook est `com.citrix.adc.stylebooks`.
- La version du StyleBook est `1.0`.

Utilisez une opération `Or` entre les expressions de valeur qui est définie pour l'expression de clé.

Exemple :

- La requête `name=lb-mon|lb` est valide. Elle renvoie les StyleBooks ayant un nom `lb-mon` ou `lb`.
- La requête `name=lb-mon | version=1.0` est invalide.

Appuyez sur `Enter` pour afficher les résultats de la recherche et cliquez sur **Enregistrer la requête**.

La requête enregistrée apparaît dans la **Requête de filtres personnalisés**. En fonction de la requête enregistrée, NetScaler Console fournit aux utilisateurs l'accès à ces StyleBooks.

b. Sélectionnez les StyleBooks requis dans la liste et cliquez sur **OK**.

Vous pouvez sélectionner les StyleBooks requis lorsque vous créez des groupes et ajoutez des utilisateurs à ce groupe. Lorsque votre utilisateur sélectionne le StyleBook autorisé, tous les StyleBooks dépendants sont également sélectionnés.

Packs de configuration :

Dans **Packs de configuration**, sélectionnez l'une des options suivantes :

- **Toutes les configurations** : Cette option est sélectionnée par défaut. Elle permet aux utilisateurs de gérer toutes les configurations présentes dans NetScaler Console.
- **Toutes les configurations des StyleBooks sélectionnés** : Cette option ajoute tous les packs de configuration du StyleBook sélectionné.
- **Configurations spécifiques** : Cette option vous permet d'ajouter des configurations spécifiques de n'importe quel StyleBook.
- **Toutes les configurations créées par le groupe d'utilisateurs** : Cette option permet aux utilisateurs d'accéder uniquement aux configurations créées par les utilisateurs du même groupe.

Vous pouvez sélectionner les packs de configuration applicables lorsque vous créez des groupes et attribuez des utilisateurs à ce groupe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Noms de domaine :

Si vous souhaitez sélectionner le nom de domaine spécifique qu'un utilisateur peut afficher ou gérer, procédez comme suit :

a. Décochez la case **Tous les noms de domaine** et cliquez sur **Ajouter un nom de domaine**.

b. Sélectionnez les noms de domaine requis dans la liste et cliquez sur **OK**.

2. Cliquez sur **Créer un groupe**.
3. Dans la section **Attribuer des utilisateurs**, sélectionnez l'utilisateur dans la liste **Disponible** et ajoutez l'utilisateur à la liste **Configuré**.

REMARQUE :

Vous pouvez également ajouter des utilisateurs en cliquant sur **Nouveau**.

4. Cliquez sur **Terminer**.

Gérer l'accès des utilisateurs à plusieurs entités de fonction réseau

En tant qu'administrateur, vous pouvez gérer l'accès des utilisateurs au niveau individuel des entités de fonction réseau dans NetScaler Console. Et, vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou à un groupe au niveau de l'entité en utilisant le filtre d'expression régulière.

Ce document décrit comment définir l'autorisation de l'utilisateur au niveau de l'entité.

Avant de commencer, créez un groupe. Consultez Configurer des groupes sur NetScaler Console pour plus d'informations.

Scénario d'utilisation :

Prenons un scénario où une ou plusieurs applications (serveurs virtuels) sont hébergées sur le même serveur. Un super administrateur (George) souhaite accorder à Steve (un administrateur d'application) l'accès uniquement à App1 et non au serveur d'hébergement.

Le tableau suivant illustre cet environnement, où le serveur A héberge les applications App-1 et App-2.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SERVEUR HÔTE	APPLICATION (SERVEUR VIRTUEL)	SERVICE	GROUPE DE SERVICES
Serveur A	App1	App-service-1	App-service-group-1
Serveur A	App2	App-service-2	App-service-group-2

REMARQUE

NetScaler Console traite les serveurs virtuels, les services, les groupes de services et les serveurs comme des entités de fonction réseau. Le type d'entité serveur virtuel est appelé application.

Pour attribuer des autorisations utilisateur aux entités de fonction réseau, George définit l'autorisation utilisateur comme suit :

1. Accédez à **Compte > Administration des utilisateurs > Groupes** et ajoutez un groupe.
2. Dans l'onglet **Paramètres d'autorisation**, sélectionnez Choisir des applications.
3. Choisissez **Sélectionner un type d'entité individuel**.
4. Sélectionnez le type d'entité **Toutes les applications** et ajoutez l'entité App-1 à partir de la liste disponible.
5. Cliquez sur **Créer un groupe**.
6. Dans **Attribuer des utilisateurs**, sélectionnez les utilisateurs qui nécessitent l'autorisation. Pour ce scénario, George sélectionne le profil utilisateur de Steve.
7. Cliquez sur **Terminer**.

Avec ce paramètre d'autorisation, Steve peut gérer uniquement App-1 et non d'autres entités de fonction réseau.

REMARQUE :

Assurez-vous que l'option **Appliquer également sur les entités liées** est désactivée. Sinon, NetScaler Console accorde l'accès à toutes les entités de fonction réseau liées à App-1. Par conséquent, l'accès au serveur d'hébergement est également accordé.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un super administrateur peut spécifier les expressions régulières (regex) pour chaque type d'entité. L'expression régulière est stockée dans le système pour mettre à jour la portée de l'autorisation utilisateur. Lorsque de nouvelles entités correspondent à l'expression régulière de leur type d'entité, NetScaler Console peut accorder dynamiquement aux utilisateurs l'accès aux entités de fonction réseau spécifiques.

Pour accorder des autorisations utilisateur de manière dynamique, le super administrateur peut ajouter des expressions régulières dans l'onglet **Paramètres d'autorisation**.

Dans ce scénario, George ajoute `App*` comme expression régulière pour le type d'entité Applications, et les applications qui correspondent aux critères de l'expression régulière apparaissent dans la liste. Avec ce paramètre d'autorisation, Steve peut accéder à toutes les applications qui correspondent à l'expression régulière `App*`. Cependant, son accès est limité uniquement aux applications et non au serveur hébergé.

Comment l'accès utilisateur change en fonction de la portée de l'autorisation

Lorsqu'un administrateur ajoute un utilisateur à un groupe ayant des paramètres de stratégie d'accès différents, l'utilisateur est mappé à plusieurs portées d'autorisation et stratégies d'accès.

Dans ce cas, NetScaler Console accorde à l'utilisateur l'accès aux applications en fonction de la portée d'autorisation spécifique.

Considérons un utilisateur affecté à un groupe qui a deux stratégies : Stratégie-1 et Stratégie-2.

- **Stratégie-1** – Autorisation de consultation uniquement pour les applications.
- **Stratégie-2** – Autorisation de consultation et de modification pour les applications.

L'utilisateur peut consulter les applications spécifiées dans la Stratégie-1. De plus, cet utilisateur peut consulter et modifier les applications spécifiées dans la Stratégie-2. L'accès en modification aux applications du Groupe-1 est restreint car il ne relève pas de la portée d'autorisation du Groupe-1.

Mappage du RBAC lors de la mise à niveau de NetScaler Console de la version 12.0 vers les versions ultérieures

Lorsque vous mettez à niveau NetScaler Console de la version 12.0 à la version 13.1, vous ne voyez pas les options permettant de fournir des autorisations « lecture-écriture » ou « lecture » lors de la création de groupes. Ces autorisations sont remplacées par des « rôles et stratégies d'accès », ce qui vous offre plus de flexibilité pour accorder des autorisations basées sur les rôles aux

© 1997–2026 Citrix Systems, Inc. All rights reserved.

utilisateurs. Le tableau suivant montre comment les autorisations de la version 12.0 sont mappées à la version 13.1 :

12.0	AUTORISER LES APPLICATIONS UNIQUEMENT	13.1
admin lecture-écriture	Faux	`admin`
admin lecture-écriture	Vrai	`appAdmin`
admin lecture seule	Faux	`readonly`
admin lecture seule	Vrai	`appReadonly`

Configurer les rôles

Dans NetScaler Console, chaque rôle est lié à une ou plusieurs stratégies d'accès. Vous pouvez définir des relations un-à-un, un-à-plusieurs et plusieurs-à-plusieurs entre les stratégies et les rôles. Vous pouvez lier un rôle à plusieurs stratégies, et vous pouvez lier plusieurs rôles à une seule stratégie.

Par exemple, un rôle peut être lié à deux stratégies, l'une définissant les autorisations d'accès pour une fonctionnalité et l'autre définissant les autorisations d'accès pour une autre fonctionnalité. Une stratégie peut accorder l'autorisation d'ajouter des instances NetScaler dans NetScaler Console, et l'autre stratégie peut accorder l'autorisation de créer et de déployer des StyleBooks et de configurer des instances NetScaler.

Lorsque plusieurs stratégies définissent des autorisations de modification et de lecture seule pour une seule fonctionnalité, les autorisations de modification ont la priorité.

NetScaler Console fournit quatre rôles prédéfinis :

- **admin**. A accès à toutes les fonctionnalités de NetScaler Console. (Ce rôle est lié à adminpolicy.)
- **readonly**. A un accès en lecture seule. (Ce rôle est lié à readonlypolicy.)
- **appAdmin**. A un accès administratif uniquement aux fonctionnalités d'application dans NetScaler Console. (Ce rôle est lié à appAdminPolicy).
- **appReadonly**. A un accès en lecture seule aux fonctionnalités d'application. (Ce rôle est lié à appReadOnlyPolicy.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Les rôles prédéfinis ne peuvent pas être modifiés.

Vous pouvez également créer vos propres rôles (définis par l'utilisateur).

Pour créer des rôles et leur attribuer des stratégies :

1. Dans NetScaler Console, accédez à **Paramètres > Utilisateurs et rôles**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom du rôle**, saisissez le nom du rôle et indiquez la description dans le champ **Description du rôle** (facultatif).
4. Dans la section **Stratégies**, ajoutez ou déplacez une ou plusieurs stratégies vers la liste **Configuré**.

   
5. Cliquez sur **Créer**.

Configurer les utilisateurs

Par défaut, NetScaler Console dispose d'un utilisateur :

nsroot - L'utilisateur racine (nsroot) dispose de privilèges administratifs complets sur l'appliance. L'utilisateur nsroot est le super administrateur de NetScaler Console.

Vous pouvez créer des utilisateurs supplémentaires en configurant des comptes pour eux. Lorsque vous ajoutez de nouveaux utilisateurs à NetScaler Console, vous pouvez définir leurs autorisations en leur attribuant les groupes, rôles et stratégies appropriés.

Vous pouvez attribuer un utilisateur à un groupe et lier le groupe à des rôles. Vous pouvez définir une relation un-à-un, un-à-plusieurs ou plusieurs-à-plusieurs entre les utilisateurs, les groupes, les rôles et les stratégies d'accès. Un utilisateur peut être affecté à plusieurs groupes. Un groupe peut avoir plusieurs rôles, et plusieurs groupes peuvent avoir des rôles identiques.

Pour configurer les utilisateurs dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Paramètres > Utilisateurs et rôles**.
2. Cliquez sur **Ajouter**.
3. Saisissez les détails suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Nom d'utilisateur**. Nom de l'utilisateur

b. **Mot de passe**. Mot de passe avec lequel l'utilisateur se connecte à NetScaler Console

4. Vous pouvez éventuellement sélectionner **Activer l'authentification externe** afin que l'utilisateur puisse être authentifié via un serveur d'authentification externe.
5. Si vous avez créé des groupes et que vous souhaitez attribuer l'utilisateur à un groupe, dans la section **Groupes**, déplacez un ou plusieurs groupes de la liste **Disponible** vers la liste **Configuré**.



6. Cliquez sur **Créer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tâches exploitables et recommandations

REMARQUE :

- L'onglet **À faire** est renommé en **Recommandations**. Dans **Recommandations**, vous pouvez continuer à examiner les tâches existantes et cliquer sur **Me guider** pour terminer la tâche.
- L'onglet **Archive** n'est plus disponible. Au lieu de cela, vous pouvez choisir de **rejeter** une recommandation de la liste.

Vous pouvez avoir des centaines d'instances NetScaler découvertes et plusieurs serveurs virtuels (applications) configurés à partir de chaque instance. En tant qu'administrateur, vous devez vous assurer que toutes les instances NetScaler et vos applications sont gérées efficacement afin d'obtenir des informations pour une meilleure priorisation et un meilleur dépannage.

À mesure que vous développez votre infrastructure, vous devrez peut-être également vous concentrer sur les problèmes critiques affectant vos instances et applications qui nécessitent votre attention immédiate. Vous devez également vous assurer que votre déploiement NetScaler Console est efficace, sécurisé et conforme. En fonction de votre utilisation et de votre abonnement actuels, la fonctionnalité **Tâches** de NetScaler Console vous permet d'afficher à la fois les **Tâches** exploitables pour lesquelles vous devez prendre des mesures immédiates et les **Recommandations** pour garantir un déploiement efficace.

En tant qu'administrateur, en utilisant ces **Tâches** exploitables et ces **Recommandations**, vous pouvez :

- Obtenir une visibilité instantanée sur toute observation ou tout problème nécessitant une action immédiate de votre part.
- Configurer des notifications pour en recevoir chaque fois que NetScaler Console détecte des tâches et prendre des mesures de manière proactive.
- Réaliser un déploiement efficace de NetScaler Console et des instances NetScaler.
- Réduire le temps et les efforts cruciaux nécessaires à l'identification des problèmes critiques.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Assurez-vous d'utiliser toutes les capacités de NetScaler Console, activez la découverte de produits et les fonctionnalités recommandées par le produit pour une administration efficace du déploiement.

Dans l'interface graphique de NetScaler Console, cliquez sur **Tâches** pour afficher les **Tâches** et les **Recommandations**.



- **Tâches** - Vous permet d'afficher une liste de tâches qui nécessitent votre attention et votre action immédiates. À mesure que vous développez votre infrastructure, certains problèmes critiques peuvent passer inaperçus et entraîner une faille de sécurité. Par exemple, les instances NetScaler avec des CVE nécessitent une attention immédiate et vous devez prendre des mesures immédiates pour vous assurer que les instances exécutent la version et la build recommandées. Dans **Tâches**, vous pouvez obtenir ces informations immédiatement. En fonction de votre utilisation actuelle, vous pouvez afficher un total de 4 tâches. Les tâches sont affichées en fonction de la gravité (Critique et Moyenne).

  

- **Recommandations** - Fournit certaines recommandations basées sur votre utilisation actuelle pour améliorer votre déploiement NetScaler Console. Vous pouvez utiliser l'option **Guide Me** pour compléter toute recommandation. Toute recommandation que vous complétez à l'aide de l'option **Guide Me** est déplacée vers la section Terminées. Vous pouvez également ignorer des recommandations, elles sont alors déplacées sous la catégorie **Ignorées**. Pour afficher vos recommandations ignorées, utilisez le filtre **Par statut** et sélectionnez **Ignorées**.

  Vous pouvez également utiliser le **Filtre par catégorie** pour filtrer des recommandations spécifiques en fonction des catégories (Infrastructure, Application et Sécurité). Alternativement, vous pouvez également utiliser la barre de **Recherche**, taper les premiers caractères pour affiner la tâche.

  

Tâches

Sous **Tâches**, vous pouvez afficher les 4 tâches suivantes en fonction de votre déploiement NetScaler Console actuel.

- **Certificats SSL expirés** – Fournit des informations sur les certificats SSL expirés installés dans votre NetScaler Console. Sélectionnez cette tâche pour afficher les onglets suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Supprimer les certificats inutilisés** : Affiche les certificats qui ne sont pas utilisés dans les instances NetScaler. Pour terminer la tâche, examinez les certificats inutilisés, sélectionnez le certificat, cliquez sur **Afficher et supprimer**.

  Action recommandée : Vous êtes redirigé vers **Infrastructure > Tableau de bord SSL > Certificats SSL - Expirés**. Pour supprimer un certificat, cliquez sur **Supprimer**. Si vous souhaitez mettre à jour le certificat, sélectionnez le certificat et cliquez sur **Mettre à jour**. Pour plus d'informations, consultez Comment mettre à jour un certificat installé.

- **Mettre à jour les certificats** : Affiche les certificats déjà expirés. Pour terminer la tâche, examinez les certificats, sélectionnez le certificat et cliquez sur **Afficher et mettre à jour**.

  Action recommandée : Vous êtes redirigé vers **Infrastructure > Tableau de bord SSL > Certificats SSL - Expirés**. Sélectionnez le certificat et cliquez sur **Mettre à jour** ou **Supprimer**. Pour plus d'informations, consultez Comment mettre à jour un certificat installé.

- **Certificats SSL expirant** – Fournit des informations sur les certificats SSL qui sont sur le point d'expirer.

  Action recommandée : Sélectionnez cette tâche pour afficher les onglets en fonction du nombre total de jours avant la date d'expiration. Pour terminer la tâche, sélectionnez le certificat dans l'onglet, cliquez sur **Afficher et mettre à jour**. Vous êtes redirigé vers la page pertinente dans **Infrastructure > Tableau de bord SSL**. Sélectionnez le certificat et cliquez sur **Mettre à jour**. Pour plus d'informations, consultez Comment mettre à jour un certificat installé.

- **Dérives de configuration** – Fournit des informations sur les écarts de configuration (différence entre la configuration enregistrée et la configuration en cours d'exécution, et différence entre le modèle et la configuration en cours d'exécution) dans les instances NetScaler. Sélectionnez cette tâche pour afficher les onglets suivants :

  - **Instances avec configuration non enregistrée** : Vous pouvez afficher les instances qui ont une configuration non enregistrée. Pour terminer la tâche, sélectionnez l'instance, cliquez sur **Afficher et enregistrer la configuration**.

    Action recommandée : Vous êtes redirigé vers **Infrastructure > Configuration > Audit de configuration > Rapports d'audit** et vous pouvez afficher les instances qui ont des configurations non enregistrées. Cliquez sur **Enregistrer la configuration** pour terminer cette tâche. Pour plus d'informations, consultez la documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Instances avec des dérives par rapport au modèle** : Vous pouvez afficher les instances qui présentent des écarts par rapport au modèle. Pour terminer la tâche, sélectionnez l'instance, cliquez sur **Afficher et exécuter les commandes correctes**.

  Action recommandée : Vous êtes redirigé vers **Infrastructure > Configuration > Audit de configuration > Rapports d'audit** et vous pouvez afficher les instances qui présentent des écarts par rapport au modèle. Suivez la documentation pour terminer la tâche.

- **Avis de sécurité** – Fournit des informations sur les CVE qui affectent vos instances NetScaler. Sélectionnez cette tâche pour afficher les onglets suivants :

  - **CVE détectées** : Affiche les CVE détectées et les instances NetScaler affectant les CVE. Pour terminer cette tâche, sélectionnez une CVE, cliquez sur **Afficher et corriger**.

    Action recommandée : Vous êtes redirigé vers la page **Avis de sécurité** dans **Infrastructure > Avis d'instance > Avis de sécurité**. Suivez la documentation pour terminer la tâche.

  - **Instances affectées** : Affiche les instances NetScaler affectées par des CVE. Pour terminer la tâche, sélectionnez l'instance, cliquez sur **Afficher et corriger**.

    Action recommandée : Vous êtes redirigé vers la page **Avis de sécurité** dans **Infrastructure > Avis d'instance > Avis de sécurité**. Suivez la documentation pour terminer la tâche.

- **Avis de mise à niveau** : Fournit des informations sur vos instances NetScaler® qui ont déjà atteint ou sont sur le point d'atteindre la fin de vie (EOL) ou la fin de maintenance (EOM) dans les 90 jours.

  

  Action recommandée : Cliquez sur **Prendre des mesures** et mettez à niveau les instances vers une version recommandée.

- **Mise à niveau de la note SSL A+** : Fournit des informations sur vos applications qui ne sont pas conformes à une note A+.

  

  Action recommandée : Sélectionnez les applications dans la liste et cliquez sur **Mettre à niveau vers A+**.

  Une fois la mise à niveau réussie, vous verrez le message de succès suivant :

  

  Une fois la mise à niveau terminée, les détails de l'application sont supprimés de la tâche.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Points à noter :

- Selon le nombre d'applications sélectionnées, la durée du processus de mise à niveau peut varier.
- Après avoir lancé un processus de mise à niveau, il est recommandé d'en lancer un autre une fois le processus en cours terminé.
- Vous pouvez également afficher l'état du processus de mise à niveau dans **Infrastructure > Configuration > Tâches de configuration**.
- Si le processus de mise à niveau échoue, vous pouvez afficher l'état dans **Infrastructure > Configuration > Tâches de configuration**. Vous pouvez relancer le processus de mise à niveau à partir de la tâche.
- Si vous effectuez une mise à niveau en bloc et qu'une ou plusieurs applications ne parviennent pas à se mettre à niveau, vous ne pouvez afficher que les détails de ces applications ayant échoué dans la tâche. Vous pouvez relancer le processus de mise à niveau pour le terminer.

REMARQUE :

- Vous pouvez afficher la page suivante si votre NetScaler Console n'a aucune tâche en attente :



- Dans certains scénarios, les vérifications se produisent sur toutes les instances et le chargement de toutes les tâches peut prendre plus de temps.



Recommandations

Le tableau suivant décrit les recommandations que vous pouvez afficher dans l'interface graphique de NetScaler Console :

REMARQUE

Pour les licences en pool, vous recevez des recommandations basées sur vos droits de licence en pool existants.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA RECOMMANDATION	QUAND LA TÂCHE EST-ELLE VISIBLE DANS L'INTERFACE GRAPHIQUE ?
Ajouter un NetScaler	Après votre intégration à NetScaler Console et si aucune instance NetScaler n'est découverte.
Ajouter un agent externe pour utiliser le maximum de fonctionnalités dans NetScaler Console	Si un agent externe n'est pas configuré. Vous pouvez commencer avec un agent intégré. Cependant, un agent externe est requis pour utiliser toutes les fonctionnalités telles que l'analyse, les licences en pool, etc.
Enregistrer un NetScaler d'un agent intégré vers un agent externe	Après votre intégration à NetScaler Console à l'aide du workflow Service Connect, les instances NetScaler sont intégrées à l'aide de l'agent intégré. Vous pouvez enregistrer ces instances NetScaler auprès d'un agent externe pour utiliser toutes les fonctionnalités telles que l'analyse, les licences en pool, etc.
Vous souhaitez réaffecter de la bande passante sur votre NetScaler ? C'est simple !	Si les licences en pool sont allouées dans l'interface graphique de NetScaler et que ces instances NetScaler sont découvertes dans NetScaler Console, vous pouvez effectuer la réaffectation à l'aide de NetScaler Console.
Activer l'accès granulaire basé sur les rôles pour vos utilisateurs d'entreprise clés	Si le contrôle d'accès basé sur les rôles (RBAC) n'est pas encore configuré dans NetScaler Console.
Configurez des règles et ne manquez jamais aucun événement critique sur vos instances NetScaler	Si une règle d'événement personnalisée n'est pas encore configurée.
Besoin de surveiller plusieurs applications et leurs performances ? Créez simplement une application personnalisée.	Si l'application personnalisée n'est pas encore configurée.
Soyez averti et ne manquez jamais les événements critiques dans vos applications	Si la politique d'action n'est pas configurée pour l'écart de score d'application, le temps de traitement du serveur, la latence du réseau client, la latence du réseau serveur ou le temps de réponse.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA RECOMMANDATION	QUAND LA TÂCHE EST-ELLE VISIBLE DANS L'INTERFACE GRAPHIQUE ?
Évitez les pannes d'application et ne manquez jamais les certificats SSL expirant dans une application	Si aucune alerte ou notification n'est configurée pour les certificats SSL expirant.
Avis de sécurité - Maintenez vos instances NetScaler à jour avec les CVE et les mesures d'atténuation	Si les instances NetScaler ont un impact CVE.
Configurez une politique d'entreprise et surveillez les écarts	Si les paramètres d'entreprise SSL ne sont pas modifiés ou sont toujours par défaut.
Vous répétez des tâches manuellement ? Créez des tâches de configuration et appliquez-les à plusieurs instances NetScaler	Si la tâche **Config Job** n'est pas encore configurée.
Gérez et surveillez le score de votre instance en sélectionnant les indicateurs personnalisés de votre choix.	Si les paramètres et seuils par défaut dans **Instance Score Settings** ne sont pas modifiés.
Suivez le score de votre application en sélectionnant les indicateurs personnalisés de votre choix.	Si les composants du score d'application dans le tableau de bord de l'application sont utilisés par défaut et qu'aucune personnalisation n'est effectuée.
Ajoutez des blocs d'adresses IP privées pour visualiser les requêtes client dans la carte géographique.	Si les blocs d'adresses IP ne sont pas configurés. Vous pouvez créer des blocs d'adresses IP pour mapper et visualiser les requêtes client sur une carte géographique en fonction de leurs adresses IP/plages privées.
Abonnez-vous et exportez vos violations AppSec vers Splunk en temps réel.	Si l'intégration de Splunk dans NetScaler Console n'est pas encore configurée.
Personnalisez le seuil par défaut ou créez un nouveau seuil pour vos services Kubernetes.	Si seuls les seuils par défaut sont utilisés dans le graphique de service et qu'aucun seuil simple ou double n'est appliqué aux services.
Configurez de manière proactive les profils de notification et recevez des notifications dans vos destinations de communication.	Si un profil de notification n'est pas encore configuré.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA RECOMMANDATION	QUAND LA TÂCHE EST-ELLE VISIBLE DANS L'INTERFACE GRAPHIQUE ?
Planifiez des exportations récurrentes et recevez des notifications sur les détails de l'infrastructure.	Si aucune planification d'exportation n'est encore configurée dans **Infrastructure > Instances**.
Vous utilisez ServiceNow et souhaitez l'intégrer à NetScaler Console ?	Si l'intégration de ServiceNow dans NetScaler Console n'est pas encore configurée.
Automatisez la gestion des certificats SSL à l'aide de Venafi et NetScaler Console.	Si le serveur Venafi n'est pas encore configuré dans NetScaler Console.
Renouvelez votre licence groupée avant son expiration.	Si votre licence existante est sur le point d'expirer dans 30 jours.
Démarrez avec la licence groupée en allouant votre bande passante groupée achetée aux instances NetScaler.	Si vous n'avez pas encore commencé à allouer vos droits de licence groupée.
Envisagez d'acheter plus de capacité de bande passante groupée.	Si vous avez utilisé 90 % ou plus de votre droit de bande passante groupée.
Votre droit de bande passante groupée actuel est sous-utilisé. Examinez et envisagez d'allouer davantage	Si l'utilisation de votre allocation de licence groupée est inférieure à 70 %.

Comment utiliser le flux de travail Guide me et compléter la recommandation ?

Considérez que vous souhaitez configurer des règles pour tout événement. Cliquez sur **Guide me** pour la tâche suivante :



Après avoir cliqué sur **Guide me**, vous êtes redirigé vers **Infrastructure > Événements > Règles**. Cliquez sur **Ajouter** pour créer une règle. Pour plus d'informations, consultez Créer des règles d'événement.

Une fois la création d'une règle terminée, la recommandation est complète et elle est déplacée vers **Terminé**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

De même, si vous souhaitez compléter une recommandation ultérieurement, vous pouvez sélectionner **Ignorer** dans la liste et elle est déplacée vers **Ignoré**.

Ignorer la recommandation(/en-us/netscaler-application-delivery-management-software/media/dismiss-recommendation.png)

Configurer les notifications

Vous pouvez configurer et recevoir des notifications chaque fois que NetScaler Console identifie des tâches ouvertes nécessitant votre action immédiate. Si vous n'avez pas configuré de notifications, vous pouvez cliquer sur **Configurer la notification** dans le coin supérieur droit.

Notification(/en-us/netscaler-application-delivery-management-software/media/create-notification.png)

Dans la page **Notifications**, vous pouvez configurer des profils pour **Email** et **Slack**, puis cliquer sur **Enregistrer** pour recevoir des notifications. Pour chaque type de notification, l'interface graphique de NetScaler Console affiche la liste de distribution ou le profil configuré. NetScaler Console envoie des notifications à la liste de distribution ou au profil sélectionné.

FAQ

1. Quels types de recommandations sont proposés aux administrateurs ?

   Actuellement, les recommandations sont spécifiques aux déploiements et aident les administrateurs dans les tâches de configuration et de mise en place pour rendre le déploiement efficace. Cela permet également une meilleure découverte du produit et les administrateurs peuvent savoir ce qu'une tâche fait et comment elle peut aider sans aucune connaissance préalable ou sans savoir si la fonctionnalité existe ou non dans NetScaler Console.

2. Que se passe-t-il si j'ignore une recommandation ?

   Les recommandations que vous ignorez sont déplacées vers **Ignorées**. Vous pouvez compléter ces recommandations ultérieurement.

3. La recommandation passe-t-elle à **Terminées** si je commence un « guide-moi » et que je l'interromps ?

   Non, la recommandation n'est pas terminée tant que l'action n'est pas enregistrée ou complétée.

4. Puis-je effectuer une recherche ou un filtrage ?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Oui ! Vous pouvez utiliser la barre de recherche ou affiner la sélection à des tâches spécifiques en sélectionnant la catégorie dans la liste.

5. Recevrai-je des tâches pour agir sur des événements dynamiques ?

   Oui ! Actuellement, vous pouvez afficher un total de 4 tâches exploitables. Pour plus d'informations, consultez Tâches.

6. Toutes les tâches exploitables et plus de 20 recommandations s'afficheront-elles même si je n'ai pas d'instances NetScaler ajoutées dans NetScaler Console ?

   Non. Vous devez disposer d'instances NetScaler et de serveurs virtuels disponibles dans NetScaler Console pour afficher toutes les tâches et recommandations.

7. À quelle fréquence les tâches seront-elles actualisées ?

   Lorsque vous cliquez sur **Tâches** dans le volet de navigation de gauche, elles sont actualisées et disponibles avec le dernier statut. Les détails sont récupérés et mis à jour.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un tableau de bord unifié pour afficher les détails des métriques clés de l'instance

Dans NetScaler Console, vous pouvez afficher diverses informations sur l'utilisation et les performances des applications, l'infrastructure NetScaler, les violations de sécurité (Bot et WAF), etc. En tant qu'administrateur, vous devrez peut-être naviguer vers différentes options dans l'interface graphique de NetScaler Console pour afficher plusieurs informations. Par exemple, pour vérifier les serveurs virtuels (applications) et les informations sur les instances NetScaler :

- Vous devez d'abord naviguer vers **Applications > Tableau de bord** pour afficher les informations sur les applications.
- Ensuite, vous devez naviguer vers **Infrastructure > Analyse de l'infrastructure** pour afficher les informations sur les instances NetScaler.

Pour une meilleure expérience de surveillance, il est nécessaire de disposer d'un privilège qui contient un aperçu de toutes les informations requises. Naviguez vers **Vue d'ensemble > Tableau de bord** pour visualiser un tableau de bord unique avec un aperçu des détails des métriques clés basées sur les catégories suivantes :

- Applications
- Infrastructure NetScaler
- Sécurité des applications
- Passerelle

Applications

Sous **Applications**, vous pouvez afficher :

- **État de l'application** – Fournit un aperçu des applications qui sont en état **Hors service** et **Hors service**, et en fonction de leur statut tel que **Critique**, **En cours d'examen**, **Bon** et **Non applicable**. Cliquez sur **Afficher toutes les applications** pour afficher les détails dans le tableau de bord de l'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Anomalies des signaux dorés** – Fournit un aperçu des applications présentant des erreurs de serveur et des anomalies de temps de réponse. Cliquez sur **Afficher les détails** pour plus d'informations.
- **Optimisation de la configuration de l'application** – Fournit un aperçu du nombre total d'applications présentant des problèmes de performances. Cliquez sur **Voir plus** pour afficher les détails du problème dans le tableau de bord de l'application.
- **Certificats SSL** – Fournit un aperçu des certificats SSL ainsi que de leur validité. Cliquez sur **Gérer les certificats SSL** pour afficher plus d'informations dans le tableau de bord SSL.
- **Application SSL Config Optimization** – Fournit un aperçu du nombre total d'applications présentant des problèmes liés au SSL. Cliquez sur **See More** pour afficher les détails du problème.



Infrastructure NetScaler

Sous **NetScaler Infrastructure**, vous pouvez afficher les métriques clés suivantes liées aux instances NetScaler :

- **NetScaler Instance Health** – Fournit un aperçu du nombre total d'instances NetScaler basé sur le score de l'instance.
- **NetScaler Instances impacted by CVEs** – Fournit un aperçu du nombre total d'instances NetScaler affectées par des vulnérabilités et expositions courantes (CVE).
- **NetScaler Instance Issues** – Fournit un aperçu des problèmes d'instance NetScaler en fonction de la catégorie de problème. Pour plus d'informations, consultez Infrastructure Analytics.
- **NetScaler Instance Upgrade Summary** – Fournit un aperçu du nombre total d'instances NetScaler qui ne sont pas sur la dernière version. Cliquez sur View NetScaler Instances Dashboard pour plus d'informations.



Sécurité des applications

Fournit un aperçu du nombre total d'applications affectées et du nombre total de violations (Bot et WAF) signalées pour la durée sélectionnée. Cliquez sur **View Security Dashboard** pour afficher les détails de la sécurité et des violations de bot.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Passerelle

Fournit un aperçu du nombre total d'utilisateurs de passerelle actifs, du nombre total d'utilisateurs ICA® actifs et du nombre total de connexions ICA actives. Vous pouvez également afficher les erreurs, les détails de connexion des utilisateurs et une carte géographique qui fournit des détails sur les emplacements des utilisateurs.



Personnaliser le tableau de bord

Vous pouvez utiliser l'option **Modifier le tableau de bord** et personnaliser l'affichage du tableau de bord selon vos préférences. À l'aide de l'option **Modifier le tableau de bord**, vous pouvez :

- Faire glisser les widgets
- Supprimer l'intégralité du widget (Applications, Infrastructure NetScaler, Gateway ou Sécurité des applications).
- Supprimer les widgets plus petits présents sous chaque widget.
- Cliquez sur **Ajouter un widget** et sélectionnez les métriques clés requises que vous souhaitez afficher sous chaque widget.

  
- Rétablir les paramètres par défaut
- Rétablir la dernière sauvegarde

Après avoir effectué des modifications, cliquez sur **Enregistrer**.

REMARQUE

- Par défaut, tous les widgets sont affichés. Si vous personnalisez le tableau de bord, enregistrez les modifications et utilisez à nouveau l'option **Rétablir les paramètres par défaut**, tous les widgets sont ajoutés au tableau de bord.
- L'option **Rétablir la dernière sauvegarde** charge la configuration précédemment enregistrée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les détails de l'agent

Dans le tableau de bord unifié, vous pouvez visualiser un aperçu des détails de l'agent. Dans **Vue d'ensemble > Tableau de bord**, à côté de l'**état de l'agent NetScaler®**, vous pouvez afficher les états suivants qui vous permettent d'analyser la disponibilité globale de l'agent :

- **Tous disponibles**. Indique que tous les agents sont opérationnels.
- **Tous indisponibles**. Indique que tous les agents sont hors service et inaccessibles.
- **indisponibles**. Indique que quelques agents sont hors service et inaccessibles.
- **Tous hors service**. Indique que tous les agents sont hors service.
- **hors service**. Indique que quelques agents sont hors service.
- **Agent externe introuvable**. Indique qu'aucun agent (via des hyperviseurs) n'est configuré.

Cliquez sur **Afficher les détails** pour visualiser un aperçu des détails de l'agent, tels que le nombre total d'agents intégrés, le nombre total d'agents externes, l'adresse IP de l'agent, l'état, l'utilisation du système, les vérifications de diagnostic, etc.



Créer et appliquer des filtres

Vous pouvez appliquer des filtres et afficher des informations uniquement pour les instances ou applications sélectionnées dans les éléments suivants :

- Applications
- Infrastructure NetScaler
- Sécurité des applications

Par défaut, toutes les applications sont sélectionnées. Vous pouvez créer un filtre personnalisé à partir du tableau de bord en cliquant sur l'icône de filtres disponible dans la vignette.

Dans la fenêtre **Filtrer les applications** :

1. Sélectionnez **Créer un nouveau filtre**.
2. Fournissez un nom de filtre selon votre choix.
3. Cliquez sur **Sélectionner des applications** et ajoutez toutes les applications requises pour le filtre. Lorsque vous sélectionnez des applications, vous pouvez également utiliser les filtres (**Nom de l'application** et **Type**) et ensuite sélectionner des applications.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez sur **Créer et appliquer le filtre**.



Le filtre est maintenant créé et appliqué. Vous pouvez créer d'autres filtres en suivant la même procédure. Après avoir créé des filtres, vous pouvez les sélectionner et les appliquer via la liste **Sélectionner un filtre parmi les filtres existants**.



Modifier les filtres

Vous pouvez modifier un filtre en le sélectionnant dans la liste et en cliquant sur **Modifier**. À l'aide de l'option de modification, vous pouvez ajouter ou supprimer des applications, puis mettre à jour le filtre.



Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

REMARQUE

Lorsque vous créez un filtre avec des applications et que l'une des applications est supprimée dans le tableau de bord des applications, les détails de l'application sont immédiatement supprimés du tableau de bord unifié.

Créer des tableaux de bord personnalisés pour afficher les détails des métriques clés d'instance

À l'instar du tableau de bord unifié (**Vue d'ensemble > Tableau de bord**), vous pouvez afficher les détails des métriques d'instance en fonction de votre choix en créant des tableaux de bord personnalisés. Vous pouvez créer jusqu'à 30 tableaux de bord en utilisant un nom unique pour chacun. En tant qu'administrateur, cette amélioration vous permet de créer plusieurs tableaux de bord et de surveiller uniquement les informations d'instance requises.

Pour commencer, imaginez que vous souhaitez surveiller les métriques clés pour les **Applications** et la **Sécurité des applications** :

1. Accédez à **Vue d'ensemble > Tableau de bord personnalisé**.
2. Cliquez sur **+** pour créer un nouveau tableau de bord.

   Dans la page **Créer un tableau de bord personnalisé** :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Nom du tableau de bord personnalisé** - Spécifiez un nom unique pour le tableau de bord.

b. **Description** - Fournissez une brève description pour avoir des détails supplémentaires.

c. **Ajouter un widget au tableau de bord** - Dans cet exemple, l'exigence est d'ajouter des widgets pour les applications et la sécurité des applications. Sélectionnez les widgets que vous souhaitez surveiller dans les catégories **Application** et **Sécurité des applications**.

d. **Filtre d'application** - Par défaut, le filtre est appliqué à toutes les applications. Vous pouvez également créer un filtre et sélectionner uniquement des applications spécifiques. Pour plus d'informations, consultez Créer et appliquer des filtres.

e. Cliquez sur **Enregistrer**.

Le tableau de bord est créé avec succès. De même, vous pouvez créer jusqu'à 20 tableaux de bord et sélectionner des catégories selon votre choix en spécifiant un nom unique pour chaque tableau de bord.

Vous pouvez utiliser les options suivantes après avoir créé un tableau de bord personnalisé :

- **Modifier** : Vous pouvez modifier le tableau de bord en ajoutant ou en supprimant des widgets, en appliquant des filtres, et ainsi de suite.
- **Renommer** : Vous pouvez modifier le nom du tableau de bord.
- **Supprimer** : Vous pouvez supprimer le tableau de bord.

Plus d'options dans le tableau de bord

Dans le tableau de bord personnalisé que vous avez créé, vous pouvez utiliser les options suivantes :

- **Modifier la configuration** : Vous pouvez également utiliser cette option pour modifier le tableau de bord en ajoutant ou en supprimant des widgets, en appliquant des filtres, et ainsi de suite.
- **Modifier la disposition** : Vous pouvez utiliser cette option pour personnaliser davantage le tableau de bord.
  - Vous pouvez choisir de déplacer vers le haut, vers le bas ou de supprimer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Dans les widgets, vous pouvez supprimer n'importe quel widget en sélectionnant l'option Supprimer.



- Faites glisser et déposez pour placer les widgets où vous le souhaitez.
- Augmentez ou diminuez la taille du widget pour une meilleure visibilité de certaines informations.



Après avoir effectué des modifications, cliquez sur **Enregistrer** pour afficher le tableau de bord mis à jour.

Partager le tableau de bord avec d'autres utilisateurs

Vous pouvez partager le tableau de bord avec d'autres utilisateurs. Sélectionnez un tableau de bord existant et cliquez sur **Partager**. Saisissez le nom d'utilisateur et cliquez sur **Inviter** pour partager le tableau de bord. L'utilisateur assigné peut afficher le tableau de bord en mode lecture seule.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications

La fonctionnalité d'analyse et de gestion des applications de NetScaler Console vous permet de surveiller les applications via une approche centrée sur l'application. Cette approche vous aide à :

- Vérifier le score et analyser les performances globales des applications
- Vérifier la persistance de tout problème avec le serveur ou le client
- Détecter les anomalies dans les flux de trafic des applications et prendre des mesures correctives

> **REMARQUE**
>
> Les applications font référence à un ou plusieurs serveurs virtuels configurés sur les instances (NetScaler).

Vous pouvez surveiller les applications pour des durées telles que 1 heure, 1 jour, 1 semaine et 1 mois.

Prérequis

- Assurez-vous d'avoir ajouté des instances NetScaler dans NetScaler Console
- Assurez-vous de disposer d'une licence valide pour vos instances NetScaler. Pour plus d'informations, consultez Licences
- Assurez-vous d'avoir appliqué une licence pour les serveurs virtuels. Pour plus d'informations, consultez Gérer les licences sur les serveurs virtuels

Présentation des applications

Les applications peuvent être :

- Applications discrètes
- Applications personnalisées
- Applications de microservices (k8s_discrete)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications discrètes

Tous les serveurs virtuels sous licence sont appelés applications discrètes.

Applications personnalisées

Les serveurs virtuels d'une même catégorie sont appelés applications personnalisées. En tant qu'administrateur, vous devez ajouter des applications personnalisées en fonction d'une catégorie. Vous pouvez ensuite gérer et surveiller les applications via le tableau de bord. Vous bénéficiez d'une facilité de surveillance des applications spécifiques regroupées sous une même catégorie.

Par exemple, vous pouvez créer une catégorie pour votre centre de données 1 et y ajouter ses instances NetScaler. Une fois que vous avez défini une catégorie et ajouté l'instance pour votre centre de données 1, le tableau de bord de l'application s'affiche avec une catégorie distincte, comprenant toutes les applications liées à votre centre de données 1.

Points à noter

- Les applications discrètes ajoutées aux applications personnalisées sont supprimées des applications discrètes.
- Toutes les applications qui ne sont ajoutées à aucune catégorie sont disponibles sous la forme **« autres »**.
- Par défaut, NetScaler Console vous permet d'ajouter des licences pour un maximum de 2 applications. En fonction de votre licence, vous pouvez sélectionner et appliquer des licences pour les applications que vous souhaitez surveiller.

Applications de microservices

Dans un cluster Kubernetes, NetScaler fournit un contrôleur d'entrée pour NetScaler MPX (matériel), NetScaler VPX (virtualisé) et NetScaler CPX (conteneurisé). Pour plus d'informations, consultez Contrôleur d'entrée NetScaler.

Les applications discrètes configurées à l'aide des instances NetScaler CPX sont appelées applications de microservices.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion des applications et tableau de bord des applications

NetScaler Console vous permet de gérer les applications à partir de la page **Applications** et d'afficher les détails des applications à partir de la page **Tableau de bord**.

Gérer les applications

Depuis le tableau de bord des applications, cliquez sur **Gérer les applications** pour afficher toutes les applications personnalisées et discrètes.

Depuis la page **Gérer les applications**, en tant qu'administrateur, vous pouvez :

- Ajouter des applications
- Afficher les détails de l'application tels que le nom de l'application, le type d'application, la catégorie d'application, les serveurs virtuels associés, les services associés, etc.
- Modifier ou supprimer des applications personnalisées

Pour plus d'informations, consultez Gérer les applications.

Tableau de bord des applications

Accédez à **Applications** > **Tableau de bord** pour afficher la liste des applications en mode tableau ou en mode graphique.



Toutes les applications ne s'affichent dans le tableau de bord qu'après avoir commencé à générer des données. Depuis le tableau de bord, cliquez sur une application pour afficher des informations détaillées sur les performances de l'application. Pour plus d'informations, consultez Détails de l'application.

Si les analyses d'application ne s'affichent pas même après environ 10 à 15 minutes, effectuez les étapes de dépannage à l'adresse Dépanner le tableau de bord de l'application.

Mises à jour du nouveau comportement du tableau de bord par rapport à l'ancien tableau de bord

- Après avoir ajouté ou modifié une application personnalisée, quelques minutes peuvent être nécessaires pour que l'application s'affiche dans le tableau de bord.
- Si vous supprimez une application personnalisée, le tableau de bord affiche toujours l'application supprimée, jusqu'à ce que NetScaler Console dispose de ses données analytiques (durée maximale d'un mois).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considérez un scénario dans lequel vous avez créé une application le Jan 2, 2020 et vous avez supprimé l'application le Jan 4, 2020. Dans ce scénario :

- Le tableau de bord peut toujours afficher l'application supprimée le Jan 4, 2020, lorsque vous sélectionnez la durée pour le dernier jour, la dernière semaine et le dernier mois.
- Le tableau de bord peut toujours afficher l'application supprimée le Jan 5, 2020, lorsque vous sélectionnez la durée pour la dernière semaine et le dernier mois.
- Lorsque la durée dépasse la date de suppression de l'application, l'application n'est pas affichée dans le tableau de bord. Autrement dit, le tableau de bord n'affiche pas l'application supprimée le Jan 6, 2020 (pour le dernier jour), le Jan 12, 2020 (pour la dernière semaine), et après le February 5, 2020 (pour le dernier mois).

  REMARQUE

  Après avoir ajouté une application, si l'instance NetScaler associée est Hors service, hors ligne ou inaccessible en raison d'un problème réseau temporaire :

  -Les applications associées à l'instance NetScaler ne sont visibles que dans la page **Applications**, mais pas dans le tableau de bord.
  -Les applications sont affichées dans le tableau de bord une fois que l'instance NetScaler est opérationnelle.

Gérer les applications

Depuis le tableau de bord, cliquez sur **Gérer les applications** pour afficher les détails de l'application et ajouter, modifier ou supprimer des applications personnalisées.

Afficher les détails de l'application

- **Nom de l'application** – Indique le nom de l'application
- **Disponibilité** – Indique la disponibilité actuelle de l'application, telle que **Actif**, **Inactif**, **Partiellement actif**, **Hors service** et **N/A**
  - **Actif** – Tous les serveurs virtuels associés à l'application sont actifs.
  - **Inactif** – Tous les serveurs virtuels associés à l'application sont inactifs.
  - **Partiellement actif** – Soit un serveur virtuel associé à l'application est inactif, soit il est hors service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Hors service** – Tous les serveurs virtuels associés aux applications sont hors service.
- **N/A** – Aucun serveur virtuel n'est configuré pour l'application.

- **Type** – Indique si l'application appartient à Personnalisé ou Discret
- **Catégorie** – Indique la catégorie d'application regroupée.
- **Serveur virtuel/état** – Indique le nombre total de serveurs virtuels configurés et l'état actuel de tous les serveurs virtuels. Passez le pointeur de la souris pour afficher les détails tels que le nombre total de serveurs virtuels, le type de serveur virtuel et l'état du serveur virtuel.



- **Services/état** – Indique le nombre total de services configurés et l'état actuel de tous les services
- **Groupes de services/état** – Indique le nombre total de groupes de services configurés et l'état de tous les groupes de services
- **Serveurs/état** – Indique le nombre total de serveurs configurés pour l'application et l'état actuel de tous les serveurs
- **Actions** – Permet de modifier ou de supprimer les applications personnalisées

Ajouter une application

1. Cliquez sur **Nouvelle application** pour créer une nouvelle application

   La page **Définir l'application** s'affiche

   

   REMARQUE

   Vous pouvez également cliquer sur **Applications**, puis sélectionner **Nouvelle application** pour ajouter une nouvelle application

2. Définissez les paramètres suivants :

CHAMP	DESCRIPTION
Nom	Nom de l'application personnalisée. Par exemple, LB_TEST.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHAMP	DESCRIPTION
Catégorie	La catégorie dans laquelle vous pouvez regrouper les applications. Cliquez pour accéder à la page Catégorie d'application. Sélectionnez la catégorie et cliquez sur **Sélectionner**. Pour ajouter une catégorie :
	1. Cliquez sur **Ajouter**
	2. Saisissez un nom de votre choix.
	3. Cliquez sur **Créer**
Sélectionner les applications existantes	Permet de sélectionner les applications existantes ajoutées aux instances NetScaler.
Ajouter une application	Affiche tous les serveurs virtuels configurés sur les instances. Sélectionnez les applications dans la liste et cliquez sur **OK**.
Définir les critères de sélection	Option permettant de définir l'application par plage de serveurs virtuels, ou par plage d'adresses IP de serveur d'origine/de service.
	- **Serveur.** Spécifiez l'adresse IP du serveur ou du service, le nom du serveur ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez saisir une adresse IP, une plage d'adresses IP ou une combinaison des deux, séparées par des virgules. Par exemple, vous pouvez saisir 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
	- **Serveurs virtuels.** Vous pouvez spécifier l'un des éléments suivants : l'adresse IP du serveur virtuel, le nom du serveur virtuel ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez saisir une adresse IP, une plage d'adresses IP ou une combinaison des deux, séparées par

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHAMP	DESCRIPTION
	des virgules. Par exemple, vous pouvez saisir 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
Créer une nouvelle application à partir d'un StyleBook	Permet de créer une application à l'aide du StyleBook. Pour plus d'informations, consultez Créer une application à l'aide du StyleBook.

a. Cliquez sur **OK**.

REMARQUE

Actuellement, le tableau de bord des applications ne prend en charge que les serveurs virtuels d'équilibrage de charge et de commutation de contenu.

Le tableau de bord des applications s'affiche maintenant avec la catégorie et toutes les applications sont regroupées en dessous.

Si vous sélectionnez l'option **Créer une nouvelle application à partir d'un StyleBook** pour l'application personnalisée, vous devez autoriser NetScaler Console à sélectionner automatiquement les serveurs virtuels pour la licence. Pour activer la sélection automatique des serveurs virtuels :

a. Accédez à **Paramètres** > **Configuration des licences et de l'analyse**.

b. Sous **Allocation de licence de serveur virtuel**, cliquez sur **Sélectionner automatiquement les serveurs virtuels** et **Sélectionner automatiquement les serveurs virtuels non adressables** pour activer.

Créer une application à l'aide du StyleBook

Pour créer une application à l'aide du StyleBook :

1. Dans NetScaler Console, accédez à **Applications** > **Tableau de bord** et cliquez sur **Définir une application personnalisée** pour créer une application personnalisée.
2. Dans la page **Définir l'application**, saisissez le nom de l'application dans le champ **Nom**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Sélectionnez la catégorie d'application dans la section Catégorie. NetScaler Console vous permet de définir des catégories pour regrouper les applications définies par l'utilisateur. Vous pouvez également ajouter d'autres catégories si nécessaire.
4. Cliquez pour sélectionner **Créer une nouvelle application à partir d'un StyleBook** et cliquez sur **OK**.

   La page Choisir un StyleBook s'affiche. Cette page contient tous les StyleBooks par défaut disponibles dans NetScaler Console.
5. Sélectionnez le StyleBook. La page **Détails de la configuration** s'affiche.
6. Saisissez les valeurs de tous les paramètres dans le StyleBook. Vous pouvez également cliquer sur Afficher la définition pour afficher la construction du StyleBook avant de l'utiliser.

   Pour plus d'informations, consultez Utiliser les StyleBooks par défaut.
7. Cliquez sur **Créer**.

   Vous pouvez également cliquer sur **Exécution à blanc** pour vérifier les configurations que NetScaler Console tente de créer sur l'instance NetScaler sélectionnée. Cette option est uniquement à des fins de test pour voir la vérification finale des configurations. Même si l'option Exécution à blanc est réussie, la configuration réelle sur le NetScaler sélectionné peut toujours échouer pour diverses raisons (conflit d'adresses IP, instance inaccessible, etc.).

Modifier ou supprimer une application

Depuis la page **Applications**, vous pouvez modifier ou supprimer les applications personnalisées. Cliquez sur le bouton de modification pour modifier une application et cliquez sur le bouton de suppression pour supprimer l'application.

Exporter les rapports du tableau de bord des applications et du tableau de bord de sécurité

NetScaler Console vous permet de prendre un instantané du tableau de bord des applications actuel et de l'exporter sous forme de rapports. À intervalles fréquents, les administrateurs d'applications peuvent avoir besoin d'utiliser ces rapports pour mettre à jour l'utilisation des applications et les pénalités de performance.

Grâce à cette fonctionnalité, les administrateurs peuvent extraire ces données sous forme de rapports .png, .jpeg ou .pdf.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Contrairement aux autres options d'exportation de rapports dans NetScaler Console, vous ne pouvez exporter les rapports du tableau de bord des applications et du tableau de bord de sécurité qu'au format .pdf ou .png. Le format .csv n'est pas pris en charge actuellement.

Le rapport est téléchargé sur votre système. Depuis les pages Tableau de bord des applications et Tableau de bord de sécurité des applications, vous pouvez également naviguer vers des pages de deuxième niveau et les exporter sous forme de rapports. Actuellement, vous ne pouvez télécharger les rapports que d'une seule application à la fois.

Afficher les applications

Par défaut, le tableau de bord des applications affiche toutes les applications. Selon vos besoins, vous pouvez utiliser l'option de filtre pour afficher les applications.



Le tableau de bord affiche les détails d'application suivants :

- **Nom de l'application** – Indique le nom de l'application
- **Score de l'application** – Indique le score de l'application et le statut tel que **Critique**, **Bon**, **Moyen** et **Non applicable**
- **Disponibilité** – Indique la disponibilité actuelle de l'application, telle que **Actif**, **Inactif**, **Partiellement actif**, **Hors service** et **NA**
  - **Actif** – Tous les serveurs virtuels associés à l'application sont actifs.
  - **Inactif** – Tous les serveurs virtuels associés à l'application sont inactifs.
  - **Partiellement actif** – Soit un serveur virtuel associé à l'application est inactif, soit il est hors service.
  - **Hors service** – Tous les serveurs virtuels associés aux applications sont hors service.
  - **NA** – Aucun serveur virtuel n'est configuré pour l'application.
- **Problème principal** – Indique le problème qui a le nombre maximal d'erreurs sur l'application
- **Catégorie de problème principal** – Indique la catégorie du problème
- **Nombre de problèmes** – Indique le nombre total de problèmes pour l'application
- **Temps de réponse** – Indique le temps de réponse moyen de l'application
- **Pourcentage d'erreurs** – Indique le pourcentage total d'erreurs 5xx pour l'application

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

La métrique de pourcentage d'erreurs 5xx est affichée uniquement pour **NetScaler 13.0 ou version ultérieure**. Pour les versions antérieures, la valeur est affichée comme **0**.

- **Requêtes totales** – Indique le nombre total de requêtes reçues par l'application
- **Débit** – Indique le débit réseau total pour l'application. Le débit est calculé par les octets de requête/seconde + octets de réponse/seconde pour les serveurs virtuels
- **Volume de données** – Indique le volume total de données traitées par l'application
- **Connexions client** – Indique le nombre moyen de connexions client établies par l'application
- **Connexions serveur** – Indique le nombre moyen de connexions serveur établies par l'application

Configurer et associer une application à plusieurs applications personnalisées

Dans le **tableau de bord des applications**, vous pouvez configurer une application et l'associer à plusieurs applications personnalisées. Grâce à cette fonctionnalité, vous pouvez réutiliser la même application pour plusieurs applications personnalisées, au lieu de créer une application distincte pour chaque application personnalisée.

Supposons que vous gériez deux portails de commerce électronique nommés respectivement **ComABC** et **ComCDE**, et que vous souhaitiez utiliser un serveur de passerelle de paiement nommé **PaymentApp** pour les deux portails. Dans ce scénario, vous devez :

- Créez deux applications personnalisées nommées **ComABC** et **ComCDE**.
- Créez une application nommée **PaymentApp** et associez-la à **ComABC** et **ComCDE**.

Pour implémenter ce scénario, vous devez :

- Créez les **applications personnalisées (ComABC et ComCDE)** :
  a. Accédez à **Applications > Tableau de bord**, puis cliquez sur **Gérer les applications**.
  b. Cliquez sur **Nouvelle application**.
  c. Spécifiez un nom et une catégorie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Sélectionnez le type pour choisir l'application. Dans cet exemple, l'option **Sélectionner les applications existantes** est sélectionnée. Pour plus d'informations, consultez Ajouter une application.

e. Sous **Applications**, cliquez sur **Ajouter des applications**.

f. Sélectionnez les applications dans la liste et cliquez sur **OK** pour créer l'application personnalisée.

- Créez la **PaymentApp**. Pour cela, vous devez convertir une application discrète en application personnalisée :

a. Accédez à **Applications > Tableau de bord**, puis cliquez sur **Gérer les applications**.

b. Cliquez sur **Nouvelle application**.

c. Spécifiez un nom et une catégorie.

d. Sélectionnez le type pour choisir l'application. Dans cet exemple, l'option Sélectionner les applications existantes est sélectionnée. Pour plus d'informations, consultez Ajouter une application.

e. Sous **Applications**, cliquez sur **Ajouter des applications**.

f. Sélectionnez les applications dans la liste et cliquez sur **OK** pour créer l'application personnalisée.

- Ensuite, vous pouvez utiliser l'application **PaymentApp** et l'associer à **ComABC** et **ComCDE**.

a. Accédez à **Applications > Tableau de bord**, et **cliquez sur Gérer les applications**.

b. Localisez l'application **ComABC** et cliquez sur **Modifier**.



c. Sous **Applications référencées**, cliquez sur **Ajouter des applications personnalisées**, et sélectionnez l'application **PaymentApp**.

d. L'application **PaymentApp** est maintenant disponible sous **Applications référencées**. Cliquez sur **OK** pour associer l'application **PaymentApp** à l'application personnalisée **ComABC**.



e. Répétez la même procédure pour l'application personnalisée **ComCDE**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Une fois l'application associée à l'application personnalisée, le score final de l'application personnalisée est calculé en fonction du score le plus bas entre l'application personnalisée et l'application référencée. Dans cet exemple, si le score de l'application **ComABC** est de 85 et celui de l'application **PaymentApp** est de 69, le score final de l'application **ComABC** devient 69.

Vue d'ensemble du tableau de bord des applications

Le tableau de bord des applications affiche les applications discrètes sous **Autres** et les applications personnalisées regroupées sous leurs catégories respectives.

Accédez à **Application** > **Tableau de bord** pour afficher le tableau de bord de l'application.



1 – Affiche les détails de l'application pour la durée sélectionnée, tels que 1 heure, 1 jour, 1 semaine et 1 mois.

2 – Vous permet de gérer les applications et d'en ajouter de nouvelles

3 – Vous permet d'afficher les applications en mode tableau ou en mode graphique

4 – Vous permet de rechercher une application à l'aide de la barre de recherche

5 – Vous permet d'appliquer des filtres pour afficher les applications. Cliquez pour voir les détails.



Vous pouvez sélectionner le curseur de carrousel qui vous permet d'accéder facilement à toutes les options.

Vous pouvez :

- Sélectionnez pour afficher les applications en fonction des scores.
    - **Critique** – Le score de l'application est compris entre 0 et < 40
    - **Moyen** – Le score de l'application est compris entre 40 et < 75
    - **Bon** – Le score de l'application est supérieur à 75
    - **Non applicable** – Soit aucun serveur virtuel sous licence n'est configuré pour l'application, soit le type de serveur virtuel n'est pas l'équilibrage de charge ou la commutation de contenu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le tableau suivant décrit les différences entre l'ancien score d'application et le score d'application actuel.

SCORE DE L'APPLICATION (CRITIQUE, À EXAMINER, BON, NON APPLICABLE)	SCORE DE L'APPLICATION (VUE PRÉCÉDENTE AVEC LÉGENDES DE COULEUR)
Le score est calculé comme **100 moins le score de pénalité de tous les problèmes actuels de l'application**	Le score est calculé comme **100 – (Ressource du serveur d'applications + Ressource système NetScaler)**
Les applications sont affichées dans des couleurs telles que **Rouge (critique)**, **Orange (à examiner)**, **Vert (bon)** et **Gris (non applicable)**	Les applications sont affichées dans les légendes de couleur.

- Sélectionnez pour afficher les applications en fonction de leur état, tel que Actif, Inactif et Hors service
- Sélectionnez pour afficher les applications en fonction de leur type, tel que Discret ou Personnalisé
- Sélectionnez pour afficher les applications en fonction des catégories regroupées ci-dessous
- Faites glisser l'histogramme pour appliquer des filtres et afficher les applications.

  Par exemple, si vous souhaitez afficher les applications dont l'état de santé du serveur virtuel est compris entre 0 et 20, faites glisser l'histogramme de l'état de santé du serveur virtuel pour filtrer les résultats.

  

  REMARQUE

  Vous pouvez également cliquer sur l'histogramme pour afficher les applications pertinentes.

  Cliquez sur **Effacer tout** pour effacer le filtre appliqué.

  

  Voici le récapitulatif des applications pour lesquelles vous pouvez appliquer des filtres :

  - **Temps de réponse** – Un histogramme qui affiche le temps de réponse moyen reçu par les applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Taux d'erreur** – Un histogramme qui affiche le pourcentage d'erreur moyen des erreurs 5xx pour les applications
- **Requêtes totales** – Un histogramme qui affiche le nombre total de requêtes reçues par les applications
- **Débit** – Un histogramme qui affiche le débit réseau total traité par les applications
- **Volume de données** – Un histogramme qui affiche le volume total de données traitées par les applications. Le volume de données est calculé à partir du nombre total d'octets de requête et d'octets de réponse pour les applications.
- **Connexions client** – Un histogramme qui affiche le nombre moyen de connexions client établies par les applications
- **Connexions serveur** – Un histogramme qui affiche le nombre moyen de connexions serveur établies par les applications
- **Paquets envoyés** – Un histogramme qui affiche le nombre total de paquets envoyés par les applications
- **Paquets reçus** – Un histogramme qui affiche le nombre total de paquets reçus par les applications
- **État du serveur virtuel** – Un histogramme qui affiche le nombre total d'applications dont le score se situe entre 0 % et 100 %. L'état d'un serveur virtuel correspond au pourcentage de services actifs associés à l'application. Par exemple, si un serveur virtuel est configuré avec 2 services et que l'un d'eux est hors service, le score est de 50 %.

Rechercher et filtrer les résultats à l'aide de la barre de recherche

Vous pouvez placer le pointeur de la souris sur la barre de recherche et sélectionner la catégorie pour affiner la recherche.

Créer et appliquer des balises aux applications

Si vous avez un grand nombre d'applications, vous pouvez créer et appliquer des balises à ces applications. Ces balises améliorent la fonctionnalité de recherche.

Exemple :

La procédure suivante répertorie les étapes pour créer des balises pour les applications d'équilibrage de charge :

1. Dans **App Dashboard**, sélectionnez les applications d'équilibrage de charge pour lesquelles vous souhaitez créer des balises et cliquez sur **Tags**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Dans **Mettre à jour les balises** :
   - Spécifiez un nom de votre choix. Par exemple : **Type**.
   - Spécifiez la valeur qui vous permet d'attribuer les balises. Vous pouvez également saisir plusieurs valeurs. Par exemple : **Loadbalance**.
   - Cliquez sur **Appliquer**.

   

   La balise est créée.

Pour appliquer des balises et récupérer les applications d'équilibrage de charge :

1. Dans la barre de recherche du tableau de bord de l'application, cliquez à l'intérieur de la zone de texte pour afficher le tag créé et sélectionnez le nom du tag.

   

2. Sélectionnez l'opérateur (**IN**) et la valeur qui est créée, puis cliquez sur **Rechercher**.

   

   Toutes les applications d'équilibrage de charge qui sont taguées sous **Loadbalance** sont listées. De même, vous pouvez créer des tags pour d'autres applications.

Détails de l'application

REMARQUE :

À partir de la version **14.1-21.x**, vous pouvez afficher les détails des métriques pour les applications créées à partir des partitions d'administration NetScaler.

Cliquez sur une application dans le tableau de bord pour obtenir des informations détaillées.



La page de l'application sélectionnée s'affiche.



Depuis la page des détails de l'application :

- Sélectionnez la durée dans la liste pour afficher les détails pour cette durée spécifique.
- Cliquez sur **Service Graph** pour afficher le graphique de service de l'application sélectionnée. Pour plus d'informations, consultez Service Graph for Applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cliquez sur **Transaction Logs** pour afficher les transactions détaillées pour les erreurs 5xx.
- Cliquez sur **Audit logs** pour afficher les informations détaillées du journal d'audit.
- Cliquez sur **Configure** pour afficher ou modifier la configuration du service et du groupe de services pour l'application.
- Cliquez sur **Service** pour afficher les services liés à l'application.

Après avoir sélectionné la durée, les détails de l'application suivants s'affichent :

- **Score de l'application** – Le score de l'application pour la durée sélectionnée. Le score final est calculé comme **100 moins la pénalité totale**.

  Ce tableau de bord vous permet également d'afficher les problèmes actuels qui affectent le score de l'application. Vous pouvez afficher les détails des problèmes sous Problèmes.

- **Serveurs virtuels** –

  REMARQUE

  La section **Serveurs virtuels** s'affiche uniquement pour les applications personnalisées. Pour les applications discrètes, cliquez sur l'**adresse IP** pour afficher les détails du serveur virtuel.

  Affiche tous les serveurs virtuels associés à l'application personnalisée

  Cliquez sur **Afficher les détails** pour afficher et gérer les paramètres du serveur virtuel.

- **Tous les services** – Les services liés à l'application

  Cliquez pour afficher les détails du service et gérer les paramètres du service

  Vous pouvez également sélectionner un service et utiliser l'option **Moniteurs liés** pour afficher l'état.

- **Problèmes** – Les problèmes applicables à l'application sélectionnée. Vous pouvez afficher les problèmes suivants avec leur catégorie :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCES	ÉTAT DE L'INSTANCE	CONFIGURATION	RESSOURCES SYSTÈME
Temps de réponse	Utilisation moyenne du CPU	Serveur instable	Type de persistance incorrect
Services actifs	Utilisation de la mémoire	Paquets HTTP inhabituellement volumineux	Saturation de la carte NIC
Faible réutilisation de session		Dépassements de la limite de la file d'attente de réassemblage TCP	
Accumulation de SurgeQueue			
Trafic SSL en temps réel			
Accumulation de sessions			
Basculement de service			

Cliquez sur chaque problème pour vérifier les détails tels que le message de détection, le moment où le problème est survenu, les actions recommandées et d'autres détails.

Pour plus d'informations, consultez Indicateurs de performance pour l'analyse des applications.

L'image suivante est l'affichage précédent de la page App Activity Investigator :



Vous pouvez désormais afficher tous les problèmes dans la section **Problèmes**, ainsi que la catégorie que vous pouviez afficher dans la page **App Activity Investigator**.



- Les problèmes affichés dans l'onglet **Actuel** font référence aux problèmes d'application pour la durée sélectionnée.
- Les problèmes affichés dans l'onglet **Tous** font référence à l'ensemble des problèmes d'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'exemple suivant présente les problèmes d'application pour une durée d'un jour. L'onglet **Actuel** n'indique aucun problème actuel ayant un impact sur le score de l'application.

L'onglet **Tous** affiche le nombre total de problèmes détectés sur une durée d'un jour.



Sélectionner les composants de l'App Score et définir des seuils

Dans le **tableau de bord des applications**, en tant qu'administrateur, vous pouvez choisir de sélectionner les composants et de configurer des seuils pour le calcul du score d'application. L'App Score est le système de notation qui définit :

- Dans quelle mesure une application fonctionne bien
- Si l'application fonctionne bien en termes de réactivité

Accédez à **Applications > Tableau de bord**, puis sélectionnez l'icône des paramètres.

Dans la page **Configurer l'App Score**, vous pouvez sélectionner les composants et configurer des seuils pour déterminer le score d'application final.



Le calcul de l'App Score est basé sur les composants suivants :

COMPOSANTS DE L'APP SCORE	SEUILS CONFIGURÉS PAR L'UTILISATEUR	DESCRIPTION
Utilisation de la mémoire NetScaler	Oui	La valeur de seuil basse et haute pour l'utilisation totale de la mémoire dans l'instance NetScaler
Accumulation de la file d'attente de surtension	Oui	La valeur de seuil basse et haute pour le total des requêtes de surtension qui sont en file d'attente et nécessitent une réponse.
Utilisation du CPU NetScaler	Oui	La valeur de seuil basse et haute pour l'utilisation totale du CPU dans l'instance NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANTS DE L'APP SCORE	SEUILS CONFIGURÉS PAR L'UTILISATEUR	DESCRIPTION
Temps de réponse	Oui	L'intervalle de temps entre l'envoi d'un paquet de requête et la réception du premier paquet de réponse du service configuré sur le serveur virtuel.
Utilisation CPU App	Oui	La valeur de seuil basse et haute pour l'utilisation totale du CPU par l'application.
Services actifs	Oui	La valeur de seuil du pourcentage de services qui doivent être actifs et qui sont liés au serveur virtuel.
Type de persistance incorrect	Non	Indique si l'utilisation de la persistance sur un serveur virtuel est faible.
Erreur de serveur (5xx)	Non	Indique si le serveur web répond avec des erreurs 5xx.
Paquets HTTP exceptionnellement volumineux	Non	Indique les occurrences, si la taille des en-têtes HTTP des messages HTTP dépasse les valeurs configurées dans l'instance NetScaler.
Trafic SSL en temps réel	Non	Analyse le trafic SSL pour identifier le trafic en temps réel et suggère des paramètres de configuration optimaux pour améliorer la latence.
Accumulation de sessions SSL	Non	Indique l'accumulation de sessions sur une période donnée, ce qui peut entraîner une consommation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COMPOSANTS DE L'APP SCORE	SEUILS CONFIGURÉS PAR L'UTILISATEUR	DESCRIPTION
		importante de mémoire par ces sessions dans l'instance NetScaler.
Faible réutilisation de session	Non	Indique si le nombre réel de sessions réutilisées par l'instance NetScaler est inférieur.
Saturation de la carte NIC	Non	Indique le nombre total de paquets ignorés par les interfaces.
Dépassements de la limite de la file d'attente de réassemblage TCP	Non	Indique si les paquets hors séquence sur une connexion TCP dépassent la taille configurée de la file d'attente de paquets hors séquence.

Par défaut, tous les composants sont activés. Si vous désactivez un composant, NetScaler Console effectue le calcul final du score d'application uniquement en fonction des composants sélectionnés.

Remarque

> Vous pouvez également continuer à configurer les seuils en accédant à **Paramètres > Paramètres d'analyse** et en cliquant sur **Configurer le score d'application**.

Détails de l'application pour les applications de microservices

Cliquez sur une application de microservices dans le tableau de bord pour obtenir des informations détaillées.

La page de l'application sélectionnée s'affiche. À partir de la page des détails de l'application :

- Sélectionnez la durée dans la liste pour afficher les détails de la durée spécifique

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Cliquez sur **Graphe de service** pour afficher le graphe de service de l'application sélectionnée. Pour plus d'informations, consultez Graphe de service pour les applications
- Cliquez sur **Journaux de transactions** pour afficher les transactions détaillées de l'application sélectionnée
- Cliquez sur **Journaux d'audit** pour afficher les informations détaillées des journaux d'audit

Après avoir sélectionné la durée, les détails de l'application suivants s'affichent :

- **Score de l'application** – Le score de l'application pour la durée sélectionnée. Vous pouvez également afficher les problèmes actuels de l'application, connus sous le nom de score de pénalité applicable en fonction de la catégorie de problème. Le score final est calculé comme **100 moins la pénalité totale**.

  

  1 – Indique le score actuel de l'application

  2 – Indique l'adresse IP CPX, le type d'application tel que l'équilibrage de charge ou la commutation de contenu, ainsi que l'espace de noms de service et le nom du cluster où le service est hébergé

  3 – Indique les problèmes affectant le score actuel de l'application

  Ce tableau de bord vous permet également d'afficher les problèmes actuels qui affectent le score de l'application. Vous pouvez afficher les détails des problèmes sous Problèmes.

- **Détails du service K8s**

  Vous pouvez afficher les détails suivants :

  

  - **Nom du service** – Le nom du service
  - **Nom du cluster** – Le nom du cluster où le service est hébergé
  - **Espace de noms** – L'espace de noms attribué au service
  - **Étiquettes de service** – Les étiquettes de service attribuées au service

- **Détails du pod**

  Un pod est un groupe de conteneurs hébergés dans le cluster Kubernetes. À l'intérieur d'un pod, vous pouvez déployer plusieurs applications conteneurisées. Chaque pod est associé à une adresse IP.

  

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cliquez sur l'état du pod pour afficher les détails



- **Adresse IP du pod** – Indique l'adresse IP du pod
- **Nom d'hôte** – Indique le nom d'hôte attribué au pod
- **Instance** – Indique l'adresse IP du NetScaler CPX
- **État du POD** – Indique l'état actuel du pod

- **Métriques clés** – Les détails des métriques clés, tels que le **Temps de réponse**, les **Erreurs 5xx**, les **Requêtes par seconde**, le **Débit**, les **Connexions client**, les **Connexions serveur** et le **Volume de données** sont affichés.

  Pour chaque métrique, vous pouvez afficher la valeur moyenne et la valeur de différence pour la durée sélectionnée. La valeur de différence est calculée comme la **première valeur moins la dernière valeur** de la durée sélectionnée.

  Vous pouvez afficher les métriques d'instance suivantes sous forme de graphique pour la durée sélectionnée :

  

  L'image suivante est un exemple pour le **Volume de données** et la durée sélectionnée est de 1 mois. La valeur 202,66 Mo est le volume de données total pour la durée d'un mois et la valeur 8,13 Mo est la valeur de différence. Dans le graphique, la première valeur est 14,11 et la dernière valeur est 5,98. La valeur de différence est 14,11 – 5,98 = 8,13 Mo.

  

- **Problèmes** – Les problèmes applicables à l'application sélectionnée. Vous pouvez afficher les problèmes suivants avec leur catégorie :

PERFORMANCE	ÉTAT DE L'INSTANCE	CONFIGURATION	RESSOURCES SYSTÈME
Temps de réponse	Utilisation moyenne du CPU	Réponse 5xx élevée	Type de persistance incorrect
Faible réutilisation de session	Utilisation de la mémoire	Paquets HTTP inhabituellement volumineux	Saturation de la carte NIC
Accumulation de SurgeQueue		Dépassements de la limite de la file	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PERFORMANCE	ÉTAT DE L'INSTANCE	CONFIGURATION	RESSOURCES SYSTÈME
		d'attente de réassemblage TCP	
Trafic SSL en temps réel			

Cliquez sur chaque problème pour afficher les informations suivantes :

- Nombre total d'occurrences
- Actions recommandées pour résoudre le problème
- Les détails du problème tels que l'heure, le nom du service, le nombre total d'occurrences, la gravité et le message de détection

  - Les problèmes affichés dans l'onglet **Actuel** font référence aux problèmes d'application pour la durée sélectionnée.
  - Les problèmes affichés dans l'onglet **Tous** font référence à l'ensemble des problèmes d'application.

L'exemple suivant présente les problèmes d'application sur une durée d'un jour. L'onglet **Actuel** n'indique aucun problème actuel ayant un impact sur le score de l'application.

L'onglet **Tous** affiche le nombre total de problèmes détectés sur une durée d'un jour.

Analyse intelligente des applications

L'analyse intelligente des applications vous permet d'identifier les problèmes de performance des applications à l'aide d'algorithmes d'apprentissage automatique et basés sur des règles. La fonctionnalité d'analyse intelligente des applications de NetScaler Console :

- Fournit une solution simple et évolutive pour la surveillance et le dépannage des applications qui sont fournies via des instances NetScaler.
- Surveille tous les niveaux de l'application afin de réduire le temps de résolution des problèmes et d'améliorer la disponibilité globale de l'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans un déploiement typique, des milliers de serveurs répondent aux besoins en données des utilisateurs. Le trafic envoyé à ces serveurs est équilibré en charge et surveillé par des serveurs virtuels configurés sur des appliances NetScaler. Chaque serveur virtuel est lié à plusieurs services représentant les serveurs backend. Dans de tels déploiements, la fonctionnalité d'analyse intelligente des applications vous aide à :

- Surveiller, gérer et prendre des décisions lors de pannes et d'autres événements
- Surveiller les serveurs virtuels et les services configurés pour une application
- Afficher des informations critiques sur les serveurs virtuels et les services, afin que vous puissiez modifier les configurations si nécessaire pour que les applications atteignent des performances optimales.

Lorsque vous augmentez la taille de votre ferme de serveurs d'entreprise, il devient difficile de suivre les problèmes associés à l'énorme quantité de trafic reçue sur les serveurs et de cibler le dépannage nécessaire.

Lorsqu'une application est en cours d'exécution et reçoit une grande quantité de trafic, vous pouvez rencontrer divers problèmes. Vous pouvez afficher les indicateurs de performance pour l'analyse des applications en accédant à **Applications** > **Tableau de bord**, en sélectionnant une application et en faisant défiler vers le bas pour afficher les problèmes dans la section **Problèmes**.

Configurer l'analyse intelligente des applications

REMARQUE :

À partir de la **version 14.1-21.x**, le collecteur de métriques est désactivé par défaut dans les nouvelles instances NetScaler ajoutées dans NetScaler Console. La configuration du collecteur de métriques pour les instances gérées existantes reste inchangée.

La fonctionnalité d'analyse intelligente des applications est prise en charge uniquement dans **NetScaler 12.1.50.x ou version ultérieure**. Le **collecteur de métriques** envoie les données de compteur NetScaler à NetScaler Console, qui sont utilisées pour détecter les problèmes d'application. Pour utiliser la fonctionnalité d'analyse intelligente des applications, le **collecteur de métriques** doit être configuré sur chaque instance NetScaler.

À partir de la version 14.1-29.x, le collecteur de métriques et l'analyse d'utilisation allégée sont activés au niveau du serveur virtuel au lieu du niveau de l'instance. Grâce à cette amélioration, le

© 1997–2026 Citrix Systems, Inc. All rights reserved.

collecteur de métriques et l'analyse d'utilisation allégée restent activés uniquement sur vos serveurs virtuels actifs à fort trafic.

Vous pouvez examiner vos serveurs virtuels et activer le collecteur de métriques et l'utilisation allégée sur d'autres serveurs virtuels

Pour examiner et activer le **collecteur de métriques** :

1. Accédez à **Paramètres > Configuration de l'analyse**.
2. Cliquez sur **Configurer les métriques** sous **Résumé des métriques du serveur virtuel**.

   
3. Dans la page **Tous les serveurs virtuels**, vous pouvez afficher l'état du collecteur de métriques sur chaque serveur virtuel. Sélectionnez les serveurs virtuels que vous souhaitez activer et cliquez sur **Activer les métriques**.

   
4. Sélectionnez **Activer les métriques** pour activer le collecteur de métriques. Vous pouvez également sélectionner **Données allégées** si vous souhaitez activer et afficher l'analyse d'utilisation de la période allégée. Après avoir sélectionné, cliquez sur **Enregistrer la configuration**. Pour plus d'informations, consultez Analyse d'utilisation de pointe et allégée.

   

Vous pouvez également activer le collecteur de métriques et l'utilisation allégée pour les serveurs virtuels à partir de la page des instances NetScaler :

1. Naviguez vers **Infrastructure > Instances**, sélectionnez le type d'instance, et sélectionnez **Metrics Collector** dans la liste **Sélectionner l'action**.
2. Sélectionnez les serveurs virtuels pour lesquels vous souhaitez activer le collecteur de métriques et cliquez sur **Activer les métriques**.
3. Sélectionnez **Activer les métriques** pour activer le collecteur de métriques. Vous pouvez également sélectionner **Données allégées** si vous souhaitez activer et afficher les analyses d'utilisation de la période creuse. Après la sélection, cliquez sur **Enregistrer la configuration**.

Une fois l'option **Metrics Collector** activée sur le serveur virtuel, accédez à **Applications** > **Tableau de bord**. Sélectionnez une instance pour afficher les anomalies dans la section **Problèmes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Pour afficher les anomalies pour les **Erreurs de serveur** et sa **transaction web détaillée**, vous devez activer l'analyse sur les serveurs virtuels.

Indicateurs de performance pour l'analyse des applications

Vous pouvez afficher les indicateurs de performance, ainsi que leurs catégories qui apparaissent dans les applications web NetScaler. Pour afficher ces indicateurs, vous devez vous assurer d'activer l'analyse et le (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/dashboard/intelligent-app-analytics/configure-intelligent-app-analytics.html) sur l'instance NetScaler :

Après avoir activé l'analyse et le collecteur de métriques, vous pouvez afficher les indicateurs suivants en accédant à **Applications** > **Tableau de bord**, en sélectionnant une application et en faisant défiler jusqu'à la section **Problèmes** :

- Temps de réponse
- Services actifs
- Utilisation moyenne du CPU
- Utilisation de la mémoire
- Saturation de la carte NIC
- Instabilités de service
- Faible réutilisation de session
- Type de persistance incorrect
- Serveur instable (5xx)
- Trafic SSL en temps réel
- Paquets HTTP anormalement volumineux
- Atteinte de la limite de la file d'attente de réassemblage TCP
- Accumulation de la file d'attente en cas de pic

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Temps de réponse

Ce problème est détecté lorsque le temps de réponse de l'application aux requêtes client s'écarte de la valeur de seuil configurée. Cliquez sur l'onglet **Temps de réponse** pour afficher les détails du problème.



Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la période sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Quand le problème est survenu
- Le nombre total d'occurrences pour la période sélectionnée
- La gravité du problème, telle que faible, moyenne et élevée
- Le message de détection indiquant que le temps de réponse total des transactions dépasse la valeur de seuil configurée

Services actifs

Ce problème est détecté lorsque le pourcentage de services actifs liés au serveur virtuel est inférieur à la valeur de seuil configurée. Cliquez sur l'onglet **Services actifs** pour afficher les détails du problème.



Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Quand le problème est survenu
- Le nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème (faible, moyenne et élevée)
- Le message de détection indiquant le pourcentage de sessions de service actives et la valeur de seuil configurée

Utilisation moyenne du CPU

Ce problème est détecté lorsque l'utilisation du CPU NetScaler pour cette application dépasse la valeur de seuil configurée. Cliquez sur l'onglet **Utilisation moyenne du CPU** pour afficher les détails du problème.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails.
- Quand le problème est survenu
- Le nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, telle que faible, moyenne et élevée
- Le message de détection indiquant le pourcentage d'utilisation moyenne du CPU NetScaler et la valeur de seuil configurée

Utilisation de la mémoire

Ce problème est détecté lorsque l'utilisation de la mémoire NetScaler pour cette application dépasse la valeur de seuil configurée. Cliquez sur l'onglet **Utilisation de la mémoire** pour afficher les détails du problème.



Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails.
- Quand le problème est survenu
- Le nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème (faible, moyenne et élevée)
- Le message de détection indiquant le pourcentage moyen d'utilisation de la mémoire NetScaler et la valeur de seuil configurée

Basculement de services

En tant qu'administrateur réseau, vous devez garantir la disponibilité optimale de l'application. En cas de problèmes réseau ou de configuration, l'état et la disponibilité d'un serveur d'applications peuvent avoir un impact sur les performances globales.

Les événements de basculement de services vous permettent d'identifier l'application qui rencontre des problèmes. Les événements de basculement de services vous aident également à :

- Comprendre quel service est en état HORS SERVICE (DOWN) pendant une durée spécifique

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Comprendre combien de services sont en état ACTIF (UP) ou HORS SERVICE (DOWN) pendant une durée spécifique

Cliquez sur l'onglet **Basculement de services** pour afficher les détails des basculements de services.



Vous pouvez afficher des détails tels que le nombre d'occurrences et l'heure de la dernière occurrence.

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie de basculement de service s'est produite
- Le nom du service/groupe de services
- L'adresse IP du service
- L'état actuel du service

Serveur instable

Dans certains scénarios, le serveur web répond avec des codes d'état lorsqu'il est incapable de traiter les requêtes pour des raisons telles que des requêtes invalides, une surcharge temporaire ou une maintenance du serveur. Ces erreurs sont affichées avec des codes d'erreur, qui définissent divers scénarios d'erreurs. Par exemple,

- **502 Bad Gateway** Le serveur agit comme une passerelle ou un proxy et a reçu une réponse invalide du serveur en amont.
- **503 Service Unavailable** Le serveur est actuellement indisponible. Les serveurs peuvent être surchargés ou en maintenance.
- **504 Gateway Time-out** Le serveur agit comme une passerelle ou un proxy et n'a pas reçu de réponse en temps voulu du serveur en amont.

Ces conditions peuvent être temporaires, mais parfois vous devez mettre en œuvre une mesure corrective sur les serveurs web pour que les pages web soient opérationnelles et disponibles.

À l'aide de l'indicateur **Serveur instable**, vous pouvez visualiser ces défaillances et prendre des décisions concernant les actions correctives pour résoudre les problèmes et garantir que les requêtes des clients sont traitées et que les pages web sont toujours disponibles.

Sélectionnez l'onglet **Serveur instable** pour afficher les détails du problème.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les **Actions recommandées** pour résoudre le problème sont :

- Configurez des moniteurs L7 avec des paramètres appropriés pour le serveur qui répond avec des erreurs 5xx. Un moniteur est une entité qui surveille l'état du service. L'appliance sonde périodiquement les serveurs à l'aide du moniteur lié à chaque service. Si un serveur ne répond pas dans le délai de réponse spécifié et que les sondes spécifiées échouent, le service est marqué comme HORS SERVICE (DOWN). L'appliance effectue ensuite l'équilibrage de charge parmi les services restants. Pour plus d'informations sur la configuration d'un moniteur, consultez Moniteurs personnalisés
- Dépanner le serveur

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie du serveur instable s'est produite
- Le nom du service/groupe de services
- Nombre total d'occurrences
- La gravité de l'anomalie (élevée, faible et moyenne)
- Le message de détection indiquant le pourcentage des réponses de ce service signalant des erreurs 5xx

Pour des informations détaillées sur les transactions web d'erreurs de serveur, consultez Analyse des transactions web pour les erreurs de serveur

Accumulation de sessions

Pour toutes les transactions sécurisées, NetScaler effectue le processus de déchargement SSL pour la première transaction, puis stocke la session SSL en fonction de la configuration de **Réutilisation de session**.

En fonction du débit de trafic, une accumulation de sessions peut se produire sur une période donnée, ce qui peut entraîner une consommation importante de mémoire par ces sessions dans NetScaler.

Les événements d'accumulation de sessions alertent les administrateurs et fournissent des actions recommandées pour résoudre cet événement. Cliquez sur l'onglet **Accumulation de sessions** pour afficher les détails du problème.

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie d'accumulation de sessions s'est produite

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le nom du serveur virtuel
- La gravité de l'anomalie (par exemple, élevée, faible et moyenne)
- Le message indiquant que **X** sessions SSL sont disponibles sur le serveur virtuel et qu'actuellement, il y a **Y** poignées de main SSL par seconde dans la session de délai d'attente configurée.

L'**Action recommandée** pour corriger cette anomalie est soit de réduire le délai d'expiration de la session, soit de désactiver la réutilisation de la session. Pour plus d'informations, consultez Délai d'expiration de session.

Faible réutilisation de session

Les instances NetScaler traitent les transactions SSL en déchargeant le processus de négociation SSL du serveur. Dès réception de la réponse du serveur, l'instance NetScaler termine la transaction sécurisée avec le client. En utilisant les paramètres de session mis en cache, l'instance NetScaler termine le processus de négociation SSL pour les requêtes consécutives.

Si ces sessions ne sont pas réutilisées, elles deviennent une surcharge pour les instances NetScaler. À l'aide de l'indicateur **Faible réutilisation de session**, vous pouvez identifier si le nombre réel de sessions réutilisées est inférieur.

Cliquez sur l'onglet **Faible réutilisation de session** pour afficher les détails du problème.



L'**Action recommandée** pour résoudre le problème consiste à désactiver la réutilisation de session ou à réduire le délai d'expiration de session. Pour plus d'informations, consultez Réutilisation de session.

Sous **Détails**, vous pouvez afficher :

- Nombre total d'applications présentant une faible réutilisation de session
- L'heure à laquelle l'anomalie de faible réutilisation de session s'est produite
- Nombre total d'occurrences
- La gravité de l'anomalie (élevée, faible et moyenne)
- Le message de détection indiquant que seulement % des sessions configurées sont réutilisées

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accumulation de la file d'attente de surtension

Lorsqu'un serveur reçoit un afflux de requêtes, il devient lent à répondre aux clients. Souvent, la surcharge entraîne également la réception de pages d'erreur par les clients. Un serveur virtuel doit disposer de suffisamment de serveurs back-end configurés pour gérer les requêtes entrantes.

À l'aide de l'indicateur **Accumulation de la file d'attente de surtension**, vous pouvez afficher les serveurs virtuels présentant une accumulation de la file d'attente de surtension. Cliquez sur l'onglet **Accumulation de la file d'attente de surtension** pour afficher les détails du problème.

File d'attente de surtension(/en-us/netscaler-application-delivery-management-software/media/iaa-surgequeue.png)

Les **actions recommandées** pour résoudre le problème sont :

- Augmentez la limite du nombre de connexions client. Pour plus d'informations, consultez Définir une limite sur le nombre de connexions client
- Augmentez le nombre de serveurs back-end pour traiter les requêtes d'application

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie d'accumulation de la file d'attente de surtension s'est produite
- Nombre total d'occurrences
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Le message de détection indiquant l'accumulation de la file d'attente de surtension sur le serveur virtuel

Paquets HTTP inhabituellement volumineux

Une transaction HTTP utilise des messages de requête-réponse entre le client et le serveur. Dans les messages de requête et de réponse, les en-têtes HTTP sont les valeurs affichées dans le protocole HTTP. Vous pouvez configurer la longueur de l'en-tête HTTP dans le serveur virtuel, le service ou le groupe de services pour éviter les erreurs 4xx.

Lorsqu'une requête/réponse HTTP dépasse la longueur maximale de l'en-tête, il peut s'agir d'une attaque potentielle. À l'aide de l'indicateur **Paquets HTTP inhabituellement volumineux**, vous pouvez afficher les occurrences où les messages HTTP dont la taille de l'en-tête HTTP dépasse les valeurs configurées.

Cliquez sur l'onglet **Paquets HTTP inhabituellement volumineux** pour afficher les détails du problème.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Les **Actions recommandées** pour résoudre le problème sont :

- Examinez le trafic pour déterminer si la taille de l'en-tête est légitime. Si la taille de l'en-tête est légitime, mettez à jour la valeur de l'en-tête sur le profil HTTP. Pour plus d'informations, consultez Vérification du dépassement de tampon.
- Si la taille de l'en-tête n'est pas légitime, ajoutez la source à la liste de blocage pour éviter les attaques.

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie s'est produite
- Nombre total d'occurrences
- La gravité de l'anomalie (par exemple, élevée, faible et moyenne)
- Le message de détection indiquant la longueur actuelle de l'en-tête HTTP configurée sur le serveur virtuel, le serveur ou le groupe de services

Type de persistance incorrect

Vous devez configurer la persistance sur un serveur virtuel si vous souhaitez maintenir les états des connexions sur les serveurs représentés par ce serveur virtuel (par exemple, les connexions utilisées dans le commerce électronique). L'appliance utilise alors la méthode d'équilibrage de charge configurée pour la sélection initiale du serveur, mais transmet toutes les requêtes ultérieures à ce même serveur depuis le même client.

La persistance est efficace lorsque les sessions existantes sont réutilisées pour traiter les requêtes ultérieures. Si la réutilisation des sessions de persistance est faible, les sessions créées sur NetScaler ne sont qu'une surcharge.

À l'aide de l'indicateur **Type de persistance incorrect**, vous pouvez déterminer si l'utilisation de la persistance sur un serveur virtuel est faible. Cliquez sur l'onglet **Type de persistance incorrect** pour afficher les détails du problème.



L'**Action recommandée** pour résoudre le problème est de vérifier le type de persistance ou de désactiver la persistance. Pour plus d'informations, consultez Paramètres de persistance.

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie s'est produite
- Nombre total d'occurrences

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Le message de détection indiquant le pourcentage de sessions inutilisées

Dépassements de la limite de la file d'attente de réassemblage TCP

TCP maintient une file d'attente hors-séquence pour conserver les paquets hors-séquence dans la communication TCP. Ce paramètre a un impact sur la mémoire NetScaler si la taille de la file d'attente est importante, car les paquets doivent être conservés en mémoire d'exécution.

Cette taille de file d'attente doit être à un niveau optimisé en fonction des caractéristiques du réseau et de l'application.

En utilisant l'indicateur **Dépassements de la limite de la file d'attente de réassemblage TCP**, vous pouvez voir si les paquets hors-séquence sur une connexion TCP dépassent la taille configurée de la file d'attente de paquets hors-séquence.

Cliquez sur l'onglet **Dépassements de la limite de la file d'attente de réassemblage TCP** pour afficher les détails du problème.



Les **Actions recommandées** pour résoudre le problème sont :

- Examiner le trafic et bloquer la source s'il s'agit d'une attaque
- Si ce comportement est un comportement réseau attendu, mettez à jour la valeur de la taille des paquets hors-séquence sur le profil TCP. Pour plus d'informations, consultez Optimisation TCP
- S'il s'agit juste d'un problème réseau temporaire, aucune autre action n'est requise

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie s'est produite
- Nombre total d'occurrences
- La gravité de l'anomalie, telle que faible, moyenne et élevée
- Le message de détection indiquant le profil TCP actuel et les paramètres oooQsize

Trafic SSL en temps réel

Dans l'instance NetScaler, vous pouvez utiliser un profil SSL pour le traitement du trafic SSL. Le profil SSL comprend certains paramètres SSL pour les serveurs virtuels, les services et les groupes de services. L'indicateur **Trafic SSL en temps réel** analyse le trafic SSL pour identifier le

© 1997–2026 Citrix Systems, Inc. All rights reserved.

trafic en temps réel et suggère des paramètres de configuration optimaux pour améliorer la latence.

Cliquez sur l'onglet **Trafic SSL en temps réel** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème est d'améliorer la latence du réseau en mettant à jour les paramètres SSL. Pour plus d'informations, consultez Paramètres SSL globaux.

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle l'anomalie s'est produite
- Le nom du service/groupe de services
- La gravité de l'anomalie, telle que faible, moyenne et élevée
- Le message de détection avec le paramètre actuel de l'application

Dépanner le tableau de bord des applications

Après avoir ajouté une application dans le tableau de bord des applications, le tableau de bord affiche immédiatement les détails de configuration de base de l'application. Les détails d'analyse de l'application, tels que le score de l'application, les métriques clés et les problèmes, commencent à s'afficher en quelques minutes (environ 10 à 15 minutes). Pour plus d'informations, consultez Applications.

Vous devez vous assurer qu'il n'y a aucun problème avec le flux de données de métriques (collecteur AppFlow ou profil Analytics) depuis l'instance NetScaler. Vous trouverez plus d'informations sur le collecteur AppFlow et le profil Analytics dans ce document.

Ce document décrit les étapes de dépannage que vous devez effectuer lorsque :

- Vous cliquez sur une application, les analyses de l'application sélectionnée n'affichent pas les données requises même après la durée mentionnée (10 à 15 minutes).
- L'application CS ou LB indique toujours une couleur grise (état **Non applicable**) dans le tableau de bord des applications.

REMARQUE

Les procédures de dépannage mentionnées dans ce document ne s'appliquent qu'aux serveurs virtuels de **commutation de contenu** et d'**équilibrage de charge**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scénario de dépannage



L'application est sous licence

Vous devez vous assurer que l'application est sous licence. À partir de la version **14.1-21.x**, tous les serveurs virtuels sont automatiquement sous licence. Si vous utilisez une version antérieure, accédez à **Paramètres > Configuration des licences et des analyses** et vérifiez si l'application est sous licence sous **Résumé des licences de serveurs virtuels**. Si l'application n'est pas sous licence, Gérer les licences et activer les analyses sur les serveurs virtuels.

Le collecteur de métriques est activé

REMARQUE :

À partir des versions **14.1-21.x ou ultérieures**, le collecteur de métriques est désactivé par défaut dans les nouvelles instances NetScaler ajoutées dans NetScaler Console. La configuration du collecteur de métriques pour les instances gérées existantes reste inchangée.

Vous devez vous assurer que **Metrics Collector** est activé dans l'instance NetScaler. Pour vérifier si le collecteur de métriques est activé :

1. Accédez à **Infrastructure > Instances**. Sous Instances, sélectionnez le type d'instance (par exemple, NetScaler VPX).
2. Sélectionnez l'instance NetScaler.
    a. Dans la liste **Sélectionner une action**, sélectionnez **Metrics Collector**.



3. Sur la page **Configurer les paramètres du collecteur de métriques**, assurez-vous que l'option **Activer** est sélectionnée. Si ce n'est pas le cas, sélectionnez l'option **Activer** et cliquez sur **OK**.

Après avoir activé le collecteur de métriques et si vous ne parvenez toujours pas à afficher les données, validez :

- Le collecteur AppFlow dans l'instance NetScaler version 13.0 **antérieure à la version 47.x**.
- Le profil d'analyse dans la version de l'instance NetScaler **47.x ou ultérieure**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instance NetScaler® versions antérieures

Dans NetScaler :

1. Exécutez la commande suivante pour vous assurer que le collecteur est **ACTIF** et fonctionne sur le port 5563 :

   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```

2. Si aucun collecteur n'est disponible, effectuez un sondage manuel de l'instance dans NetScaler Console.

   a. Accédez à **Infrastructure > Fonction réseau > Interroger maintenant**

   b. Sélectionnez l'instance et cliquez sur **Démarrer l'interrogation**.

   Si l'interrogation échoue, supprimez l'instance NetScaler de NetScaler Console, puis ajoutez-la à nouveau. Lorsque vous ajoutez l'instance NetScaler, le collecteur est ajouté sur NetScaler.

Si le collecteur indique l'état **Hors service** :

1. Assurez-vous que le SNIP est configuré.

   Si le SNIP n'est pas configuré, vous devez le configurer. Pour plus d'informations, consultez Configuration du SNIP.

2. Assurez-vous que l'instance NetScaler est accessible depuis NetScaler Console.

   Vous pouvez valider en effectuant un test ping. Exécutez `ping -S <SNIP> <adm_receiver_ip>`

Versions ultérieures de l'instance NetScaler

Dans NetScaler Console, assurez-vous que le service de collecte de métriques est disponible :

1. Accédez à **Infrastructure > Fonction réseau > Équilibrage de charge > Services**.
2. Dans la barre de recherche, filtrez par **Instance : (adresse IP)** et **Nom : NetScaler Console**.
3. Vérifiez si `adm_metric_collector_svc_<adm_receiver ip>` est disponible. L'adresse IP peut être soit l'IP de gestion de NetScaler Console, soit l'IP de l'agent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assurez-vous que ce service est en état **UP** et qu'il s'exécute sur le port 5563.



Si vous ne parvenez toujours pas à afficher les données, assurez-vous que le service de collecte est lié au profil d'analyse de séries chronologiques dans NetScaler.

1. Connectez-vous à NetScaler
2. Exécutez la commande suivante :

   ```
   sh analytics profile ns_analytics_time_series_profile
   ```

   

Si le collecteur indique l'état **Down** :

1. Vérifiez si le SNIP est configuré.

   

   Si le SNIP n'est pas configuré, vous devez configurer le SNIP. Pour plus d'informations, consultez Configuration du SNIP.
2. Assurez-vous que l'instance NetScaler est accessible depuis NetScaler Console.

   Vous pouvez valider en effectuant un test ping. Exécutez `ping -S <SNIP> <adm_receiver_ip>`

   
3. Assurez-vous que la connectivité du trafic via telnet peut se connecter au service.

   

   Si telnet est capable de se connecter au service, alors un pare-feu existe et bloque le flux de données métriques. Vous devez résoudre le problème de blocage du pare-feu.

Si aucun service de collecteur n'est lié au profil d'analyse de séries chronologiques dans NetScaler, le collecteur s'affiche comme vide.



Vous devez effectuer un sondage manuel d'instance dans NetScaler Console.

1. Accédez à **Infrastructure > Fonction réseau > Interroger maintenant**
2. Sélectionnez l'instance et cliquez sur **Démarrer le sondage**.

   

   Si le sondage échoue, ajoutez le service de collecteur directement sur l'instance NetScaler à l'aide des commandes suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled
```

Le profil d'analyse de séries chronologiques est mis à jour.

Si le problème persiste même après avoir effectué toutes les étapes de dépannage mentionnées, contactez le **support NetScaler**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utilisation et anomalies des applications

En tant qu'administrateur, vous devez vous assurer de la manière dont l'application est utilisée. Les métriques clés de l'application peuvent vous aider à identifier son utilisation. Étant donné que la plage de trafic vers l'application est imprévisible, des écarts de performance inhabituels peuvent survenir pendant une durée spécifique. Dans de tels scénarios, en tant qu'administrateur, vous pourriez vouloir visualiser et analyser ces anomalies soudaines, et vous assurer si un dépannage immédiat est nécessaire.

NetScaler Console détecte ces anomalies et fournit les détails nécessaires. Accédez à **Applications > Tableau de bord**, cliquez sur une application et sélectionnez l'onglet **Métriques clés**. NetScaler Console surveille le modèle de trafic et analyse si les métriques clés se situent dans la plage attendue. S'il y a un écart par rapport à la plage attendue, NetScaler Console signale ces écarts comme des anomalies.

Vous pouvez afficher les anomalies pour les métriques clés suivantes :

- Temps de réponse
- Débit
- Volume de données
- Requêtes par seconde



Cliquez sur l'onglet **Métriques avec anomalies** pour afficher les détails.



Dans chaque métrique, vous pouvez également cliquer sur l'option **Voir plus** pour afficher les détails. L'exemple suivant concerne le volume de données de l'application :



Vous pouvez afficher :

- Le graphique indiquant la valeur maximale, la valeur totale, la plage attendue et les anomalies
- Les **Actions recommandées** pour résoudre le problème
- L'heure et les détails de l'anomalie sous **Détails**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyse de l'utilisation de pointe et creuse

Une application web peut recevoir un trafic élevé ou un trafic faible, et la plage de trafic pour chaque jour ou heure est certainement imprévisible. De même, une application web nécessite également une période d'indisponibilité pendant une durée spécifique lors d'une maintenance planifiée ou d'une mise à niveau. En tant qu'administrateur, vous devez analyser le trafic et trouver le bon moment pour :

- Mettre à l'échelle l'application web
- Planifier une période d'indisponibilité de l'application web

La fonctionnalité d'analyse des périodes de pointe et creuses de NetScaler Console vous permet d'analyser les métriques clés pour une durée sélectionnée. À partir de ces métriques, vous pouvez analyser le trafic et prendre la décision de quand vous souhaitez mettre à l'échelle l'application web ou planifier une période d'indisponibilité.

Évaluer les limites de mise à l'échelle de l'application

Cliquez sur une application depuis le **Tableau de bord des applications** et sélectionnez l'onglet **Métriques clés** pour visualiser la vue consolidée de toutes les métriques. Sélectionnez la durée dans la liste pour analyser les métriques.



Pour chaque métrique, vous pouvez afficher :

- **Max** – Indique la valeur maximale pour la durée sélectionnée
- **Moyenne** – Indique la valeur moyenne pour la durée sélectionnée

Selon l'exemple de l'image, la valeur maximale du temps de réponse indique 1,3 s. À partir du graphique, vous pouvez analyser le nombre de fois où un temps de réponse élevé s'est produit pour la durée sélectionnée. De même, vous pouvez également afficher les détails d'autres métriques, analyser si l'application a connu une utilisation de pointe et prendre la décision de mettre à l'échelle l'environnement de production.

Identifier les 5 principales fenêtres de maintenance d'application

Cliquez sur une application depuis le **Tableau de bord des applications** et sélectionnez l'onglet **Métriques clés** pour afficher la période creuse de l'application. Une période d'indisponibilité typique pour une application peut être d'1 heure, 2 heures ou 4 heures, selon les besoins. Vous pouvez sélectionner la durée dans la liste (1 heure, 2 heures ou 4 heures) que vous souhaitez planifier pour la période d'indisponibilité. Après avoir sélectionné la durée dans la liste, vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pouvez analyser le trafic pour des métriques telles que les requêtes totales, le débit et le volume de données. Vous pouvez choisir le bon moment pour planifier une période d'indisponibilité, lorsque l'utilisation de l'application est faible. L'exemple suivant analyse la période d'indisponibilité pour une durée d'1 heure.



La vue de la carte thermique indique l'utilisation de l'application pour la durée sélectionnée. Plus la couleur (bleue) est foncée, plus l'utilisation de l'application est élevée.

La vue de la carte thermique suggère également les 5 périodes les moins sollicitées (1, 2, 3, 4 et 5) pour planifier le temps d'arrêt de l'application.

1 – Indique la première suggestion pour le mercredi de 16h à 17h

2 – Indique la deuxième suggestion pour le jeudi de 21h à 22h

3 – Indique la troisième suggestion pour le dimanche de 7h à 20h

4 – Indique la quatrième suggestion pour le mercredi de 12h à 13h

5 – Indique la cinquième suggestion pour le lundi de 7h à 20h

Vous pouvez également sélectionner tout autre jour et heure pour planifier un temps d'arrêt, après avoir analysé le trafic pour tous les autres jours.

Cliquez sur **Voir les détails** pour afficher des informations plus détaillées. Cliquez sur l'onglet **Total des requêtes**, **Débit** ou **Volume de données** pour afficher les détails des 5 périodes les moins sollicitées et également pour les autres jours.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyse de l'utilisation des applications

Les propriétaires d'applications doivent avoir la capacité d'évaluer et de visualiser l'application complète du point de vue des performances et de l'utilisation.

Le **Tableau de bord des applications** amélioré vous permet de visualiser toutes les performances des applications et les métriques d'utilisation ensemble. Lorsque vous cliquez sur une application, en plus des métriques de performance d'application existantes, l'onglet **Web Insight** affiche les détails des métriques qui vous aident à :

- Comprendre l'utilisation de votre application.
- Corréler les écarts de performance avec les métriques d'utilisation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES

- À partir de la version 14.1 build 51.x, les analyses Web Insight sont visibles pour les serveurs virtuels configurés avec une adresse IPv6.
- À partir de la version **14.1-4.x**, lorsque vous explorez une métrique, la vue analytique dans le graphique de séries chronologiques affiche des valeurs nulles (par exemple, 0 ms et 0 requête) pour la durée sélectionnée. Auparavant, s'il n'y avait pas de trafic ou de transaction reçu pour la durée sélectionnée, la vue analytique affichait les graphiques en ignorant ces valeurs nulles.
- Pour chaque métrique, vous pouvez afficher des options qui indiquent la valeur maximale et la valeur totale. Par exemple :
  - - La latence maximale du réseau client pour la durée sélectionnée. Considérez que vous avez une latence réseau pour le client 1 = 644 ms, le client 2 = 15 ms et le client 3 = 3 ms. Dans ce scénario, la **Latence réseau client** affiche 644 ms.
  - - La bande passante totale consommée par tous les clients/serveurs disponibles pour la durée sélectionnée. Considérez que vous avez une consommation de bande passante pour le client 1 = 79,54 Mo, le client 2 = 45 Mo, le client 3 = 40 Mo. Dans ce scénario, la Bande passante affiche (79,54 Mo + 45 Mo + 40 Mo) = 164,54 Mo.

Voici les métriques Web Insight que vous pouvez afficher depuis l'onglet **Utilisation** :

- **Clients** – Affiche les informations pour les clients accédant à l'application :
  - **Clients totaux** – Affiche le nombre total de clients accédant à l'application. Cliquez sur l'onglet **Requêtes** pour afficher :
    - **Client** – L'adresse IP du client.
    - **Latence réseau client (moy)** – La latence réseau moyenne du client.
    - **Latence réseau client (max)** – La latence réseau maximale du client.
    - **Requêtes** – Le nombre total de requêtes du client.
    - **Distribution en pourcentage par requêtes** – La distribution en pourcentage basée sur les requêtes. Par exemple, si le nombre total de clients est de 4 et que chaque client a 100 requêtes, la distribution en pourcentage pour chaque client est de 25 %.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Latence réseau client** – Affiche la latence réseau du client vers NetScaler. Cliquez sur l'onglet **Latence réseau client** pour afficher :
  - **Client** – L'adresse IP du client.
  - **Latence réseau client (moy)** – La latence réseau moyenne du client.
  - **Latence réseau client (max)** – La latence réseau maximale du client.
  - **Requêtes** – Le nombre total de requêtes du client.
  - **Distribution en pourcentage par requêtes** – La distribution en pourcentage basée sur les requêtes.
- **Temps de rendu** – Affiche le temps nécessaire pour rendre la réponse du serveur. Cliquez sur l'onglet **Temps de rendu** pour afficher :
  - **Client** – L'adresse IP du client.
  - **Temps de rendu (moy)** – Le temps de rendu moyen du client.
  - **Requêtes** – Le nombre total de requêtes du client.
  - **Distribution en pourcentage par requêtes** – La distribution en pourcentage basée sur les requêtes.

- **Serveurs** – Affiche les informations pour les serveurs accédant à l'application :

  REMARQUE

  Pour les requêtes de cache intégré, vous pouvez afficher l'adresse IP du serveur virtuel NetScaler avec une notification IC. Pour plus d'informations, consultez Requêtes de cache intégré.

  - **Serveurs totaux** – Affiche le nombre total de serveurs accédant à l'application. Cliquez sur l'onglet **Requêtes** pour afficher :
    - **Serveur** – L'adresse IP du serveur.
    - **Latence réseau du serveur (moy)** – La latence réseau moyenne du serveur.
    - **Latence réseau du serveur (max)** – La latence réseau maximale du serveur.
    - **Requêtes** – Le nombre total de requêtes provenant du serveur.
    - **Distribution en pourcentage par requêtes** – La distribution en pourcentage basée sur les requêtes. Par exemple, si le nombre total de serveurs est de 10 et que chaque

© 1997–2026 Citrix Systems, Inc. All rights reserved.

serveur a 1000 requêtes, la distribution en pourcentage pour chaque serveur est de 10 %.

- **Latence réseau du serveur (max)** – Affiche la latence réseau maximale du serveur vers NetScaler. Cliquez sur l'onglet **Latence réseau du serveur** pour afficher :
  - **Serveur** – L'adresse IP du serveur.
  - **Latence réseau du serveur (moy)** – La latence réseau moyenne du serveur.
  - **Latence réseau du serveur (max)** – La latence réseau maximale du serveur.
  - **Requêtes** – Le nombre total de requêtes provenant du serveur.
  - **Distribution en pourcentage par requêtes** – La distribution en pourcentage basée sur le nombre total de requêtes.
- **Temps de réponse du serveur** – Affiche le temps mis par le serveur pour répondre aux requêtes. Cliquez sur l'onglet **Temps de réponse du serveur** pour afficher :
  - **Serveur** – L'adresse IP du serveur.
  - **Temps de réponse du serveur (moy)** – Le temps de réponse moyen du serveur.
  - **Temps de réponse du serveur (max)** – Le temps de réponse maximal du serveur.
  - **Requêtes** – Le nombre total de requêtes du serveur.
  - **Répartition en pourcentage par requêtes** – La répartition en pourcentage basée sur le nombre total de requêtes.
- **Bande passante** – Affiche la bande passante totale consommée par les serveurs. Cliquez sur l'onglet **Bande passante** pour afficher :
  - **Serveur** – L'adresse IP du serveur.
  - **Bande passante** – La bande passante totale consommée par le serveur.
  - **Requêtes** – Le nombre total de requêtes du serveur.
  - **Répartition en pourcentage par requêtes** – La répartition en pourcentage basée sur le nombre total de requêtes.

- **Emplacements géographiques** – Affiche les informations pour les clients accédant à l'application depuis un emplacement particulier :

  - **Nombre total d'emplacements** – Affiche le nombre total d'emplacements clients accédant à l'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Temps de réponse** – Affiche le temps de réponse depuis l'emplacement du client.
- **Bande passante** – Affiche la bande passante totale consommée par les clients sur tous les emplacements.
- **Requêtes** – Affiche le nombre total de requêtes provenant de tous les emplacements clients.

  Cliquez sur chaque onglet pour afficher :

  - **Emplacement** – Le nom de l'emplacement.
  - **Temps de réponse** – Le temps de réponse moyen depuis l'emplacement client.
  - **Bande passante** – La bande passante consommée depuis l'emplacement client.
  - **Requêtes** – Le nombre total de requêtes provenant de l'emplacement client.
  - **Répartition en pourcentage par requêtes** – La répartition en pourcentage basée sur le nombre total de requêtes. Par exemple, si le nombre total d'emplacements est de 10, le nombre total de requêtes est de 1 million, et que le pays A reçoit à lui seul 0,9 million, alors la répartition en pourcentage pour le pays A est de 90 %. Les autres pays reçoivent la répartition en pourcentage restante en fonction des requêtes reçues dans chaque pays.

- **URL** – Affiche les informations pour les URL avec un temps de chargement et de rendu élevé :

  - **Nombre total d'URL** – Affiche le nombre total d'URL. Cliquez sur l'onglet **Requêtes** pour afficher :
    - **URL** – Le nom de l'URL.
    - **Temps de chargement (moy.)** – Le temps moyen nécessaire au chargement de l'URL.
    - **Requêtes** – Le nombre total de requêtes provenant de l'URL.
    - **Répartition en pourcentage par requêtes** – La répartition en pourcentage basée sur le nombre total de requêtes et dans chaque URL.
  - **Temps de chargement** – Affiche le temps nécessaire au chargement de l'URL. Cliquez sur l'onglet **Temps de chargement** pour afficher :
    - **URL** – Le nom de l'URL.
    - **Temps de chargement (moy.)** – Le temps moyen nécessaire au chargement de l'URL.
    - **Requêtes** – Le nombre total de requêtes provenant de l'URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

        - **Répartition en pourcentage par requêtes** – La répartition en pourcentage basée sur le nombre total de requêtes.

    - **Temps de rendu** – Affiche le temps nécessaire à l'URL pour être rendue et affichée. Cliquez sur l'onglet **Temps de rendu** pour afficher :

        - **URL** – Le nom de l'URL.
        - **Temps de rendu (moy.)** – Le temps moyen nécessaire à l'URL pour être rendue.
        - **Requêtes** – Le nombre total de requêtes provenant de l'URL.
        - **Répartition en pourcentage par requêtes** – La répartition en pourcentage basée sur le nombre total de requêtes.

- **Statut de la réponse HTTP** – Affiche les informations pour une requête HTTP spécifique terminée.

    

    - **Statut de la réponse** – Affiche le code de réponse tel que 2xx, 4xx, 5xx, etc.
    - **Raison du statut de la réponse** – Affiche la raison de la réponse, telle qu'une erreur de serveur interne, introuvable, etc.
    - **Nombre d'occurrences** – Affiche le nombre total d'occurrences.

- **Système d'exploitation** – Affiche les informations sur le système d'exploitation accédant à l'application.

    

    - **Requêtes** – Affiche le nombre total de requêtes provenant de chaque système d'exploitation.
    - **Bande passante** – Affiche la bande passante totale consommée par chaque système d'exploitation.
    - **Temps de chargement** – Affiche le temps total nécessaire à chaque système d'exploitation pour charger depuis le serveur.

- **Navigateurs** – Affiche les informations sur les types de navigateurs utilisés par les clients pour accéder à l'application.

    

    - **Requêtes** – Affiche le nombre total de requêtes provenant de chaque navigateur.
    - **Bande passante** – Affiche la bande passante totale consommée par chaque navigateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Temps de chargement** – Affiche le temps total nécessaire à un navigateur pour charger depuis le serveur.

- **Erreurs SSL** – Affiche les informations sur les erreurs SSL provenant du serveur frontal et du serveur principal.

  

  - **Erreurs totales** – Affiche le nombre total d'occurrences d'erreurs SSL.
  - **Serveur frontal** – Affiche le nombre total d'erreurs SSL provenant du serveur frontal. Cliquez sur l'onglet **Serveur frontal** pour afficher le type d'erreur SSL et le nombre total d'occurrences.
  - **Serveur principal** – Affiche le nombre total d'erreurs SSL provenant du serveur principal. Cliquez sur l'onglet **Serveur principal** pour afficher le type d'erreur SSL et le nombre total d'occurrences.

- **Utilisation SSL** – Affiche les informations sur l'utilisation SSL telles que les certificats SSL, les protocoles, les chiffrements et la force de la clé.

  

  - **Certificats** – Affiche le nombre total de certificats SSL. Cliquez sur l'onglet **Certificats** pour afficher le nom du certificat et le nombre total d'accès.
  - **Protocoles** – Affiche le nombre total de protocoles SSL. Cliquez sur l'onglet **Protocoles** pour afficher les détails du protocole SSL/TSL et le nombre total d'accès.
  - **Chiffrements** – Affiche le nombre total de chiffrements. Cliquez sur l'onglet **Chiffrements** pour afficher les détails de chaque nom de suite de chiffrement et le nombre total d'accès.
  - **Force de la clé** – Affiche la force totale de la clé utilisée dans les certificats SSL. Cliquez sur l'onglet **Force de la clé** pour afficher les détails de chaque force de clé et le nombre total d'accès.

Afficher les détails des métriques au format graphique

Pour chaque métrique, vous pouvez afficher plus de détails au format graphique en cliquant sur l'option **Voir plus**. Cliquez sur **>** pour afficher les détails au format graphique.



Voici les détails que vous pouvez afficher pour chaque métrique après avoir cliqué sur l'option **Voir plus** :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE L'APERÇU	MÉTRIQUES	DESCRIPTION
Clients	Clients	Indique la liste des clients
	Temps de rendu (AVG)	Indique le temps moyen nécessaire au client pour rendre la réponse du serveur
	Latence réseau client (AVG)	Indique la latence réseau moyenne du client vers l'instance NetScaler
	Requêtes	Indique le nombre total de requêtes du client
Serveurs	Serveur	Indique la liste des serveurs
	Temps de traitement du serveur (AVG)	Indique le temps moyen nécessaire au serveur pour traiter les requêtes
	Latence réseau du serveur (AVG)	Indique la latence réseau moyenne du serveur vers l'instance NetScaler
	Accès	Indique le nombre total de requêtes reçues par le serveur
Localisations géographiques	Emplacements	Indique les emplacements des clients
	Temps de réponse	Indique le temps de réponse total depuis l'emplacement du client
	Bande passante	Indique la bande passante totale consommée depuis l'emplacement
	Requêtes	Indique le nombre total de requêtes depuis l'emplacement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE L'APERÇU	MÉTRIQUES	DESCRIPTION
URL	Temps de rendu (moy.)	Indique le temps moyen nécessaire pour charger la page depuis le serveur
	Temps de chargement (moy.)	Indique le temps moyen nécessaire pour que l'URL soit rendue et affichée
	Accès	Indique le nombre total d'accès depuis l'URL
État de la réponse HTTP	Nom	Indique le nom de l'état de la réponse, tel que OK, Introuvable, Erreur interne du serveur, etc.
	État de la réponse	Indique le code d'état de la réponse reçu du serveur, tel que 200, 400, 500, etc.
	Accès	Indique le nombre total d'accès depuis le code de réponse
	Bande passante	Indique la bande passante totale consommée
Système d'exploitation	Système d'exploitation	Indique le nom du système d'exploitation, tel que Windows, MAC
	Temps de chargement	Indique le temps total nécessaire au système d'exploitation pour se charger depuis le serveur
	Bande passante	Indique la bande passante totale consommée par le système d'exploitation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE L'APERÇU	MÉTRIQUES	DESCRIPTION
	Requêtes	Indique le nombre total de requêtes provenant du système d'exploitation
Navigateurs	Navigateurs	Indique le nom du navigateur, tel que Mozilla Firefox, Chrome, etc.
	Temps de chargement	Indique le temps total nécessaire à un navigateur pour se charger depuis le serveur
	Bande passante	Indique la bande passante totale consommée par le navigateur
	Requêtes	Indique le nombre total de requêtes provenant du navigateur
Erreurs SSL	Type d'échec SSL	Indique le nom de l'erreur, tel que CLIENTAUTH FAILURE
	Occurrences	Indique le nombre total d'occurrences pour l'erreur SSL
Utilisation SSL	Utilisation SSL	Indique le nom et les versions du protocole, tels que TLS, SSL
	Requêtes	Indique le nombre total de requêtes provenant du protocole

Dépanner les problèmes de Web Insight

Pour plus de détails, consultez le document de dépannage Dépanner les problèmes de Web Insight

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyse de la notation SSL A+

REMARQUE :

Pour la mise à niveau en bloc des certificats SSL non conformes, vous pouvez utiliser la fonction **Mise à niveau de la notation SSL A+** dans **Tâches**.

Une application doit utiliser des chiffrements et des protocoles sécurisés pour les transactions SSL. Dans le cas contraire, cela peut avoir un impact sur la confidentialité, l'intégrité des données et la sécurité des utilisateurs accédant à l'application. NetScaler Console examine les paramètres SSL du serveur virtuel de l'application avec le profil frontal sécurisé NetScaler. Les paramètres requis pour une notation A+ sont préchargés dans le profil frontal sécurisé.

En tant que propriétaire d'application, vous pouvez évaluer si votre application a une notation **A+**. Vous pouvez également afficher les scores de protocole et de suite de chiffrement d'une application. Si votre application n'a pas de notation **A+**, vous pouvez passer à la notation **A+**.

Pour afficher la notation SSL de l'application, procédez comme suit :

1. Accédez à **Applications > Tableau de bord**.
2. Filtrez les applications en fonction de leurs notations SSL.

   Si une application n'a pas de notation, elle est classée sous **NA**.
3. Sélectionnez la grille d'application requise dans l'interface graphique.
4. Sélectionnez l'onglet **SSL**. Cet onglet affiche la notation SSL de l'application.

L'onglet **SSL** propose l'une des options suivantes pour modifier ou mettre à niveau la notation de votre application :

- Mettre à niveau vers la notation SSL A+
- Rétablir la note SSL(#roll-back-ssl-rating)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mettre à niveau vers la note SSL A+

Lorsque vous mettez à niveau une application vers la note SSL A+, les modifications suivantes se produisent en fonction de l'état d'un profil SSL par défaut sur une instance NetScaler :

- Si le profil SSL par défaut est désactivé, NetScaler Console modifie les paramètres SSL recommandés sur le serveur virtuel SSL.
- Si le profil SSL par défaut est activé, NetScaler Console crée un nouveau profil SSL avec les paramètres A+ recommandés basés sur un profil sécurisé.

L'application sans note **A+** affiche les détails des serveurs virtuels affectés dans l'onglet **SSL**.



Dans **Détails de l'application**, vous pouvez consulter les détails du serveur virtuel dont la configuration n'est pas conforme au profil frontal sécurisé. De plus, il affiche les mesures de correction dans la colonne **Recommandation**. Ces mesures sont données pour rendre votre application conforme au profil frontal sécurisé.

Dans cet exemple, le serveur virtuel présente quelques problèmes de sécurité. **Protocole TLSv1.0 activé** est l'un de ces problèmes. La section **Détails de l'application** recommande une action appropriée pour résoudre ce problème. Pour résoudre tous ces problèmes avec les recommandations respectives, procédez comme suit :

1. Cliquez sur **Mettre à niveau vers la note A+**.

   

   Le message de confirmation affiche les commandes qui s'exécutent sur un serveur virtuel. Ces commandes peuvent affecter le trafic de votre application.
2. Passez en revue les commandes et cliquez sur **Confirmer**.

Rétablir la note SSL

REMARQUE :

Si vous mettez à niveau une application vers une évaluation SSL A+, vous ne pouvez revenir à son évaluation d'origine que dans les 7 jours suivant la mise à niveau.

Après avoir mis à niveau l'application vers l'évaluation A+, vous pouvez analyser le trafic entrant dans SSL insight. Cette page affiche les chiffrements et les protocoles sur lesquels les transactions SSL sont négociées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cependant, si vous constatez que du trafic légitime est abandonné, vous pouvez annuler le profil frontal sécurisé configuré sur votre application. Cette action ramène l'évaluation SSL à l'évaluation précédente.

Pour annuler une évaluation SSL :

1. Cliquez sur **Annuler**.

   Le message de confirmation affiche les commandes qui s'exécutent sur un serveur virtuel.
2. Passez en revue les commandes et cliquez sur **Confirmer**.

Déterminer l'impact de l'évaluation SSL sur le trafic de l'application

Le trafic de l'application peut être affecté lorsque vous mettez à niveau l'évaluation SSL. Dans **SSL Metrics**, vous pouvez observer si des connexions sont abandonnées après la mise à niveau. Grâce à ces informations, vous pouvez décider de poursuivre ou d'annuler l'évaluation SSL.

Dans le graphique d'exemple suivant, certaines connexions sont abandonnées après la mise à niveau de l'évaluation SSL vers **A+**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau de bord Web Insight

REMARQUE :

À partir de la version 14.1 build 51.x, les analyses Web Insight sont visibles pour les serveurs virtuels configurés avec une adresse IPv6.

La fonctionnalité Web Insight améliorée est enrichie et offre une visibilité sur des métriques détaillées pour les applications web, les clients et les instances NetScaler. Cette version améliorée de Web Insight vous permet d'évaluer et de visualiser l'application complète sous les angles de la performance et de l'utilisation. En tant qu'administrateur, vous pouvez afficher Web Insight pour :

- Une application. Accédez à **Applications > Tableau de bord**, cliquez sur une application et sélectionnez l'onglet **Web Insight** pour afficher les métriques détaillées. Pour plus d'informations, consultez Analyse de l'utilisation des applications.
- Toutes les applications. Accédez à **Applications > Web Insight** et cliquez sur chaque onglet (Applications, Clients, Instances) pour afficher les métriques suivantes :

APPLICATIONS	CLIENTS	INSTANCES
Applications	Clients	Métriques d'instance
Serveurs	Localisations géographiques	Applications
Domaines	Méthodes de requête HTTP	Domaines
Localisations géographiques	Statut de réponse HTTP	URL
URL	URL	Méthodes de requête HTTP
Méthodes de requête HTTP	Système d'exploitation	Statut de réponse HTTP
Statut de réponse HTTP	Navigateurs	Clients
Erreurs SSL	Erreurs SSL	Serveurs
Utilisation SSL	Utilisation SSL	Système d'exploitation

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APPLICATIONS	CLIENTS	INSTANCES
		Navigateurs

Pour chaque métrique, vous pouvez afficher les 5 meilleurs résultats. Vous pouvez cliquer pour explorer davantage afin d'analyser le problème et d'agir plus rapidement pour le dépanner.

REMARQUE :

- À partir de la version **14.1-4.x**, lorsque vous explorez une métrique, la vue analytique du graphique de séries chronologiques affiche des valeurs nulles (par exemple, 0 ms et 0 requête) pour la durée sélectionnée. Auparavant, s'il n'y avait pas de trafic ou de transaction reçu pour la durée sélectionnée, la vue analytique affichait les graphiques en ignorant ces valeurs nulles.
- Dans certains scénarios, NetScaler peut ne pas être en mesure de calculer les valeurs RTT pour certaines transactions. Pour ces transactions, NetScaler Console affiche les valeurs RTT comme suit :
  - **NA** – S'affiche lorsque l'instance NetScaler ne peut pas calculer le RTT.
  - **< 1ms** – S'affiche lorsque l'instance NetScaler calcule le RTT en décimales entre 0 ms et 1 ms. Par exemple, 0,22 ms.

Par exemple, supposons que vous souhaitiez analyser la latence du réseau du serveur pendant une durée d'un mois et décider s'il faut augmenter ou réduire l'environnement de production. Pour analyser cela :

1. Sélectionnez Dernier 1 mois dans la liste et, depuis l'onglet **Applications**, faites défiler jusqu'à **Serveurs**, puis cliquez sur un serveur.

   Les détails des métriques pour le serveur sélectionné sont affichés.
2. Sélectionnez l'onglet **Latence du réseau du serveur** pour analyser la latence.

   Latence du réseau du serveur(/en-us/netscaler-application-delivery-management-software/media/app-wi-serverlatency.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La latence moyenne indique 10,01 s et, d'après le graphique, vous pouvez analyser que la latence du réseau du serveur pour le dernier mois semble être élevée. En tant qu'administrateur, vous pouvez prendre la décision de faire évoluer l'environnement de production.

Requêtes de cache intégré

Le cache intégré fournit un stockage en mémoire sur l'appliance NetScaler et sert le contenu Web aux utilisateurs sans nécessiter d'aller-retour vers un serveur d'origine.

Les requêtes de cache d'intégration sont actuellement visibles sous **Serveurs** avec une notification IC à côté de l'adresse IP du serveur virtuel NetScaler. Toutes les autres requêtes sont visibles avec l'adresse IP du serveur d'origine.

Cache intégré(/en-us/netscaler-application-delivery-management-software/media/web-insight-integrated-cache.png)

Lorsque vous explorez un serveur pour afficher plus de détails, les **Métriques du serveur** affichent les onglets des accès et des échecs du cache intégré.

La vue graphique dans :

- L'onglet **Accès au cache intégré** vous permet d'afficher le nombre total de réponses que l'appliance NetScaler sert à partir du cache.

  Accès au cache intégré(/en-us/netscaler-application-delivery-management-software/media/web-insight-server-integrated-cache.png)
- L'onglet **Échecs du cache intégré** vous permet d'afficher le nombre total de réponses que l'appliance NetScaler sert à partir du serveur d'origine.

  Échecs du cache intégré(/en-us/netscaler-application-delivery-management-software/media/web-insight-server-integrated-miss.png)

Dépanner les problèmes de Web Insight

Pour plus de détails, consultez le document de dépannage Résoudre les problèmes de Web Insight.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher la cause première de la latence des applications

La lenteur des applications est une préoccupation majeure pour toute organisation, car elle a un impact sur l'activité ou la productivité. Dans **Applications > Web Insight**, vous pouvez désormais afficher une nouvelle métrique appelée **Applications avec anomalies de temps de réponse**. À l'aide de cette métrique, en tant qu'administrateur, vous pouvez analyser si la latence de l'application provient des causes suivantes :

- Latence du réseau client
- Latence du réseau serveur
- Temps de traitement du serveur

NetScaler Console effectue des vérifications d'anomalies toutes les heures et signale les anomalies pour le trafic de la dernière heure, sur la base de certains prérequis. Par exemple, pour éviter les faux positifs, si le temps de réponse est < 1 ms, les vérifications d'anomalies pour ces résultats sont ignorées.

La page **Applications > Web Insight** vous permet d'afficher les applications présentant des anomalies de temps de réponse pour la durée sélectionnée. La métrique **Applications avec anomalies de temps de réponse** affiche les cinq principales applications en fonction du nombre total d'anomalies. Cliquez sur **Voir plus** pour afficher toutes les applications.



- **Application** – Indique le nom de l'application.
- **Anomalies totales et contributeurs** – Indique le nombre total d'anomalies de l'application. Lorsque vous passez le pointeur de la souris, vous pouvez afficher le nombre total d'anomalies provenant respectivement de la latence du réseau client, de la latence du réseau serveur et du temps de traitement du serveur.
- **Plage de temps de réponse** – Indique la plage de temps de réponse attendue de l'application.
- **Temps de réponse anormal maximal** – Indique le temps de réponse le plus élevé de l'application.
- **Principal contributeur d'anomalies** – Indique si le nombre maximal d'anomalies pour l'application provient de la latence du réseau client, de la latence du réseau serveur ou du temps de traitement du serveur.

Exploration des applications

Cliquez sur une application pour afficher les détails des **métriques d'application** pour la durée sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Les **métriques d'application** vous permettent d'afficher :

- **Résumé** – Un aperçu pour visualiser les performances de l'application telles que le temps de réponse, les requêtes et la bande passante.
- **Requêtes** – Le nombre total de requêtes reçues par l'application. Vous pouvez également afficher les requêtes des 5 principaux clients en fonction du nombre total de requêtes.
- **Bande passante** – La bande passante totale traitée par l'application. Vous pouvez également afficher la consommation de bande passante des 5 principaux serveurs en fonction de la consommation totale de bande passante.
- **Temps de réponse** – Un aperçu pour visualiser la latence du réseau client, la latence du réseau serveur et le temps de traitement du serveur sur le même graphique.
- **Latence du réseau client** – La latence moyenne du réseau client (du client à NetScaler).
- **Latence du réseau serveur** – La latence moyenne du réseau serveur (de NetScaler au serveur).
- **Temps de traitement du serveur** – Le temps de traitement moyen du serveur (du serveur à NetScaler).

Si l'application présente des anomalies, vous pouvez vérifier si celles-ci proviennent de la latence du réseau client, de la latence du réseau serveur ou du temps de traitement du serveur. Cliquez sur chaque onglet pour afficher les détails.

Dans les onglets **Latence du réseau client** et **Latence du réseau serveur**, vous pouvez afficher :

- **Une barre de recherche** - Cliquez sur la barre de recherche pour afficher l'adresse IP de tous les clients (dans Latence du réseau client) et serveurs (dans Latence du réseau serveur). Vous pouvez sélectionner l'adresse IP pour filtrer les résultats.
- **Une option d'exportation** - Cliquez sur **Télécharger CSV** pour exporter les détails au format CSV.



Temps de réponse

Sous **Détails de l'anomalie**, cliquez pour afficher les détails des contributeurs au temps de réponse (du client au serveur). L'exemple suivant présente une anomalie pour la latence du réseau client, la latence du réseau serveur et le temps de traitement du serveur. Vous pouvez également afficher les plages attendues et le dépassement qui s'est produit au-delà de la plage attendue.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les **Actions recommandées** vous suggèrent les résolutions possibles pour les anomalies.



De même, vous pouvez cliquer sur les onglets **Latence du réseau client**, **Latence du réseau serveur** et **Temps de traitement du serveur** pour afficher :

- Anomalie qui a dépassé la plage attendue.
- Actions recommandées qui vous suggèrent les résolutions possibles.

Si l'application fonctionne correctement, vous pouvez afficher les métriques de l'application sans anomalie.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Graphe de services

La fonctionnalité de graphe de services dans NetScaler Console vous permet de surveiller tous les services sous forme de représentation graphique. Cette fonctionnalité vous permet également d'afficher une analyse détaillée et des métriques exploitables des services. Vous pouvez afficher le graphe de services pour :

- Applications configurées sur toutes les instances NetScaler
- Applications Kubernetes
- Applications Web à 3 niveaux

Graphe de services pour les applications sur toutes les instances NetScaler

La fonctionnalité de graphe de services global vous permet d'obtenir une visualisation holistique de la vue `clients to infrastructure to application`. À partir de cette vue de graphe de services à volet unique, en tant qu'administrateur, vous pouvez :

- Comprendre depuis quelle région les utilisateurs accèdent aux applications spécifiques (applications Web à 3 niveaux et applications de microservices)
- Visualiser la vue de l'infrastructure (instance NetScaler) où la requête client est traitée
- Comprendre si les problèmes proviennent du client, de l'infrastructure ou de l'application
- Approfondir l'analyse pour résoudre le problème

Accédez à **Applications > Graphe de services** et cliquez sur l'onglet **Global** pour afficher :

- Détails de bout en bout de toutes les applications connectées du client aux serveurs back-end
- Toutes les instances NetScaler connectées à leurs centres de données respectifs

  REMARQUE

  Vous pouvez afficher les centres de données uniquement si vous avez des applications GSLB.

- Les informations sur les métriques du client

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Les informations sur les métriques NetScaler
- Toutes les instances NetScaler qui ont des applications discrètes, des applications personnalisées et des applications de microservices discrètes
- Les 4 applications les moins bien notées qui appartiennent aux applications personnalisées, aux applications discrètes et aux applications de microservices
- Les informations sur les métriques pour les 4 serveurs virtuels les moins bien notés
- L'état des applications (applications discrètes, applications personnalisées et applications de microservices) tel que **Critique**, **À réviser**, **Bon** et **Non applicable**.

Pour plus d'informations, consultez (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/holistic-view-sg.html)Vue holistique des applications dans le graphique de service.

Graphique de service pour les applications Kubernetes

Accédez à **Applications > Graphique de service** et cliquez sur l'onglet **Microservices** pour afficher :

- Assurer la performance globale de l'application de bout en bout
- Identifier les goulots d'étranglement créés par l'interdépendance des différents composants de vos applications
- Recueillir des informations sur les dépendances des différents composants de vos applications
- Surveiller les services au sein du cluster Kubernetes
- Surveiller quel service présente des problèmes
- Vérifier les facteurs contribuant aux problèmes de performance
- Afficher la visibilité détaillée des transactions HTTP de service
- Analyser les métriques HTTP, TCP et SSL

En visualisant ces métriques dans NetScaler Console, vous pouvez analyser la cause première des problèmes et prendre les mesures de dépannage nécessaires plus rapidement. Le graphique de service affiche vos applications sous forme de divers services composants. Ces services exécutés au sein du cluster Kubernetes peuvent communiquer avec divers composants à l'intérieur et à l'extérieur de l'application. Pour commencer, consultez Configuration du graphique de service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Graphique de service pour les applications Web à 3 niveaux

Accédez à **Applications > Graphique de service** et cliquez sur l'onglet **Applications Web** pour afficher :

- Détails sur la configuration de l'application (avec serveur virtuel de commutation de contenu et serveur virtuel d'équilibrage de charge)

  Pour les applications GSLB, vous pouvez afficher le centre de données, l'instance NetScaler, les serveurs virtuels CS et LB.
- Transactions de bout en bout du client au service
- L'emplacement à partir duquel le client accède à l'application
- Le nom du centre de données où les requêtes client sont traitées et les métriques NetScaler du centre de données associées (uniquement pour les applications GSLB)
- Détails des métriques pour le client, le service et les serveurs virtuels
- Si les erreurs proviennent du client ou du service
- L'état du service tel que **Critique**, **À réviser** et **Bon**. NetScaler Console affiche l'état du service en fonction du temps de réponse du service et du nombre d'erreurs.
  - **Critique (rouge)** - Indique lorsque le temps de réponse moyen du service > 200 ms ET le nombre d'erreurs > 0
  - **À revoir (orange)** - Indique quand le temps de réponse moyen du service > 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** - Indique aucune erreur et un temps de réponse moyen du service < 200 ms
- L'état du client tel que **Critique**, **À revoir** et **Bon**. NetScaler Console affiche l'état du client en fonction de la latence du réseau client et du nombre d'erreurs.
  - **Critique (rouge)** - Indique quand la latence moyenne du réseau client > 200 ms ET le nombre d'erreurs > 0
  - **À revoir (orange)** - Indique quand la latence moyenne du réseau client > 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** - Indique aucune erreur et une latence moyenne du réseau client < 200 ms
- L'état du serveur virtuel tel que **Critique**, **À revoir** et **Bon**. NetScaler Console affiche l'état du serveur virtuel en fonction du score de l'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Critique (rouge)** - Indique quand le score de l'application < 40
- **À revoir (orange)** - Indique quand le score de l'application est entre 40 et 75
- **Bon (vert)** - Indique quand le score de l'application est > 75

Points à noter :

- Seuls les serveurs virtuels d'équilibrage de charge, de commutation de contenu et GSLB sont affichés dans le graphique de service.
- Si aucun serveur virtuel n'est lié à une application personnalisée, les détails ne sont pas visibles dans le graphique de service pour l'application.
- Vous pouvez afficher les métriques pour les clients et les services dans le graphique de service uniquement si des transactions actives se produisent entre les serveurs virtuels et l'application web.
- S'il n'y a pas de transactions actives disponibles entre les serveurs virtuels et l'application web, vous ne pouvez afficher les détails dans le graphique de service qu'en fonction des données de configuration telles que l'équilibrage de charge, la commutation de contenu, les serveurs virtuels GSLB et les services.
- Si des modifications sont apportées à la configuration de l'application, cela peut prendre 10 minutes pour qu'elles soient reflétées dans le graphique de service.

Pour plus d'informations, consultez Graphique de service pour les applications.

Graphe de services pour les applications Kubernetes

Utilisez le graphe de services pour les applications Kubernetes afin de visualiser, surveiller et dépanner les microservices de votre cluster Kubernetes. Les rubriques suivantes vous aident à configurer, afficher et analyser le graphe de services :

- Configuration du graphe de services
- Afficher les détails dans le graphe de services
- Configurer les seuils dans le graphe de services
- Afficher les détails du service
- Afficher les détails d'entrée pour le dépannage
- Traçage distribué
- Afficher les diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration du graphique de service

Exigences logicielles

DISTRIBUTION KUBERNETES	VERSION DE KUBERNETES	INTERFACES RÉSEAU DE CONTENEUR (CNI)	VERSION DE CPX	VERSION DE CIC	VERSION DE NETSCALER CONSOLE	VERSION DE L'AGENT NETSCALER
Logiciel libre	v1.16.3	Flannel, Calico ou Canal	13.0–41.28 ou version ultérieure	1.5.25 ou version ultérieure	13.0–47.22 ou version ultérieure	13.0–47.22 ou version ultérieure

Vous pouvez configurer le cluster Kubernetes avec différentes topologies de déploiement et le tableau suivant fournit les topologies prises en charge dans le graphique de services :

TOPOLOGIE	PRIS EN CHARGE DANS LE GRAPHIQUE DE SERVICES
Niveau unique ou Ingress unifié	Oui
Double niveau	Oui
Cloud	Oui, mais l'équilibreur de charge cloud n'est pas affiché dans le graphique
Maillage de services léger	Oui
Maillage de services	Oui
Services de type LoadBalancer	Non
Services de type NodePort	Non

Pour terminer la configuration du graphique de services dans NetScaler Console, cliquez sur le type de topologie que vous avez configuré pour votre cluster Kubernetes et suivez les procédures mentionnées :

- Topologie d'entrée à niveau unique ou unifiée

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Topologie à deux niveaux ou Service Mesh Lite
- Topologie de maillage de services

REMARQUE

La procédure de configuration du graphique de services pour les topologies à deux niveaux et Service Mesh Lite reste la même.

Avant de commencer

Vous pouvez afficher le graphique de services dans les scénarios suivants :

- NetScaler Console et cluster Kubernetes sur le même réseau (par exemple, NetScaler Console et cluster Kubernetes hébergés sur le même Citrix Hypervisor).
- NetScaler Console et cluster Kubernetes sur un réseau différent. Dans ce scénario, vous devez configurer un agent sur site et enregistrer l'agent sur le réseau où le cluster Kubernetes est hébergé.

Topologie d'entrée à niveau unique ou unifiée

Assurez-vous d'avoir :

- Cluster Kubernetes configuré avec une topologie d'entrée à niveau unique ou unifiée.
- Ajouté une (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-unified-single-ingress-topology.html#add-vpx-or-sdx-or-mpx-or-blx-instance-in-citrix-adm) dans NetScaler Console et activé **Web Insight**.
- Ajouté le (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-unified-single-ingress-topology.html#add-kubernetes-cluster-in-citrix-adm) dans NetScaler Console.

Topologie à deux niveaux ou Service Mesh Lite

Assurez-vous d'avoir :

- Cluster Kubernetes configuré avec l'une des topologies prises en charge.
- Configuré les (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

topology.html#configure-static-routes-in-citrix-adm-agent) sur NetScaler Console pour permettre la communication entre NetScaler Console et NetScaler CPX.

REMARQUE

Vous pouvez ignorer cette procédure si vous avez déployé NetScaler Console en tant que microservice dans le même cluster.

- Téléchargé les (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#download-the-sample-deployment-files-from-github) depuis le référentiel GitHub.
- Ajouté les (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-parameters-in-cpx-yaml-file) dans le fichier YAML CPX pour assurer l'enregistrement réussi de CPX auprès de NetScaler Console.
- Ajouté une (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-vpx-or-sdx-or-mpx-or-blx-instance-in-citrix-adm) dans NetScaler Console.
- Ajouté le (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-kubernetes-cluster-in-citrix-adm) dans NetScaler Console.
- Déployé une application de microservices exemple.
- Déployé NetScaler CPX et (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#deploy-cpx-and-register-cpx-in-adm) (applicable uniquement pour l'architecture à deux niveaux)
- Activé Auto-select Virtual Servers pour attribuer des licences aux serveurs virtuels.
- Activé Web transaction and TCP transaction settings sur **Tous** pour que l'agent NetScaler obtienne les transactions HTTP et TCP.
- Envoyé traffic aux microservices.

Topologie du maillage de services

Assurez-vous d'avoir :

- Configuré la version du cluster Kubernetes `1.14.0` avec l'une des topologies de maillage de services suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - NetScaler CPX en tant que proxy sidecar pour Istio
  - NetScaler en tant que passerelle d'entrée pour Istio

- Activé `admissionregistration.k8s.io/v1beta1` API. Vous pouvez vérifier l'API en utilisant :

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  La sortie suivante indique que l'API est activée :

  ```
  admissionregistration.k8s.io/v1beta1
  ```

- Installé Istio `istio v.1.3.0`.
- Installé Helm version 3.x.
- Configuré static routes sur NetScaler Console pour permettre la communication entre NetScaler Console et NetScaler CPX.

  REMARQUE

  Vous pouvez ignorer cette procédure si vous avez déployé l'agent NetScaler en tant que microservice dans le même cluster.

- Configuré les (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#configure-the-required-parameters) paramètres requis pour renseigner les données de topologie du maillage de services.
- Déployé une (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#deploy-a-sample-application) application d'exemple.
- Ajouté le (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#add-kubernetes-cluster-in-citrix-adm) cluster Kubernetes dans NetScaler Console.
- Activé la (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#enable-auto-select-virtual-servers-for-licensing) Sélection automatique des serveurs virtuels pour attribuer des licences aux serveurs virtuels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Lorsque CPX est déployé en tant que proxy sidecar dans un déploiement de maillage de services, les serveurs virtuels sont sous licence uniquement si l'adresse IP correspond à l'adresse IP NS du CPX.

- Activé les (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#enable-web-transaction-and-tcp-transaction-settings) paramètres de transaction Web et de transaction TCP sur **Tous** pour que l'agent NetScaler obtienne les transactions HTTP et TCP.
- Envoyé du (/fr-fr/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#send-traffic-to-microservices) trafic vers les microservices.

Afficher les détails dans le graphique de service

Dans NetScaler Console, accédez à **Applications > Graphiques de service > Graphique de service Kubernetes** et sélectionnez la durée dans la liste pour afficher les détails du graphique de service.

TOPOLOGIE À DEUX NIVEAUX/SERVICE MESH LITE	TOPOLOGIE À UN SEUL NIVEAU/INGRESS UNIFIÉ
☐	☐

- **Ingress de niveau 1** – Le contrôleur d'entrée NetScaler à l'intérieur du cluster Kubernetes configure une instance NetScaler (VPX/MPX/SDX/BLX) à l'extérieur du cluster Kubernetes.
- **Ingress de niveau 2** – Le contrôleur d'entrée NetScaler s'exécutant en tant que sidecar avec l'instance NetScaler CPX à l'intérieur du cluster Kubernetes.
- **Ingress** – S'affiche pour toutes les autres topologies de déploiement.

Tableau de bord du graphique de service

☐

1 - Carte réseau de bout en bout de votre application qui montre comment vos services composants communiquent

2 – Graphique qui indique les accès et les erreurs pour une durée spécifique

3 – Barre de recherche pour rechercher des services

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4 – Liste de temps pour sélectionner la durée

5 - Appliquer des filtres pour afficher les services

6 – Icône de paramètres

7 – Vue zoom avant et zoom arrière

8 – Vue graphique ou vue tabulaire

En fonction de la durée sélectionnée, vous pouvez afficher le graphique de service.

ICÔNE DE SERVICE	DESCRIPTION
	La largeur du bord indique le nombre d'accès. Plus la largeur du bord est grande, plus le nombre d'accès est élevé.
	Un service avec une icône d'avertissement indique que le service présente des erreurs.
	Un service avec une icône de chronomètre indique que le service présente des problèmes de latence ou de temps de réponse.
	Un service avec les icônes de chronomètre et d'avertissement indique que le service présente à la fois des erreurs et des problèmes de latence/temps de réponse.

REMARQUE

Si un service n'a pas d'icône d'avertissement ou de chronomètre, cela indique que le service présente des anomalies ou un dépassement de seuil pour les accès.

En fonction de la durée sélectionnée, vous pouvez afficher le graphique de service. Sélectionnez la période dans le graphique qui indique les accès pour obtenir des informations supplémentaires.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si aucune transaction active n'est reçue par NetScaler Console, vous ne pouvez afficher que les services qui sont équilibrés en charge par l'instance NetScaler. Lorsque vous survolez un service avec le pointeur de la souris, toutes les métriques sont affichées comme 0.

Le graphique de service est affiché avec le protocole utilisé par les services. Considérez que vous avez les services suivants exécutés dans votre cluster Kubernetes, comme indiqué dans l'image :

Remarque

Si vous avez ajouté plusieurs clusters dans **Orchestration** > **Kubernetes** > **Clusters**, vous pouvez afficher les services associés à chaque cluster.

Vous pouvez afficher les statuts suivants pour vos services :

- **Critique (rouge)** - Indique lorsque le temps de réponse moyen du service > 200 ms ET le nombre d'erreurs > 0
- **À examiner (orange)** - Indique lorsque le temps de réponse moyen du service > 200 ms OU le nombre d'erreurs > 0
- **Bon (vert)** - Indique aucune erreur et un temps de réponse moyen du service < 200 ms

Voici les protocoles qui vous permettent d'identifier le protocole utilisé par un service :

- **TCP** – Indique que le service utilise le protocole TCP.
- **SSL, HTTP** – Indique que le service utilise le protocole SSL sur HTTP.
- **SSL, TCP** – Indique que le service utilise le protocole SSL sur TCP.

REMARQUE

Le service sans protocole indique que le service utilise le protocole HTTP.

Afficher les tendances des métriques clés à l'aide de la vue tabulaire

À l'aide de la vue tabulaire, vous pouvez voir :

- Métriques clés pour le service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Métriques clés entre un service source et un service de destination



En tant qu'administrateur, en utilisant ces métriques clés, vous pouvez analyser les tendances des signaux d'or pour la durée sélectionnée.

Afficher les métriques client

Vous pouvez voir depuis quel emplacement le client accède au service. En tant qu'administrateur, vous pouvez visualiser les métriques client et analyser les problèmes qui proviennent du client.

Passez le pointeur de la souris sur une région client pour afficher les métriques.



- **Requêtes** - Indique le nombre total de requêtes reçues par le client.
- **Latence du réseau client** - Indique la latence moyenne du réseau client.
- **Erreurs client 4xx** - Indique le nombre total d'erreurs client 4xx.
- **Erreurs SSL client** - Indique le nombre total d'erreurs SSL client.

Blocs IP dans NetScaler Console - NetScaler Console peut reconnaître l'emplacement du client si celui-ci utilise une adresse IP publique. NetScaler Console dispose de son fichier CSV de localisation intégré qui correspond à l'emplacement en fonction de la plage d'adresses IP du client.

NetScaler Console peut reconnaître l'emplacement du client avec une adresse IP privée uniquement lorsque l'adresse IP est ajoutée au serveur NetScaler Console. Par exemple, si l'adresse IP du client se situe dans une plage d'adresses IP privées associée à la ville A, NetScaler Console reconnaît que le trafic provient de la ville A pour ce client.

Créer un bloc d'adresses IP privées

NetScaler Console peut reconnaître l'emplacement d'un client lorsque l'adresse IP privée du client est ajoutée au serveur NetScaler Console. Par exemple, si l'adresse IP d'un client se situe dans la plage d'un bloc d'adresses IP privées associé à la ville A, NetScaler Console reconnaît que le trafic provient de la ville A pour ce client.

Pour créer un bloc d'adresses IP :

1. Dans NetScaler Console, accédez à **Paramètres** > **Paramètres d'analyse** > **Blocs IP**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer des blocs IP**, spécifiez les paramètres suivants :
    - **Nom**. Spécifiez un nom pour le bloc d'adresses IP privées

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Adresse IP de début**. Spécifiez la plage d'adresses IP la plus basse pour le bloc d'adresses IP.
- **Adresse IP de fin**. Spécifiez la plage d'adresses IP la plus élevée pour le bloc d'adresses IP.
- **Pays**. Sélectionnez le pays dans la liste.
- **Région**. En fonction du pays, la région est automatiquement renseignée, mais vous pouvez sélectionner votre région.
- **Ville**. En fonction de la région, la ville est automatiquement renseignée, mais vous pouvez sélectionner votre ville.
- **Latitude de la ville** et **Longitude de la ville**. En fonction de la ville que vous sélectionnez, la latitude et la longitude sont automatiquement renseignées.

3. Cliquez sur **Créer** pour terminer.



Blocs d'adresses IP publiques

NetScaler Console peut également reconnaître l'emplacement d'un client si celui-ci utilise une adresse IP publique. NetScaler Console dispose de son fichier CSV de localisation intégré qui correspond à l'emplacement en fonction de la plage d'adresses IP du client. Pour utiliser le bloc d'adresses IP publiques, la seule exigence est d'activer la collecte des **données géographiques** à partir de la page **Configurer Insight**.

Remarque

NetScaler Console nécessite une connexion Internet pour afficher les géocartes pour un emplacement géographique particulier. Une connexion Internet est également requise pour exporter la géocarte aux formats .pdf, .png ou .jpg.



Afficher les métriques d'entrée

Vous pouvez afficher le type d'entrée utilisé dans le cluster Kubernetes.



- Adresse IP NetScaler et son score
- **État actuel** – Indique si l'instance NetScaler est active (Up), inactive (Down) ou hors service (Out of Status)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Contribution maximale** – Indique le problème qui affecte le score de l'instance

Pour la topologie à un seul niveau, vous ne pouvez afficher qu'un seul **Ingress**.

Cliquez sur l'**Ingress** pour obtenir plus de détails. Pour plus d'informations, consultez Afficher les détails d'entrée pour le dépannage des problèmes.

Afficher les métriques TCP et SSL

À l'aide des métriques TCP et SSL, vous pouvez :

- Afficher les détails de connexion TCP entre les services
- Déterminer si les problèmes liés au TCP proviennent du service source ou de destination
- Vérifier si l'erreur SSL provient du service source ou de destination
- Afficher la version du protocole SSL utilisée par les services SSL

Métriques TCP

Passez le pointeur de la souris sur un service TCP ou son service entrant associé pour afficher les métriques TCP.



- **Connexions TCP** – Nombre total de connexions établies entre les services
- **Volume de données** – Données totales traitées par le service
- **Réinitialisation du serveur TCP** – Nombre total de réinitialisations TCP initiées depuis le serveur

Métriques SSL

Passez le pointeur de la souris sur un service qui utilise le protocole SSL pour afficher les métriques SSL.



- **Erreurs de serveur SSL** – Indique le nombre total d'erreurs SSL provenant du serveur. (Par exemple, certificat SSL inconnu)
- **Protocole SSL** – Indique la version du protocole SSL utilisée par le service
- **Erreurs client SSL** - Indique le nombre total d'erreurs SSL provenant du client. (Par exemple, erreur d'authentification client SSL)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les détails du service

Cliquez sur un service et sélectionnez **Afficher les détails** pour afficher les détails du service. Pour plus d'informations, consultez Afficher les détails du service.

Appliquer des filtres

Vous pouvez appliquer des filtres pour afficher des informations de service spécifiques. Cliquez sur la liste **Aucun filtre** pour obtenir les options de filtre.

Par exemple, si vous souhaitez afficher les services dont la latence est inférieure à 150 ms, cliquez sur le graphique à barres sous **Temps de réponse du service** pour afficher les résultats.

Cliquez sur **Service Info** pour sélectionner et appliquer des filtres pour :

- **Cluster** – Affiche tous les services applicables pour le ou les clusters sélectionnés.
- **Namespace** – Affiche tous les services applicables pour le namespace sélectionné.

  Remarque

  > Selon les étiquettes configurées pour le service dans le fichier YAML de définition de service Kubernetes, vous pouvez également afficher d'autres options de filtre.

Cliquez sur **Effacer tout** pour effacer tous les filtres.

Vous pouvez également utiliser la zone de texte de recherche et taper un nom de service pour afficher les résultats sur le graphique de service.

Utilisation de l'option de paramètres

1 – Icône de paramètres

2 – Options pour afficher le graphique de service sous forme de vues par défaut, basées sur les couches ou à force dirigée

3 – Sélectionnez les options dans la liste pour afficher les services par catégorie. Après avoir sélectionné une catégorie dans la liste, cliquez sur **+** sur le graphique pour afficher tous les services

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4 – Permet de sélectionner l'option d'affichage des services.

5 - Options pour enregistrer les paramètres ou les réinitialiser par défaut.

Analyser les erreurs

Passez le pointeur de la souris sur un service qui indique des erreurs.

ERREUR	DESCRIPTION
	La **réinitialisation du serveur TCP** indique le nombre total de réinitialisations TCP initiées par le serveur.
	La **réinitialisation du client TCP** indique le nombre total de réinitialisations TCP initiées par le client.
	Les erreurs client SSL indiquent le nombre total d'erreurs SSL provenant du client. (Par exemple, erreur d'authentification client SSL).
	Les erreurs serveur SSL indiquent le nombre total d'erreurs SSL provenant du serveur. (Par exemple, certificat SSL inconnu)

REMARQUE

- Le nombre d'erreurs client (quel que soit le type de protocole) est affiché dans n'importe quel service si le nombre d'erreurs client est **1 ou plus**.
- Le nombre d'erreurs client affiché pour un service indique que les erreurs proviennent du côté client.

Afficher les détails de la transaction HTTP

REMARQUE

Vous pouvez afficher les erreurs en passant le pointeur de la souris sur un service erroné et en cliquant sur le nombre de problèmes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Selon l'exemple montré dans l'image, vous pouvez afficher une carte réseau de bout en bout de votre application qui montre comment vos services composants communiquent.

Lorsque vous passez le pointeur de la souris sur le **Ecommerce-Service**, vous pouvez afficher les détails des métriques pour le **Ecommerce-Service**.

NetScaler Console vous permet également d'afficher les détails des transactions entre l'Ingress et les services. Passez le pointeur de la souris pour afficher des détails tels que le nombre total d'erreurs, le temps de réponse moyen du service, etc., entre l'Ingress et le service.

Requêtes – Indique le nombre total de requêtes reçues par le service.

Temps de réponse du service – Indique le temps de réponse moyen pris par le service pour répondre pour le Time To First Byte (TTFB).

Erreurs – Indique le nombre total d'erreurs telles que 4xx, 5xx, etc.

Volume de données – Indique le volume total de données traitées par le service.

Protocole SSL – Indique la version du protocole SSL.

Cliquez sur la flèche entre **Ingress** et **service** pour afficher les transactions détaillées.

Pour plus d'informations, consultez Afficher les analyses pour les transactions Web.

Configurer les seuils dans le graphique de service

En tant qu'administrateur, vous pouvez configurer des seuils pour les services Kubernetes. NetScaler Console affiche l'état du service (Critique, À réviser et Bon) en fonction du temps de réponse du service et du nombre d'erreurs. Par défaut, vous pouvez afficher le **Seuil par défaut** (temps de réponse du service = 200 ms et nombre d'erreurs = 0) appliqué à tous les services.

REMARQUE

Vous ne pouvez pas supprimer le Seuil par défaut.

Pour configurer un nouveau seuil :

Dans le graphique de service :

1. Cliquez sur l'icône des paramètres et sélectionnez l'onglet **Seuils**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur **Nouveau seuil** pour configurer un nouveau seuil.

   

   La page **Nouveau seuil** s'affiche.

3. Configurez les paramètres suivants :

   a. **Nom** – Spécifiez un nom pour le seuil.

   b. Sous **Microservices**, sélectionnez les services auxquels vous souhaitez appliquer le seuil

   c. Sous **Seuils**, sélectionnez **Simple** ou **Double** pour Temps de réponse élevé et Erreurs élevées

   d. Spécifiez les valeurs de seuil.

   REMARQUE

   Si vous sélectionnez le double seuil, assurez-vous que :

   - La valeur du seuil 1 est inférieure à la valeur du seuil 2. Par exemple, si vous configurez le seuil 1 à 250 ms, le seuil 2 doit être de 251 ms ou plus.
   - La valeur du seuil 1 ne doit pas être identique à la valeur du seuil 2.

4. Cliquez sur **Enregistrer**.

   

   Le seuil est créé avec succès. Vous pouvez afficher les détails du seuil sur la page **Seuils**.

Seuil unique

Lorsque vous configurez un seuil unique, NetScaler Console :

- Compare les valeurs actuelles avec les valeurs de seuil configurées
- Calcule la pénalité totale en fonction des seuils dépassés
- Affiche le score de service et l'état du service en fonction du calcul de la pénalité

Double seuil

Lorsque vous configurez un double seuil, NetScaler Console :

- Compare les valeurs actuelles avec les valeurs de seuil configurées
- Vérifie si les valeurs actuelles sont :
  - Inférieures au seuil 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Entre le seuil 1 et le seuil 2
    - Supérieures au seuil 2

- Calcule la pénalité totale en fonction des seuils dépassés
- Affiche le score de service et l'état du service en fonction du calcul de la pénalité

Afficher les détails du service

Cliquez sur un service et sélectionnez **Afficher les détails**.



La page des détails du service vous permet d'afficher :

- Le nom du cluster où le service est hébergé (1)
- L'espace de noms et les étiquettes de service du service (2) (4)
- Tous les services entrants et sortants associés connectés au service sélectionné (3)
- Les métriques clés du service sous forme de graphique, telles que les accès, le temps de réponse, les erreurs, le volume de données, les erreurs frontales SSL et les erreurs frontales TCP (5).
- Les pods backend associés au service (6).



En utilisant ces tendances de métriques clés, vous pouvez analyser les performances du service pour une durée spécifique.

La métrique **Temps de réponse** vous permet d'afficher :

- **99e centile** – Indique que 99 % des requêtes pour la durée sélectionnée sont inférieures à 32 ms (selon l'image d'exemple).
- **Moyenne** – Indique le temps de réponse moyen du service
- **99,9e centile** – Indique le temps de réponse le plus élevé du service

Détails des métriques

MÉTRIQUES	DESCRIPTION
Requêtes	Le nombre total de requêtes reçues par le service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Erreurs	Le nombre total d'erreurs HTTP provenant du service
Temps de réponse du service	Le temps de réponse moyen du service pour le Time To First Byte (TTFB).
Volume de données	Le volume total de données traité par le service
Erreurs SSL front-end	Le nombre total d'erreurs SSL front-end provenant du service. Par exemple : ÉCHEC D'AUTHENTIFICATION CLIENT SSL
Erreurs SSL back-end	Le nombre total d'erreurs SSL back-end provenant du service. Par exemple : Erreurs client SSL
Erreurs TCP de back-end	Le total des erreurs TCP de back-end du service. Par exemple : Réinitialisation du serveur TCP
Erreurs TCP de front-end	Le total des erreurs TCP de front-end du service. Par exemple : Réinitialisation du client TCP

Afficher les détails du pod de back-end

Cliquez sur l'onglet **Pods** pour afficher les pods de back-end associés au service.



- **Nom du pod** – Indique le nom du pod
- **Statut** – Indique si le pod est en cours d'exécution (UP) ou non (DOWN).
- **Adresse IP** – Indique l'adresse IP du pod

Utiliser l'option Interroger maintenant pour obtenir le statut du pod

L'option **Interroger maintenant** récupère le dernier statut du pod depuis le cluster.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les détails d'entrée pour le dépannage des problèmes

Dans le graphe de services, cliquez sur l'entrée et sélectionnez **Afficher les détails** pour visualiser les détails de l'instance NetScaler configurée pour le cluster Kubernetes.

Cliquez sur **Détails de l'instance** pour afficher les détails.

Les détails suivants sont affichés :

- **Informations** - Détails de l'instance tels que le type d'instance, le type de déploiement, la version, le modèle, etc.
- **Fonctionnalités** – Par défaut, les fonctionnalités non sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.
- **Modes** – Par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.

Le tableau de bord de l'instance présente un aperçu de l'instance où vous pouvez voir les détails suivants :

- **Score de l'instance**

  1 – Indique le score actuel de l'instance NetScaler pour la durée sélectionnée. Le score final est calculé comme **100 moins les pénalités totales**. Le graphique affiche les plages de scores pour la durée sélectionnée.

  2 – Indique l'état actuel de l'instance NetScaler, tel que **Actif**, **Inactif** et **Hors service**.

  3 – Indique la durée pendant laquelle l'instance NetScaler est opérationnelle.

  4 – Indique le nombre total d'interfaces réseau activées et désactivées pour l'instance. Cliquez pour afficher les détails tels que le nom de l'interface réseau et l'état (activée ou désactivée).

  5 – Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

  6 – Affiche le nombre total de problèmes et la catégorie de problèmes de l'instance NetScaler.
- **Métriques clés**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cliquez sur chaque onglet pour afficher les détails. Pour chaque métrique, vous pouvez afficher la valeur moyenne et la valeur de différence pour la durée sélectionnée.

L'image suivante est un exemple pour les requêtes HTTPS/sec et la durée sélectionnée est le dernier mois. La valeur **692** est la moyenne des requêtes HTTPS/sec pour le dernier mois et la valeur **20** est la valeur de différence. Dans le graphique, la première valeur est **139** et la dernière valeur est **119**. La valeur de différence est **139 – 119 = 20**.



Vous pouvez afficher les métriques d'instance suivantes sous forme de graphique pour la durée sélectionnée :

- **Utilisation du CPU** – Le pourcentage moyen d'utilisation du CPU de l'instance pour la durée sélectionnée (affiché pour le CPU de paquets et pour le CPU de gestion).
- **Utilisation de la mémoire** – Le pourcentage moyen d'utilisation de la mémoire de l'instance pour la durée sélectionnée.
- **Utilisation du disque** – Le pourcentage moyen d'espace disque de l'instance pour la durée sélectionnée.
- **Débit** – Le débit réseau moyen traité par l'instance pour la durée sélectionnée.
- **Requêtes HTTPS/s** – Le nombre moyen de requêtes HTTPS reçues par l'instance pour la durée sélectionnée.
- **Connexions TCP** – Le nombre moyen de connexions TCP établies par le client et le serveur pour la durée sélectionnée.
- **Transactions SSL** – Le nombre moyen de transactions SSL traitées par l'instance pour la durée sélectionnée.

- **Problèmes**

  Vous pouvez afficher les problèmes suivants qui se produisent dans l'instance NetScaler :

CATÉGORIE DE PROBLÈME	DESCRIPTION	PROBLÈMES
Ressources système	Affiche tous les problèmes liés aux ressources système NetScaler telles que l'UC, la mémoire, l'utilisation du disque, etc.	- Utilisation élevée du processeur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIE DE PROBLÈME	DESCRIPTION	PROBLÈMES
		- Utilisation élevée de la mémoire
		- Utilisation élevée du disque
		- Défaillances de la carte SSL
		- Panne de courant
		- Erreur de disque
		- Erreur Flash
		- Rejets NIC
Configuration SSL	Affiche tous les problèmes liés à la configuration SSL sur l'instance NetScaler.	- Certificats SSL expirés
		- Émetteur non recommandé
		- Algorithme non recommandé
		- Force de clé non recommandée
Déviation de configuration	Affiche tous les problèmes liés aux tâches de configuration appliquées dans l'instance NetScaler.	- Dérive de configuration
		- Exécution vs Modèle
Problèmes de capacité	Affiche les problèmes de capacité de NetScaler. La console NetScaler interroge ces événements toutes les	- Limite de débit atteinte

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIE DE PROBLÈME	DESCRIPTION	PROBLÈMES
	cinq minutes depuis l'instance NetScaler et affiche les pertes de paquets ou les incréments de compteur de limite de débit, le cas échéant. Les problèmes sont classés selon les paramètres de capacité suivants.	
		- Limite de CPU PE atteinte
		- Limite PPS atteinte
		- Limite de débit SSL
		- Limite de taux TPS SSL
Réseau	Affiche les problèmes opérationnels qui surviennent dans les instances.	Pour plus d'informations, consultez Analyse d'infrastructure améliorée avec de nouveaux indicateurs.

Cliquez sur chaque onglet pour analyser et résoudre le problème. Par exemple, considérez qu'une instance présente les erreurs suivantes pour la durée sélectionnée :

- L'onglet **Actuel** affiche les problèmes opérationnels NetScaler actuels qui affectent le score de l'instance.
- L'onglet **Tous** affiche tous les problèmes d'infrastructure détectés pour la durée sélectionnée.

Traçage distribué

Dans le graphique de service, vous pouvez utiliser la vue de traçage distribué pour :

- Analyser les performances globales du service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Visualiser le flux de communication entre le service sélectionné et ses services interdépendants.
- Identifier quel service indique des erreurs et dépanner le service erroné
- Afficher les détails des transactions entre le service sélectionné et chacun de ses services interdépendants.

Prérequis

Pour afficher les informations de trace du service, vous devez :

- Assurez-vous qu'une application maintient les en-têtes de trace suivants lors de l'envoi de trafic est-ouest :

  ☐

- Pour les **versions CIC antérieures à 1.7.23**, mettez à jour le fichier YAML CPX avec `NS_DISTRIBUTED_TRACING` et la valeur `yes`

  ☐

- Pour les **versions CIC ultérieures à 1.7.23**, vous devez utiliser une ConfigMap.

  Les ConfigMaps vous permettent de séparer vos configurations de vos pods et de rendre vos charges de travail portables. En utilisant les ConfigMaps, vous pouvez facilement modifier et gérer les configurations de vos charges de travail et réduire le besoin de coder en dur les données de configuration dans les spécifications de pod.

  Avec la prise en charge de ConfigMap, vous pouvez mettre à jour la configuration automatiquement tout en maintenant le pod du contrôleur d'entrée NetScaler en cours d'exécution. Vous n'avez pas besoin de redémarrer le pod après la mise à jour. Pour plus d'informations, consultez Prise en charge de ConfigMap pour le contrôleur d'entrée.

  En utilisant le ConfigMap, vous pouvez activer ou désactiver le traçage distribué, les événements, les journaux d'audit, etc. Pour utiliser le ConfigMap :

  a. Créez un fichier YAML en utilisant les paramètres requis.

     L'exemple de fichier YAML suivant a le traçage distribué activé et d'autres variables telles que les journaux d'audit, les événements et les transactions désactivées :

     ```
     apiVersion: v1

     kind: ConfigMap
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <Console-AgentIP> / <Console-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
```

Remarque

> Vous pouvez fournir les valeurs pour `Samplingrate` entre 0 et 100. NetScaler Console affiche le nombre de transactions de trace mentionné.

b. Déployez le ConfigMap en utilisant :

`kubectl create -f <configmap-yaml>.yaml`

c. Modifiez le fichier YAML CPX et utilisez `envFrom` ou `args` pour spécifier les arguments suivants :

```
envFrom:
 - configMapRef:
     name: cic-configmap
```

OU

d. Si vous souhaitez modifier la valeur d'une variable, modifiez les valeurs dans le ConfigMap. Dans cet exemple, toutes les autres variables sont passées de `false` à `true`.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <Console-AgentIP> / <Console-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      enable: 'true'

      port: 5557
```

e. Réappliquez le ConfigMap en utilisant la commande suivante :

```
kubectl apply -f <yaml-file>.yaml
```

Afficher les détails de la trace de service

Dans le graphique de service, cliquez sur un service et sélectionnez **Informations de trace**.

La page Récapitulatif de la trace s'affiche pour le service sélectionné.

Le **Récapitulatif de la trace** affiche :

- Une recherche avancée qui vous permet de rechercher des transactions avec des suggestions et des opérateurs (1). Pour plus d'informations, consultez Recherche avancée.
- La liste des durées qui vous permet de sélectionner la durée, telle que 1 heure, 12 heures, 1 jour, 1 semaine, 1 mois et une durée personnalisée (2).
- Le graphique Détails de la chronologie qui vous permet de glisser-déposer pour afficher les résultats pour une durée spécifique (3).
- Le panneau Filtres qui vous permet de sélectionner des options pour chaque métrique (4).
- Les détails de la transaction pour le service sélectionné (5).

Afficher les détails de la transaction

Cliquez sur une transaction pour obtenir des informations détaillées. Vous pouvez afficher les détails de la transaction pour le service sélectionné, tels que :

- Heure de début
- Heure de fin
- Métriques SSL
- Communication avec les services interdépendants (ainsi que les erreurs et le temps de réponse avec chaque service).

L'exemple suivant indique une erreur de `catalogue-store-service`. Cliquez sur **Voir les détails de la trace** pour plus de détails.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La page Détails de la trace s'affiche.

1 – Affiche l'heure de début, le temps de réponse, le nombre total de services et le nombre total de spans pour la transaction.

2 – Affiche les détails du service sélectionné qui a communiqué avec ses services interdépendants. Vous pouvez cliquer sur chaque transaction pour afficher les détails.

3 – Affiche les détails de la transaction pour chaque service.

Selon l'image d'exemple, `catalogue-store-service` a indiqué une erreur. Cliquez sur la transaction disponible pour `catalogue-store-service`.

Les détails de la transaction entre `product-catalogue-service` et `catalogue-store-service` indiquent une réponse HTTP de 500. Avec ces détails, en tant qu'administrateur, vous pouvez analyser le service erroné et dépanner `product-catalogue-service` comme solution.

Vous pouvez également filtrer les résultats en sélectionnant des options pour chaque métrique sous le panneau **Filtres**. Par exemple, si vous souhaitez afficher toutes les transactions 5xx, cliquez sur **Code de réponse** et sélectionnez **500**.

- **RTT client** : Durée nécessaire à un paquet pour voyager depuis le client.
- **RTT serveur** : Durée nécessaire à un paquet pour voyager depuis le serveur.
- **Temps de réponse de l'application** : Temps de réponse moyen de l'application
- **Temps de transfert de données** : La taille du transfert de données et le débit auquel la transmission peut s'effectuer depuis/vers un service.
- **Emplacement** : L'emplacement du client
- **Navigateur** : Les types de navigateurs utilisés par les clients. Par exemple : Chrome, Firefox.
- **Système d'exploitation client** : Le système d'exploitation client basé sur les détails de l'agent utilisateur du navigateur.
- **Appareil** : Les appareils basés sur les détails de l'agent utilisateur du navigateur. Par exemple : Tablette, Mobile.
- **Type de requête** : Le type de requête de transaction. Par exemple : GET.
- **Code de réponse** : Le code de réponse reçu du serveur. Par exemple : 501, 404, 200.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Type de contenu de réponse** : Le type de contenu de la transaction. Si la requête du client est pour text/html, alors la réponse du serveur doit être text/html.
- **Protocole SSL** : La version du protocole SSL utilisée par les clients. Par exemple : SSLv3.
- **Force du chiffrement SSL** : La force du chiffrement basée sur la taille de la clé du certificat SSL, telle que élevée, moyenne et faible.
- **Force de la clé SSL** : La force du chiffrement SSL est calculée à partir de la taille de la clé du certificat SSL. La longueur de la clé définit la sécurité de l'algorithme SSL. Par exemple : 2048
- **Raison de l'échec frontal SSL** : Le message d'erreur de la poignée de main SSL frontale. Par exemple : SSL CLIENTAUTH FAILURE

Afficher les détails de diagnostic pour les données partielles ou manquantes dans le graphe de service

Une fois que vous avez terminé la configuration requise du graphe de service et ajouté le cluster Kubernetes dans NetScaler Console, le graphe de service commence à afficher des données. Dans certains scénarios, vous pourriez observer que le graphe de service affiche des données partielles ou aucune donnée. Voici quelques-unes des raisons possibles pour les données partielles ou manquantes dans le graphe de service :

- La route statique n'est pas configurée
- L'état du cluster Kubernetes est en panne
- L'enregistrement CPX a échoué
- Les serveurs virtuels CPX ne sont pas sous licence
- La configuration d'analyse requise n'est pas définie, ce qui empêche le graphe de service de charger toutes les données

En tant qu'administrateur, il peut être difficile d'analyser les raisons lorsque le graphe de service affiche des données partielles ou aucune donnée. Les informations de diagnostic de la page du graphe de service vous permettent de voir les raisons possibles et les actions requises pour résoudre le problème de données partielles ou manquantes.

Dans NetScaler Console, accédez à **Applications** > **Graphe de service** et cliquez sur l'onglet **Microservices**.

Diagnostics pour l'absence de données

Si le graphe de service n'affiche aucune donnée, le message de diagnostic suivant s'affiche.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cliquez sur **>** pour afficher les détails. Vous pouvez consulter les raisons possibles pour lesquelles le graphe de service n'affiche aucune donnée. L'image suivante est un exemple d'absence de données dans le graphe de service.



Cliquez sur **Voir plus** pour afficher les détails des problèmes.



- **Type de problème** – Indique si les problèmes proviennent de la configuration, de la configuration des analyses ou de la licence.
- **Message** – Indique la cause du problème.
- **Action** – Indique l'action à effectuer pour résoudre le problème.

Diagnostics pour les données partielles

Si le graphique de service n'affiche que des données partielles, cliquez sur le bouton **Afficher les diagnostics** pour afficher les informations de diagnostic.

L'exemple suivant indique que les transactions TCP sont désactivées.



Pour cet exemple, vous devez activer les **Paramètres de transaction TCP** sur **Tous** en accédant à **Paramètres > Paramètres d'analyse**.

Dépannage

En tant qu'administrateur, vous pouvez utiliser ces messages de diagnostic pour valider et tenter de résoudre ces problèmes. Une fois le dépannage effectué, NetScaler Console exécute automatiquement une vérification de diagnostic périodique à intervalles réguliers. Une fois la vérification de diagnostic terminée, le problème de données partielles ou d'absence de données dans le graphique de service sera résolu.

Vous pouvez également cliquer sur **Exécuter les diagnostics**, sélectionner les **instances CPX**, puis cliquer sur **Exécuter les diagnostics**.



Pour plus de scénarios de dépannage, consultez la FAQ.

Graphe de service pour les applications

Pour afficher le graphe de service d'une application :

1. Accédez à **Applications** > **Tableau de bord**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sélectionnez une application.

   La page des détails de l'application s'affiche.

3. Sélectionnez la durée et cliquez sur **Graphe de service**.

   

   La page du graphe de service s'affiche pour l'application sélectionnée.

Vous pouvez afficher le graphe de service dans la **Vue d'application** ou dans la **Vue des fonctions réseau**.



Vous pouvez également faire glisser et sélectionner les accès et les erreurs pour modifier les résultats.



Vue d'application

Affiche l'aperçu de la configuration de l'application. Dans cette vue, vous pouvez visualiser la communication entre le client, NetScaler et les applications web.



Vue des fonctions réseau

Affiche les serveurs virtuels associés à l'application. Dans cette vue, vous pouvez visualiser si le NetScaler communique avec :

- Serveur virtuel de commutation de contenu pour accéder à l'application
- Serveur virtuel d'équilibrage de charge pour accéder à l'application
- Les serveurs virtuels de commutation de contenu et d'équilibrage de charge pour accéder à l'application



Pour une application GSLB, les détails sont affichés avec le centre de données et le NetScaler.



Vue du graphique de service pour les transactions inactives

Si aucune transaction active n'a lieu entre NetScaler et l'application web, le graphique de service affiche uniquement la configuration de base de l'application (sans client ni NetScaler).



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque vous passez le pointeur de la souris sur un service ou un serveur virtuel, les détails sont affichés comme 0 pour toutes les métriques en raison de l'absence de transactions.



Analyser les métriques

Passez le pointeur de la souris sur chaque service pour afficher les détails des métriques, soit dans la vue Application, soit dans la vue Fonctions réseau.

Mesures client

Passez le pointeur de la souris sur le client pour afficher les mesures client.



- **Latence du réseau client** – Indique la latence du réseau depuis le client.
- **Erreurs 4xx client** – Indique le nombre total d'erreurs 4xx survenues depuis le client.
- **Erreurs SSL client** – Indique le nombre total d'erreurs SSL depuis le client.

Mesures de fonction réseau

Passez le pointeur de la souris sur un service d'équilibrage de charge ou de commutation de contenu pour afficher les détails des mesures.



- **Requêtes** – Indique le nombre total de requêtes reçues par le serveur virtuel
- **Temps de traitement NetScaler** – Indique le temps de traitement moyen par l'instance NetScaler
- **Volume de données** – Indique le volume total de données traitées par le serveur virtuel
- **Score de santé** – Indique le score de l'application
- **État actuel** – Indique l'état actuel du serveur virtuel

Mesures de service

Passez le pointeur de la souris sur un service (application web) pour afficher les métriques



- **Requêtes** – Indique le nombre total de requêtes reçues par le service
- **Temps de réponse du service** – Indique le temps de réponse moyen du service
- **Erreurs** – Indique le nombre total d'erreurs survenues depuis le service
- **Volume de données** – Indique le volume total de données traitées par le service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Métriques NetScaler (uniquement pour les applications GSLB)

Passez le pointeur de la souris sur le NetScaler pour afficher les métriques.



- Affiche le nom d'hôte et le score NetScaler actuel. Le score est calculé en fonction des différents problèmes potentiels de NetScaler. Pour plus d'informations, consultez Score d'instance.
- **Adresse IP** – Indique l'adresse IP du NetScaler
- **État actuel** – Indique l'état du NetScaler, tel que Actif, Inactif ou Hors service
- **Temps de traitement NetScaler** – Indique le temps de traitement moyen par l'instance NetScaler

REMARQUE

Si aucun nom d'hôte n'est attribué à NetScaler :

-L'adresse IP du NetScaler est affichée au lieu du nom d'hôte.
-Dans les métriques, les informations d'adresse IP du NetScaler ne sont pas affichées.



Vue d'ensemble de toutes les applications dans le graphique de service

Accédez à **Applications** > **Service Graph**, puis cliquez sur **Global**.



Le graphique de service affiche les éléments suivants pour la durée sélectionnée :

- La région à partir de laquelle les utilisateurs accèdent à l'application spécifique

Centres de données où les instances NetScaler sont hébergées

- Le nombre total d'applications discrètes de toutes les instances NetScaler

REMARQUE

Si une instance NetScaler n'a pas d'applications discrètes, le bord de la flèche vers le serveur virtuel discret à partir de l'instance NetScaler n'est pas visible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le nombre total d'applications personnalisées de toutes les instances NetScaler
- Le nombre total d'applications de microservices de l'instance NetScaler CPX

Afficher les métriques client

Passez le pointeur de la souris sur une région client pour afficher les métriques.



- **Latence du réseau client** - Indique la latence moyenne du réseau client.
- **Erreurs 4xx client** - Indique le nombre total d'erreurs 4xx client.
- **Erreurs SSL client** - Indique le nombre total d'erreurs SSL client.

Afficher les détails de NetScaler

Le graphique de service vous permet d'afficher :

- Le centre de données regroupé avec le nombre total de ses instances NetScaler
- Uniquement les 4 instances NetScaler les moins bien notées de chaque centre de données



Cliquez sur **Plus d'ADC** pour afficher toutes les instances NetScaler en sélectionnant les onglets d'état respectifs (Critique, Révision, Bon et Non applicable).



Passez le pointeur de la souris sur une instance NetScaler pour afficher les métriques.



Vous pouvez afficher :

- Adresse IP et score de l'instance NetScaler
- **Nom d'hôte** – Indique le nom d'hôte attribué à l'instance NetScaler
- **État actuel** – Indique l'état actuel de l'instance NetScaler, tel que Actif, Inactif, Hors service.
- **Problème principal** – Indique le problème principal qui affecte le score NetScaler actuel

Cliquez sur l'**instance NetScaler** pour afficher les détails de l'instance tels que le score de l'instance, les métriques clés et les problèmes associés à l'instance NetScaler. Pour plus d'informations, consultez Afficher les détails de l'instance dans Infrastructure Analytics.

Afficher les applications discrètes

Le graphique de service affiche les 4 applications discrètes les moins bien notées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considérez que vous avez les applications discrètes suivantes :

NOM DE L'APPLICATION	NETSCALER	SCORE DE L'APPLICATION	STATUT DE L'APPLICATION
App1	10.102.29.50	35 (Critique)	Actif
App2	10.102.29.90	100 (Bon)	Arrêté
App 3	10.102.32.40	49 (À revoir)	Actif
App4	10.102.113.208	92 (Bon)	Arrêté
App5	10.102.25.25	86 (Bon)	Actif
App6	10.102.29.41	77 (Bon)	Actif
App7	10.102.29.102	41 (À examiner)	Actif

Dans ce scénario, vous pouvez afficher App1, App3, App6 et App7 comme les 4 applications les moins bien notées dans le graphe de services.

De même, vous pouvez également afficher les 4 applications les moins bien notées pour les applications **Personnalisées** et **Microservices**.

Passez le pointeur de la souris sur un service pour afficher les informations de métriques.

Vous pouvez afficher :

- Le nom et le score de l'application
- **État actuel** – Indique le statut actuel de l'application, tel que Actif ou Inactif.
- **Problèmes** – Indique le nombre total de problèmes applicables à l'application
- **Problème majeur** – Indique le problème principal qui a un impact sur le score global de l'application

Cliquez sur **Plus** pour afficher toutes les applications discrètes. La page du serveur virtuel discret s'affiche comme illustré dans l'image suivante :

Les serveurs virtuels sont affichés en fonction de leur statut.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Total** – Nombre total d'applications discrètes
- **Critique** – Le score de l'application est compris entre 0 et < 40
- **À examiner** – Le score de l'application est compris entre 40 et < 75
- **Bon** – Le score de l'application est > 75
- **Non applicable** – L'application n'est liée à aucun serveur virtuel

Vous pouvez cliquer sur chaque onglet pour afficher les serveurs virtuels. Lorsque vous cliquez sur une application, le graphique de service de l'application sélectionnée s'affiche.



Pour plus d'informations, consultez Graphique de service pour les applications.

Afficher les applications de microservices

Le graphique de service affiche également toutes les applications de microservices appartenant aux clusters Kubernetes. Passez le pointeur de la souris sur un service pour afficher les détails des métriques.

Vous pouvez afficher :

- Le nom du service
- Le protocole utilisé par le service, tel que SSL, HTTP, TCP, SSL sur HTTP
- **Requêtes** – Le nombre total de requêtes reçues par le service
- **Temps de réponse du service** – Le temps de réponse moyen du service.

  (Temps de réponse = RTT client + dernier octet de la requête – premier octet de la requête)
- **Erreurs** – Le nombre total d'erreurs, telles que 4xx, 5xx, etc.
- **Volume de données** – Le volume total de données traitées par le service
- **Espace de noms** – L'espace de noms du service
- **Nom du cluster** – Le nom du cluster où le service est hébergé
- **Erreurs de serveur SSL** – Le nombre total d'erreurs SSL provenant du service

Lorsque vous cliquez sur un service, le graphique de service Kubernetes pour le service sélectionné s'affiche, avec les filtres d'espace de noms de service et de nom de cluster appliqués.



Cliquez sur **Plus** pour afficher le graphique de service Kubernetes qui contient tous les services. Pour plus d'informations sur le graphique de service Kubernetes, consultez Graphique de service pour les applications cloud natives.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Barre de recherche pour filtrer les résultats

Vous pouvez utiliser la barre de recherche pour filtrer les résultats. En tant qu'administrateur, cette barre de recherche vous permet de cibler rapidement une instance/un client/une application/un centre de données particulier, lorsque vous avez :

- Une grande entreprise avec de nombreux centres de données
- De nombreuses instances NetScaler configurées pour chaque centre de données
- De nombreuses applications configurées, déployées ou accessibles via chaque instance NetScaler
- Des clients accédant à l'application depuis différents emplacements

Placez le pointeur de la souris sur la barre de recherche et sélectionnez la catégorie pour laquelle vous souhaitez créer le filtre.

Par exemple, si vous souhaitez afficher une instance NetScaler particulière, sélectionnez **Instance** dans la barre de recherche et sélectionnez l'adresse IP de l'instance. Le graphique de service global affiche l'instance sélectionnée et ses applications, centres de données et emplacements clients associés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

Les StyleBooks simplifient la tâche de gestion des configurations NetScaler complexes pour vos applications. Un StyleBook est un modèle que vous pouvez utiliser pour créer et gérer des configurations NetScaler. Vous pouvez créer un StyleBook pour configurer une fonctionnalité spécifique de NetScaler, ou vous pouvez concevoir un StyleBook pour créer des configurations pour un déploiement d'application d'entreprise tel que Microsoft Exchange ou Lync.

Les StyleBooks s'intègrent bien aux principes de l'Infrastructure-as-code pratiqués par les équipes DevOps, où les configurations sont déclaratives et gérées par version. Les configurations sont également répétées et déployées dans leur intégralité. Les StyleBooks offrent les avantages suivants :

- **Déclaratif** : Les StyleBooks sont écrits dans une syntaxe déclarative plutôt qu'impérative. Les StyleBooks vous permettent de vous concentrer sur la description du résultat ou de l'« état souhaité » de la configuration plutôt que sur les instructions étape par étape sur la façon de l'atteindre sur une instance NetScaler particulière. NetScaler Console calcule la différence entre l'état existant sur un NetScaler et l'état souhaité que vous avez spécifié, et apporte les modifications nécessaires à l'infrastructure. Étant donné que les StyleBooks utilisent une syntaxe déclarative, écrite en YAML, les composants d'un StyleBook peuvent être spécifiés dans n'importe quel ordre, et NetScaler Console détermine l'ordre correct en fonction de leurs dépendances calculées.
- **Atomique** : Lorsque vous utilisez des StyleBooks pour déployer des configurations, la configuration complète est déployée ou aucune partie n'est déployée, ce qui garantit que l'infrastructure est toujours laissée dans un état cohérent.
- **Versionné** : Un StyleBook possède un nom, un espace de noms et un numéro de version qui le distinguent de manière unique de tout autre StyleBook du système. Toute modification d'un StyleBook nécessite une mise à jour de son numéro de version (ou de son nom ou de son espace de noms) pour maintenir ce caractère unique. La mise à jour de la version vous permet également de maintenir plusieurs versions du même StyleBook.
- **Composables** : Une fois qu'un StyleBook est défini, il peut être utilisé comme une unité pour construire d'autres StyleBooks. Vous pouvez éviter de répéter les modèles de configuration courants. Cela vous permet également d'établir des blocs de construction standard au sein de votre organisation. Étant donné que les StyleBooks sont versionnés, les modifications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

apportées aux StyleBooks existants entraînent de nouveaux StyleBooks, garantissant ainsi que les StyleBooks dépendants ne sont jamais involontairement cassés.

- **Centré sur l'application** : Les StyleBooks peuvent être utilisés pour définir la configuration NetScaler d'une application complète. La configuration de l'application peut être abstraite à l'aide de paramètres. Par conséquent, les utilisateurs qui créent des configurations à partir d'un StyleBook peuvent interagir avec une interface simple consistant à remplir quelques paramètres pour créer ce qui peut être une configuration NetScaler complexe. Les configurations créées à partir de StyleBooks ne sont pas liées à l'infrastructure. Une seule configuration peut ainsi être déployée sur un ou plusieurs NetScalers, et peut également être déplacée entre les instances.
- **Interface utilisateur auto-générée** : NetScaler Console génère automatiquement des formulaires d'interface utilisateur utilisés pour renseigner les paramètres du StyleBook lorsque la configuration est effectuée à l'aide de l'interface graphique de NetScaler Console. Les auteurs de StyleBook n'ont pas besoin d'apprendre un nouveau langage d'interface graphique ni de créer séparément des pages et des formulaires d'interface utilisateur.
- **Piloté par API** : Toutes les opérations de configuration sont prises en charge à l'aide de l'interface graphique de NetScaler Console ou via des API REST. Les API peuvent être utilisées en mode synchrone ou asynchrone. En plus des tâches de configuration, les API StyleBooks vous permettent également de découvrir le schéma (description des paramètres) de tout StyleBook au moment de l'exécution.

Vous pouvez utiliser un StyleBook pour créer plusieurs configurations. Chaque configuration est enregistrée en tant que pack de configuration. Par exemple, imaginez que vous disposez d'un StyleBook qui définit une configuration d'application d'équilibrage de charge HTTP typique. Vous pouvez créer une configuration avec des valeurs pour les entités d'équilibrage de charge et l'exécuter sur une instance NetScaler. Cette configuration est enregistrée en tant que pack de configuration. Vous pouvez utiliser le même StyleBook pour créer une autre configuration avec des valeurs différentes et l'exécuter sur la même instance NetScaler ou sur une instance différente. Un nouveau pack de configuration est créé pour cette configuration. Un pack de configuration est enregistré à la fois sur NetScaler Console et sur l'instance NetScaler sur laquelle la configuration est exécutée.

Vous pouvez soit utiliser les StyleBooks par défaut, fournis avec NetScaler Console, pour créer des configurations pour votre déploiement, soit concevoir vos propres StyleBooks et les importer dans NetScaler Console. Vous pouvez utiliser les StyleBooks pour créer des configurations soit à l'aide de l'interface graphique de NetScaler Console, soit à l'aide d'API.

Ce document contient les informations suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Comment afficher les StyleBooks
- StyleBooks par défaut
- StyleBooks développés pour les applications métier
- StyleBooks personnalisés
- API dans les StyleBooks
- Grammaire des StyleBooks

Catégories de StyleBook

Il existe deux catégories de StyleBook dans NetScaler Console. Ce sont les StyleBooks par défaut et les StyleBooks personnalisés. Qu'il soit par défaut ou personnalisé, un StyleBook est soit un StyleBook public, soit un StyleBook privé. Dans NetScaler Console, vous pouvez afficher tous les StyleBooks présents dans le système, quel que soit leur type ou leur statut de visibilité. Vous pouvez également afficher une représentation graphique de la façon dont les StyleBooks sont connectés les uns aux autres.

Ce document explique les différents types de StyleBook. Il explique également les actions suivantes que vous pouvez effectuer sur les StyleBooks depuis NetScaler Console :

- Télécharger un StyleBook personnalisé et y apporter des modifications, ou créer un StyleBook basé sur un StyleBook existant.
- Masquer les StyleBooks par défaut.
- Supprimer un StyleBook personnalisé de NetScaler Console.
- Ajouter des balises aux StyleBooks.

StyleBooks par défaut et personnalisés

- **Les StyleBooks par défaut** sont les StyleBooks fournis avec NetScaler Console et ils vous permettent de créer des configurations que vous pouvez déployer sur vos instances NetScaler. Vous ne pouvez pas supprimer les StyleBooks par défaut, mais vous pouvez les masquer de l'interface graphique de NetScaler Console.
- **Les StyleBooks personnalisés** sont vos propres StyleBooks que vous avez importés dans NetScaler Console.

Les StyleBooks par défaut et personnalisés peuvent être publics ou privés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks publics et privés

Les StyleBooks à partir desquels vous pouvez créer des packs de configuration peuvent être classés comme StyleBooks **publics**. C'est-à-dire qu'ils sont tous disponibles pour votre utilisation directe afin de créer des configurations à partir de l'interface graphique et des API de NetScaler Console.

Cependant, certains StyleBooks sont utilisés comme blocs de construction pour d'autres StyleBooks. Ces StyleBooks sont marqués comme **privés**. Les StyleBooks privés ne peuvent pas être directement utilisés pour créer un pack de configuration à partir de l'interface graphique de NetScaler Console. Cependant, vous pouvez toujours afficher et visualiser ces StyleBooks sur NetScaler Console. Pour marquer l'un de vos StyleBooks personnalisés comme **privé**, définissez l'attribut privé dans le StyleBook sur **true**. Vous pouvez toujours utiliser les StyleBooks privés pour créer des packs de configuration à l'aide des API de NetScaler Console.

Exemple de StyleBook marqué comme privé

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

private: true
```

Afficher les StyleBooks

Le nombre de StyleBooks, par défaut et privés, augmente dans NetScaler Console. Vous souhaiterez peut-être rechercher le StyleBook particulier auquel vous souhaitez accéder. Vous pouvez également afficher les deux types de StyleBooks séparément.

Dans NetScaler Console, lorsque vous accédez à **Applications** > **StyleBooks**, vous pouvez afficher une liste des StyleBooks présents dans le système.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un StyleBook public par défaut comporte les icônes suivantes sur son panneau :



Alors qu'un StyleBook privé par défaut a une icône qui le déclare comme un StyleBook privé :



Bien que vous puissiez afficher la définition et les dépendances d'un StyleBook privé, vous ne pouvez pas créer de pack de configuration à partir d'un StyleBook privé à l'aide de l'interface graphique. L'objectif principal d'un StyleBook privé est de l'utiliser comme bloc de construction pour un autre StyleBook. L'utilisation des StyleBooks en tant que blocs de construction encourage la réutilisation de modèles de configuration courants.

Un StyleBook public personnalisé a une icône différente, comme le montre l'image suivante :



Alors qu'un StyleBook privé personnalisé apparaît avec cette icône :



En haut à droite de la page, vous pouvez voir une option pour sélectionner le type de StyleBooks à afficher. Il existe trois options : tous les StyleBooks, les StyleBooks publics ou les StyleBooks privés. Cliquez sur l'une des options.



Vous pouvez également rechercher un StyleBook particulier en cliquant sur l'icône de recherche. Vous pouvez rechercher par nom, espace de noms et attributs de version ou une combinaison de ces options. L'opération de recherche n'est pas sensible à la casse.



Télécharger des StyleBooks personnalisés

Pour télécharger les StyleBooks personnalisés depuis NetScaler Console, accédez à **Applications** > **StyleBooks** > **Configurations**. Dans la liste des StyleBooks affichés dans le panneau de droite, cochez l'option pour télécharger les StyleBooks définis par l'utilisateur. Cliquez sur **Télécharger**. Si le StyleBook a des StyleBooks personnalisés dépendants, vous pouvez inclure les StyleBooks dépendants dans le bundle téléchargé.

REMARQUE :

Vous pouvez télécharger des StyleBooks personnalisés marqués comme publics ou privés.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous ne pouvez pas télécharger les StyleBooks par défaut. Vous pouvez consulter leurs définitions et leurs dépendances. Pour ce faire, cliquez sur les liens **Afficher la définition** et **Afficher les dépendances** dans le panneau StyleBook.

Mettre à jour un StyleBook personnalisé

Vous pouvez mettre à jour les définitions de StyleBook personnalisées directement depuis l'interface graphique de NetScaler Console. Cela vous permet d'apporter des modifications au StyleBook sans changer sa version. Vous pouvez également mettre à jour les définitions importées à partir d'un bundle StyleBook.

IMPORTANT :

- Avant de mettre à jour la définition du StyleBook depuis l'interface graphique de NetScaler Console, assurez-vous que la définition du StyleBook n'a pas de StyleBooks dépendants.
- Vous pouvez mettre à jour une définition de StyleBook qui contient des packs de configuration.
- Assurez-vous que la définition du StyleBook est rétrocompatible. Tous les paramètres du StyleBook existant sont alors conservés dans le StyleBook mis à jour et les paramètres ajoutés apparaissent comme facultatifs.

1. Accédez à **Applications > Configuration > StyleBooks**.
2. Sélectionnez l'onglet **StyleBooks personnalisés**.
3. Sélectionnez **Mettre à jour la définition** sur le StyleBook que vous souhaitez mettre à jour.
4. Mettez à jour la définition selon les besoins et cliquez sur **Mettre à jour**.

   
5. Actualisez la page pour voir les dernières modifications.

Supprimer les StyleBooks personnalisés

Vous pouvez également supprimer un StyleBook personnalisé en cliquant sur le bouton **Supprimer**. Une fenêtre contextuelle vous invite à confirmer si vous souhaitez supprimer le StyleBook de NetScaler Console. Si le StyleBook utilise d'autres StyleBooks personnalisés, vous pouvez choisir de supprimer ces StyleBooks en cochant la case.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Ne supprimez pas un StyleBook personnalisé s'il a des StyleBooks dépendants dans NetScaler Console. Sinon, cela casserait les StyleBooks existants.

Afficher les dépendances de StyleBook

Une caractéristique importante et puissante des StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Vous pouvez importer un StyleBook dans un autre StyleBook. Un StyleBook importé est déclaré comme un type et est utilisé par les composants ou les paramètres du second StyleBook. Vous pouvez étudier les StyleBooks par défaut existants dans NetScaler Console pour apprendre comment un StyleBook peut être construit sur un autre StyleBook.

NetScaler Console vous permet d'afficher une représentation graphique de la façon dont les StyleBooks sont connectés les uns aux autres. Cette représentation est particulièrement utile pour les StyleBooks complexes qui sont construits en utilisant d'autres StyleBooks comme blocs de construction. En examinant le graphique de dépendance, il est possible de voir les relations et les dépendances entre plusieurs StyleBooks.

Un StyleBook utilisé par d'autres StyleBooks ne peut pas être supprimé du système car cela casserait les StyleBooks existants. En utilisant l'affichage du graphique de dépendance, vous pouvez identifier quels StyleBooks empêchent la suppression d'un StyleBook.

Pour afficher les dépendances de StyleBook

Dans NetScaler Console, accédez à **Applications** > **StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console. Faites défiler vers le bas et trouvez votre StyleBook. La vignette **StyleBook** affiche des liens pour créer une configuration, pour afficher la définition du StyleBook et pour afficher les dépendances du StyleBook. Cliquez sur **Afficher les dépendances**.

Dépendances en amont

L'onglet **Dépendances en amont** vous permet d'afficher les différents StyleBooks par défaut que votre StyleBook utilise. Suivez les flèches pour trouver le StyleBook qu'un StyleBook utilise. Lorsque vous pointez votre souris sur l'une des flèches, la flèche et les StyleBooks qui sont connectés les uns aux autres sont mis en surbrillance. Vous pouvez également cliquer sur les noms des StyleBooks pour afficher la définition de ce StyleBook.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dépendances en aval

L'onglet **Dépendances en aval** vous permet d'afficher graphiquement les StyleBooks qui utilisent votre StyleBook. Si vous suivez les flèches, vous pouvez voir que tous les StyleBooks affichés pointent vers votre StyleBook. Certains StyleBooks peuvent utiliser directement le StyleBook et certains StyleBooks peuvent utiliser le StyleBook via un autre StyleBook.



Auditer la configuration NetScaler par rapport au pack de configuration

Vous pouvez comparer les modifications apportées par un pack de configuration StyleBook à la configuration NetScaler actuelle. Grâce à cette comparaison, vous pouvez effectuer les opérations suivantes :

- Détecter la dérive de configuration entre le pack de configuration StyleBook et la configuration NetScaler.
- Identifier les objets modifiés et supprimés sur le NetScaler qui ne reflètent pas les modifications apportées par le pack de configuration.

Pour comparer les modifications du pack de configuration aux configurations NetScaler, procédez comme suit :

1. Accédez à **Applications** > **StyleBooks** > **Configurations**.
2. Cliquez sur **Audit de configuration**.

   La page **Audit de configuration** affiche les objets créés et audités.

   

Télécharger le bundle de support d'un pack de configuration

Le bundle de support d'un pack de configuration aide l'équipe de support technique de NetScaler® à visualiser, analyser et résoudre les problèmes liés au pack de configuration.

1. Dans **Applications > Configuration > Packs de configuration > Bundles de support**, sélectionnez un pack de configuration. Cliquez sur **Télécharger**.
2. Dans la page **Télécharger le bundle de support**, spécifiez :

   - **Chiffrer les données de configuration à l'aide d'une phrase secrète** - Sélectionnez cette option si vous souhaitez spécifier une phrase secrète pour chiffrer le fichier du bundle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Phrase secrète** - Spécifiez une phrase secrète pour chiffrer le bundle d'exportation. Cette phrase secrète sécurise les données sensibles d'un pack de configuration. La phrase secrète doit comporter au moins 20 caractères.
- **Type de fichier de compression** - Vous pouvez compresser le bundle au format de fichier ZIP ou TGZ.

3. Cliquez sur **Télécharger**.



Créer une balise pour le StyleBook

Vous pouvez ajouter des balises à n'importe quel StyleBook dans NetScaler Console. Les balises sont des paires clé-valeur qui vous permettent de regrouper les StyleBooks selon différents critères. Vous pouvez utiliser ces balises lors de la recherche ou du filtrage des StyleBooks dans NetScaler Console.

Pour ajouter une balise au StyleBook :

1. Accédez à **Applications** > **StyleBooks**.
2. Sélectionnez **Balises** sur le StyleBook auquel vous souhaitez ajouter des balises.

   

   Vous pouvez ajouter des balises à tous les types de StyleBooks.
3. Spécifiez les informations requises **Clé** et **Valeur** qui vous aident à filtrer le StyleBook.

   Par exemple, Key=team et Value=bizdata

   

   Pour ajouter d'autres balises, cliquez sur **+**.
4. Cliquez sur **Créer**.

Pour filtrer les StyleBooks à l'aide de balises dans la barre de recherche, cliquez sur **Balises** et sélectionnez une clé et une valeur dans la liste. Les StyleBooks qui correspondent à la balise spécifiée sont affichés.



Voici un exemple de recherche pour les StyleBooks qui ont une balise où `key=team` et `value=bizdata` :



Vous pouvez associer les balises StyleBook à son pack de configuration. Ainsi, vous pouvez rechercher les packs de configuration en utilisant les balises StyleBook elles-mêmes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque vous créez un pack de configuration, utilisez l'une des options suivantes dans la section **Association de balises** :

- **Associer toutes les balises StyleBook présentes et futures à la configuration** – Cette option associe toutes les balises StyleBook à un pack de configuration. Elle garantit également l'association des nouvelles balises que vous pourriez ajouter aux StyleBooks à l'avenir.
- **Sélectionner les balises** – Cette option affiche les balises du StyleBook sélectionné. Vous pouvez sélectionner les balises StyleBook requises et les associer à un pack de configuration.



Pour configurer un StyleBook à l'aide de commandes CLI

Si vous souhaitez configurer un StyleBook à l'aide de commandes CLI, procédez comme suit :

- Exécutez la commande `show ns runningConfig` dans NetScaler.
- Dans NetScaler Console, créez une configuration à l'aide de StyleBooks par défaut, de StyleBooks d'application métier ou de StyleBooks personnalisés.
- Exécutez à nouveau la commande `show ns runningConfig` dans NetScaler.

La différence entre les deux sorties affiche les commandes CLI que vous pouvez utiliser pour configurer n'importe quel StyleBook à l'aide de l'interface CLI de NetScaler.

Cloner un StyleBook

En tant qu'administrateurs, vous pouvez créer un doublon d'un StyleBook, ainsi que de ses StyleBooks dépendants. Vous pouvez ensuite utiliser ce bundle pour des personnalisations telles que la mise à jour des sections `parameters` et `components`.

Pour cloner un StyleBook :

1. Accédez à **Applications > Configuration > StyleBooks**.
2. Sélectionnez **Cloner** sur le StyleBook par défaut ou personnalisé que vous souhaitez dupliquer.

   
3. Dans la page **Cloner un StyleBook**, entrez un espace de noms et une version pour le StyleBook et les StyleBooks dépendants. Vous pouvez également choisir les espaces de noms et les versions suggérés.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Le StyleBook cloné et ses StyleBooks dépendants doivent avoir des espaces de noms et des versions différents afin de les différencier des StyleBooks existants. Vous ne pouvez pas utiliser d'espaces de noms NetScaler Console réservés pour les StyleBooks clonés.

4. Cliquez sur **Cloner**. Le package StyleBook cloné est importé dans NetScaler Console et apparaît sur la page **StyleBooks**.

Importer et synchroniser des StyleBooks à partir d'un référentiel externe

Considérez un scénario où vous utilisez des processus CI/CD pour votre développement. Ou, un scénario où vous gérez tout le code source de l'application et les objets de déploiement dans GitHub/GitLab.

Dans le référentiel GitHub/GitLab, vous avez peut-être créé plusieurs StyleBooks pour déployer les configurations NetScaler et gérer ces StyleBooks. Ces StyleBooks sont également requis dans NetScaler Console. Vous pouvez désormais importer directement ces StyleBooks dans NetScaler Console. Vous n'avez pas besoin de les copier manuellement depuis GitHub/GitLab, puis de les télécharger dans NetScaler Console, ni de synchroniser manuellement les fichiers dans NetScaler Console et GitHub/GitLab.

Pour importer des StyleBooks et des packs de configuration, définissez un référentiel dans NetScaler Console qui représente un référentiel GitHub/GitLab. Fournissez l'URL du référentiel GitHub/GitLab, votre nom d'utilisateur et le jeton API ou d'accès personnel (PA) créé dans GitHub/GitLab. Cela signifie que seuls les utilisateurs autorisés disposant d'un compte valide dans GitHub/GitLab peuvent importer et synchroniser des StyleBooks.

Vous pouvez importer et synchroniser les types de référentiels suivants :

- **Référentiels accessibles publiquement** - Les référentiels qui sont ouverts au public et peuvent être consultés sur Internet.
- **Référentiels GitLab/GitHub sur site ou privés** - Les référentiels qui sont hébergés en privé et sont généralement accessibles uniquement au sein de l'intranet d'une entreprise. Pour ces référentiels, vous devez sélectionner un agent NetScaler pendant le processus d'enregistrement. L'agent NetScaler agit comme un proxy pour accéder aux référentiels au sein de l'intranet de l'entreprise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir créé le référentiel, vous pouvez synchroniser NetScaler Console avec votre référentiel GitHub/GitLab. NetScaler Console se connecte à GitHub/GitLab et importe les StyleBooks trouvés dans ce référentiel. NetScaler Console valide ensuite les StyleBooks et les ajoute à la liste des StyleBooks dans NetScaler Console. Les StyleBooks ne sont pas ajoutés à NetScaler Console s'ils échouent à la validation. Corrigez les erreurs et validez les versions mises à jour dans votre référentiel GitHub/GitLab. Plus tard, vous pourrez essayer de les importer ou de les synchroniser à nouveau dans NetScaler Console.

REMARQUE

- Les fichiers StyleBooks peuvent être importés et synchronisés depuis n'importe quelle branche d'un référentiel GitHub/GitLab.
- Vous pouvez également importer et synchroniser des StyleBooks qui ont des StyleBooks dépendants associés.
- La synchronisation des StyleBooks à partir d'un référentiel GitHub/GitLab doit être initiée manuellement depuis l'interface graphique ou l'API de NetScaler Console. C'est-à-dire que, actuellement, l'importation et la synchronisation des StyleBooks ne se produisent pas automatiquement en fonction de l'activité de commit de GitHub/GitLab.

Ajouter un référentiel et importer des StyleBooks depuis un référentiel externe

Avant de commencer, assurez-vous d'avoir un compte valide dans GitHub/GitLab.

Vous pouvez importer des fichiers StyleBook dans NetScaler Console depuis n'importe quel dossier du référentiel GitHub/GitLab.

1. Dans NetScaler Console, accédez à **Applications** > **StyleBooks** > **Référentiels**.
2. Cliquez sur **Ajouter**. Dans la fenêtre **Ajouter un référentiel**, saisissez les paramètres suivants :

   - **Nom**. Saisissez le nom du référentiel. Ce nom peut être identique à celui du référentiel dans GitHub/GitLab ou différent.
   - **URL du référentiel** - Saisissez l'URL du référentiel GitHub/GitLab.

     Vous pouvez spécifier une URL d'entreprise GitHub/GitLab. Cela vous aide à importer ou synchroniser des StyleBooks et des packs de configuration à partir de comptes d'entreprise GitHub/GitLab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Est-ce une URL privée ?** - Si le référentiel est un référentiel GitLab/GitHub sur site ou privé, cochez cette case, puis sélectionnez un **Agent**.
- **Nom d'utilisateur et mot de passe**. Saisissez le nom d'utilisateur et le mot de passe avec lesquels vous accédez au compte GitHub/GitLab.

REMARQUE

Vous pouvez également fournir le jeton API à la place d'un mot de passe. Les jetons API peuvent être utilisés à la place d'un mot de passe pour GitHub/GitLab via HTTPS. Pour plus d'informations sur la création de jetons API/PA pour votre référentiel GitHub/GitLab, consultez la documentation GitHub/GitLab sur la création de jetons d'accès personnels.

3. Cliquez sur **Créer**.



Le référentiel est créé dans NetScaler Console.

4. Pour importer ou synchroniser des StyleBooks, sélectionnez le référentiel dans la page **Référentiels**, puis cliquez sur **Synchroniser**.

Les autres actions que vous pouvez utiliser ici sont :

- **Modifier**. Vous pouvez modifier l'URL du référentiel, le nom d'utilisateur et le mot de passe (ou le jeton d'API).
- **Supprimer**. Vous pouvez supprimer le référentiel ainsi que tous les StyleBooks présents dans NetScaler Console qui ont été importés précédemment depuis ce référentiel GitHub/GitLab.

REMARQUE

Vous ne pouvez pas supprimer un référentiel de NetScaler Console s'il contient des StyleBooks auxquels des ConfigPacks sont associés. Tout d'abord, supprimez tous les packs de configuration de ces StyleBooks. Vous pourrez ensuite supprimer le référentiel de NetScaler Console pour nettoyer les StyleBooks de ce référentiel.

- **Réinitialiser**. Vous pouvez supprimer tous les StyleBooks dans NetScaler Console synchronisés à partir de ce référentiel sans réellement supprimer l'entrée du référentiel de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Lister les fichiers**. Vous pouvez voir une liste de tous les StyleBooks présents dans NetScaler Console qui proviennent du référentiel GitHub/GitLab.

Étapes pour importer des StyleBooks et des packs de configuration depuis GitHub/GitLab

Une fois les prérequis remplis, suivez les étapes pour importer des StyleBooks et des packs de configuration depuis un référentiel GitHub/GitLab :

1. Facultatif, ajoutez un référentiel si vous ne l'avez pas déjà fait.
2. Sélectionnez le référentiel dans la page Référentiels.
3. Cliquez sur **Synchroniser**.

Utiliser les StyleBooks par défaut

Un ensemble de StyleBooks par défaut est fourni avec NetScaler Console. Lorsque vous utilisez un StyleBook par défaut, vous devez spécifier des valeurs pour les paramètres du StyleBook et sélectionner les adresses IP des instances NetScaler sur lesquelles vous souhaitez exécuter la configuration. Après avoir soumis la configuration, NetScaler Console valide les valeurs de paramètres que vous avez spécifiées, crée un graphique de la configuration, se connecte aux instances NetScaler et exécute la configuration sur les instances.

Pour créer une configuration à partir d'un StyleBook par défaut

1. Accédez à **Applications** > **Configurations > StyleBooks**. La page StyleBooks affiche tous les StyleBooks dans NetScaler Console. Cette liste inclut les StyleBooks par défaut et personnalisés. Vous pouvez taper le nom du StyleBook dans le champ de recherche et appuyer sur la touche **Entrée**. Sinon, vous pouvez faire défiler la liste pour trouver le StyleBook.
2. Cliquez sur **Créer une configuration**. Spécifiez les valeurs requises pour les paramètres.

   REMARQUE :

   Les paramètres de configuration et les valeurs peuvent différer en fonction du StyleBook choisi.

3. Sous **Instances cibles**, cliquez et sélectionnez l'adresse IP de l'instance NetScaler sur laquelle vous souhaitez exécuter la configuration. Si vous souhaitez exécuter cette configuration sur plusieurs instances, cliquez sur « + » pour ajouter d'autres instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si l'option **Demander les informations d'identification pour la connexion à l'instance** est activée dans **NetScaler Console** > **Paramètres > Modifier les paramètres système** > **Modifier les paramètres système**, il vous sera demandé vos informations d'identification d'instance NetScaler lorsque vous exécuterez les configurations sur les instances NetScaler sélectionnées. Sinon, NetScaler Console utilise les informations d'identification d'instance stockées dans le profil d'instance pour se connecter à l'instance.

Pour activer **Demander les informations d'identification pour les opérations StyleBook**, suivez ces étapes :

a. Accédez à **Paramètres > Administration**.

b. Sur la page **Administration système**, sous **Configuration système**, sélectionnez **Système, Fuseau horaire, URL autorisées et Paramètres de l'agent**.

c. Sur la page **Configurations système**, sous **Paramètres système**, sélectionnez **Demander les informations d'identification pour la connexion à l'instance** et **Demander les informations d'identification pour les opérations StyleBook**.

d. Cliquez sur **Enregistrer**.

À partir de la version 14.1 build 25.x, vous pouvez fournir les informations d'identification pour toutes les instances NetScaler sélectionnées.

Lorsque vous choisissez deux instances NetScaler ou plus et sélectionnez **Utiliser les mêmes informations d'identification pour toutes les instances**, cela vous permet d'appliquer les mêmes informations d'identification aux instances NetScaler sélectionnées.

Si vous souhaitez tester ou valider votre configuration avant de l'exécuter sur l'instance NetScaler, sélectionnez **Exécution à blanc**, puis cliquez sur **Créer**. Si votre configuration est valide, les objets créés sur la base des valeurs que vous avez fournies s'affichent.

4. Décochez la case **Exécution à blanc** et cliquez sur **Créer** pour créer la configuration et l'exécuter sur l'instance NetScaler. La configuration StyleBook que vous avez créée apparaît dans la liste des configurations, comme illustré ci-dessous.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

Vous pouvez maintenant examiner, mettre à jour ou supprimer ce pack de configuration à l'aide de NetScaler Console.

StyleBook de pare-feu d'application Web

NetScaler Web App Firewall est un pare-feu d'application Web (WAF) qui protège les applications et les sites Web contre les attaques connues et inconnues, y compris toutes les menaces de la couche application et les menaces zero-day.

NetScaler Console fournit désormais un StyleBook par défaut avec lequel vous pouvez créer plus facilement une configuration de pare-feu d'application sur les instances NetScaler.

Déploiement des configurations de pare-feu d'application

La tâche suivante vous aide à déployer une configuration d'équilibrage de charge, ainsi que le pare-feu d'application et la politique de réputation IP sur les instances NetScaler de votre réseau d'entreprise.

Pour créer une configuration d'équilibrage de charge avec les paramètres du pare-feu d'application :

1. Dans NetScaler Console, accédez à **Applications** > **Configurations** > **StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console. Faites défiler vers le bas et recherchez le StyleBook d'équilibrage de charge HTTP/SSL avec politique de pare-feu d'application et politique de réputation IP. Vous pouvez également rechercher le StyleBook en tapant le nom comme `lb-appfw`. Cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.

2. Saisissez les valeurs des paramètres suivants :

   - **Nom de l'application équilibrée en charge**. Nom de la configuration équilibrée en charge avec pare-feu d'application à déployer dans votre réseau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Adresse IP virtuelle de l'application équilibrée en charge**. Adresse IP virtuelle à laquelle l'instance NetScaler reçoit les requêtes client.
- **Port virtuel de l'application équilibrée en charge**. Le port TCP à utiliser par les utilisateurs pour accéder à l'application équilibrée en charge.
- **Protocole de l'application équilibrée en charge**. Sélectionnez le protocole frontal dans la liste.
- **Protocole du serveur d'applications**. Sélectionnez le protocole du serveur d'applications.



3. En option, vous pouvez activer et configurer les **Paramètres avancés de l'équilibreur de charge**.



4. En option, vous pouvez également configurer un serveur d'authentification pour authentifier le trafic du serveur virtuel d'équilibrage de charge.



5. Cliquez sur « + » dans la section Adresses IP et ports du serveur pour créer des serveurs d'applications et les ports sur lesquels ils peuvent être accessibles.



6. Vous pouvez également créer des noms de domaine complets (FQDN) pour les serveurs d'applications.



7. Vous pouvez également spécifier les détails du certificat SSL.



8. Vous pouvez également créer des moniteurs dans l'instance NetScaler cible.



9. Pour configurer un pare-feu d'application sur le serveur virtuel, activez les paramètres WAF.

   Assurez-vous que la règle de stratégie du pare-feu d'application est vraie si vous souhaitez appliquer les paramètres du pare-feu d'application à tout le trafic sur ce VIP. Sinon, spécifiez la règle de stratégie NetScaler pour sélectionner un sous-ensemble de requêtes auxquelles appliquer les paramètres du pare-feu d'application. Ensuite, sélectionnez le type de profil à appliquer - HTML ou XML.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Vous pouvez éventuellement configurer des paramètres détaillés de profil de pare-feu d'application en activant la case à cocher Paramètres de profil de pare-feu d'application.
11. En option, si vous souhaitez configurer des signatures de pare-feu d'application, entrez le nom de l'objet de signature créé sur l'instance NetScaler où le serveur virtuel doit être déployé.

    REMARQUE :

    Vous ne pouvez pas créer d'objet de signature à l'aide de ce StyleBook.

12. Ensuite, vous pouvez également configurer d'autres paramètres de profil de pare-feu d'application tels que les paramètres StartURL, les paramètres DenyURL et d'autres.

    Pour plus d'informations sur le pare-feu d'application et les paramètres de configuration, consultez Pare-feu d'application.

13. Dans la section **Instances cibles**, sélectionnez l'instance NetScaler sur laquelle déployer le serveur virtuel d'équilibrage de charge avec le pare-feu d'application.

    REMARQUE :

    Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

14. Vous pouvez également activer la **vérification de la réputation IP** pour identifier l'adresse IP qui envoie des requêtes indésirables. Vous pouvez utiliser la liste de réputation IP pour rejeter préventivement les requêtes provenant d'une IP ayant une mauvaise réputation.
15. Cliquez sur **Créer** pour créer la configuration sur les instances NetScaler sélectionnées.

    CONSEIL

    Nous vous recommandons de sélectionner **Exécution à blanc** pour vérifier les objets de configuration qui doivent être créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

    Lorsque la configuration est créée avec succès, le StyleBook crée le serveur virtuel d'équilibrage de charge, le serveur d'applications, les services, les groupes de services, les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

étiquettes de pare-feu d'application, les stratégies de pare-feu d'application requis, et les lie au serveur virtuel d'équilibrage de charge.

La figure suivante montre les objets créés dans chaque serveur :



16. Pour afficher le Pack de configuration créé sur NetScaler Console, accédez à **Applications** > **Configurations**.



Masquer tous les StyleBooks par défaut

NetScaler Console répertorie tous les StyleBooks présents dans le système de dossiers NetScaler Console. La liste des StyleBooks comprend des StyleBooks par défaut et personnalisés qui peuvent être à la fois privés et publics. En tant qu'administrateur, vous souhaiterez peut-être masquer tous les StyleBooks par défaut. Vous pouvez autoriser vos utilisateurs à afficher et à accéder uniquement aux StyleBooks personnalisés créés par vous ou par les utilisateurs.

NetScaler Console vous permet d'afficher vos StyleBooks personnalisés et de masquer tous les StyleBooks par défaut fournis avec NetScaler Console. Une nouvelle option d'interface graphique est fournie où vous pouvez masquer tous les StyleBooks par défaut.

Pour masquer tous les StyleBooks par défaut :

1. Dans NetScaler Console, accédez à **Applications** > **Configurations > Paramètres**.
2. La page **Paramètres** affiche des informations indiquant si les StyleBooks par défaut sont visibles par les utilisateurs ou non.
3. Pour masquer les StyleBooks par défaut, cliquez sur l'icône de modification en haut à droite.
4. Sur la page **Configurer les paramètres StyleBook**, sélectionnez l'option **Masquer les StyleBooks par défaut**.
5. Cliquez sur **OK**.



La page **Configurer les paramètres StyleBook** est toujours visible pour les utilisateurs si vous n'avez pas choisi de masquer la page à l'aide de la fonctionnalité RBAC. Les utilisateurs pourraient toujours avoir la possibilité de démasquer les StyleBooks par défaut.

Pour masquer la page **Configurer les paramètres StyleBook**, vous devez créer une stratégie et attribuer cette stratégie aux utilisateurs qui ne devraient pas voir les StyleBooks par défaut.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour créer une stratégie RBAC :

1. Dans NetScaler Console, accédez à **Compte** \> **Administration des utilisateurs** \> **Stratégies d'accès**.
2. Cliquez sur **Ajouter** pour créer une stratégie.
3. Saisissez le nom de la stratégie.
4. Dans la section **Autorisations**, assurez-vous que sous **Tout** > **Applications** > **Configuration** > **Paramètres** n'est pas sélectionné, puis cliquez sur **OK**.

Après avoir créé des stratégies, vous devez créer des rôles, lier chaque rôle à une ou plusieurs stratégies et attribuer des rôles à des groupes d'utilisateurs. Pour en savoir plus sur l'association de stratégies aux utilisateurs, consultez Configuration du contrôle d'accès basé sur les rôles.

StyleBook d'analyse Prometheus

Vous pouvez exporter des métriques de NetScaler vers Prometheus en créant un profil d'analyse dans NetScaler et en spécifiant le fichier de schéma. Dans les StyleBooks, vous pouvez utiliser le StyleBook `Prometheus TimeSeries Analytics Configuration` et exécuter la configuration sur toutes les instances gérées.

Prérequis

Assurez-vous que les instances NetScaler gérées sont en version **13.1 build 39-27 ou ultérieure**.

Pour configurer à l'aide du StyleBook `Prometheus TimeSeries Analytics Configuration` :

1. Accédez à **Applications** > **Configurations** > **StyleBooks**, recherchez le StyleBook en tapant le nom `Prometheus TimeSeries Analytics Configuration`, puis cliquez sur **Créer une configuration**.
2. Dans **Détails du pack de configuration** :
   a. Spécifiez le nom du profil d'analyse. Pour plus d'informations, consultez Configurer le collecteur de métriques.
   b. **Fichier de schéma de compteur** :
      - Si vous souhaitez conserver le schéma par défaut, vous pouvez ignorer cette étape.
      - Si vous souhaitez utiliser le schéma personnalisé, téléchargez le fichier de schéma que vous avez modifié avec les paramètres. Dans NetScaler, un fichier de référence `reference_schema.json` avec tous les compteurs pris en charge est disponible sous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

le chemin `/var/metrics_conf/`. Vous pouvez utiliser un client FTP pour copier le fichier en local.

3. Dans **Instances cibles**, sélectionnez les instances ou le groupe d'instances sur lesquels vous souhaitez exécuter la configuration.
4. Dans **Association de balises**, associez toutes les balises StyleBook actuelles et futures à la configuration.

   Cette option associe toutes les balises StyleBook à un pack de configuration. Elle garantit également l'association des nouvelles balises que vous pourriez ajouter aux StyleBooks à l'avenir.

   REMARQUE

   .

   Cliquez sur **Exécution à blanc** pour afficher les résultats qui sont créés, modifiés ou supprimés des instances NetScaler®.

5. Cliquez sur **Créer** pour exécuter la configuration.

Migrer la configuration d'application NetScaler® à l'aide du générateur de configuration StyleBooks

Le générateur de configuration StyleBooks est utilisé pour créer un StyleBook de configuration d'application à partir d'une configuration NetScaler existante. Cette fonctionnalité automatise également la migration de la configuration d'application d'une instance NetScaler vers une autre instance.

L'utilisation du générateur de configuration vous permet de rationaliser le processus de création d'un StyleBook personnalisé, le rendant facile même si vous n'avez pas une compréhension approfondie de la grammaire et des constructions StyleBook. Dans le cas contraire, une familiarité avec la grammaire et les constructions StyleBook est requise pour créer un StyleBook.

Le générateur de configuration crée également un pack de configuration dans lequel la configuration d'une instance NetScaler peut être dupliquée vers une autre instance NetScaler. La source de configuration initiale peut être l'une des suivantes :

- **Une instance NetScaler :** Spécifiez l'instance où la configuration d'application que vous souhaitez dupliquer est disponible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le générateur de configuration convertit la configuration NetScaler en un StyleBook et un pack de configuration même si vous ne spécifiez pas l'instance cible. Vous pouvez ultérieurement utiliser ce pack de configuration pour migrer la configuration NetScaler vers d'autres instances NetScaler.

- **Un ensemble de commandes CLI :** Collez la configuration depuis `ns.conf` ou `Application config`.
- **Télécharger le fichier de configuration :** Téléchargez une configuration depuis votre machine locale.

Le générateur de configuration identifie la liste des applications distinctes intégrées dans la configuration source. Lorsque vous sélectionnez la configuration d'application qui vous intéresse, le générateur de configuration extrait l'ensemble des commandes CLI pour l'application sélectionnée. Ces commandes CLI sont extraites de la configuration source. Il identifie également les attributs de déploiement et de configuration qui pourraient nécessiter votre saisie.

- **Informations de déploiement d'application** - Vous pouvez afficher et modifier l'adresse IP et le port des serveurs virtuels, des services, des membres de groupes de services à partir de la configuration d'origine. Vous pouvez également afficher et modifier l'état et l'ARP d'un serveur virtuel.
- **Attributs de configuration** - Ces attributs peuvent être des mots de passe ou des certificats spécifiés dans la configuration source.

Après avoir spécifié les informations nécessaires, commencez à migrer ou à dupliquer la configuration d'application sur une instance NetScaler cible.

Une fois la création et la migration de l'application terminées, un pack de configuration est créé dans NetScaler Console avec son StyleBook correspondant. Ce pack de configuration représente la configuration d'application sur l'instance NetScaler cible. Pour afficher le pack de configuration créé, accédez à **Applications** > **StyleBooks** > **Configurations**.

Partage d'entités de configuration entre les configurations migrées

Vous pouvez réutiliser les entités de configuration lors de la migration de configurations à l'aide de l'utilitaire de migration de configuration. Les migrations ultérieures réutilisent avec succès les entités de configuration existantes. Auparavant, la migration des configurations échouait avec une erreur **La ressource existe déjà** lors de la migration de deux configurations partageant certaines entités de configuration. Cette option simplifie le flux de travail de migration en permettant la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

réutilisation des entités de configuration dans les scénarios où elles sont utilisées dans plusieurs configurations.

Fonctionnalités NetScaler prises en charge

Le Générateur de configuration StyleBook reconnaît et prend en charge les fonctionnalités NetScaler suivantes dans la configuration source :

- Analyse
- AppFlow®
- Configuration de la qualité d'expérience au niveau de l'application (AppQoE)
- Authentification et autorisation
- Audit
- Gestion des bots
- Redirection de cache
- Commutation de contenu
- DNS
- Optimisation du frontend
- Compression HTTP
- Mise en cache intégrée
- Équilibrage de charge
- Surveillance
- Protocole QUIC
- Limitation de débit
- Répondeur
- Réécriture
- Déchargement SSL
- Débordement
- Gestion du trafic
- Transformation d'URL
- Pare-feu d'applications Web (WAF)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Créer un StyleBook pour migrer la configuration d'application NetScaler

La procédure suivante permet de créer un StyleBook qui migre la configuration d'application NetScaler dans NetScaler Console :

1. Accédez à **Applications** > **Configuration** > **Packs de configuration**.
2. Cliquez sur **Migrer la configuration NetScaler**.
3. Cliquez sur **Démarrer**.
4. Dans **Spécifier la configuration**, choisissez l'une des sources de configuration suivantes :

   - **Importer depuis un NetScaler** :

     - **Instance NetScaler source** - Sélectionnez une instance NetScaler à partir de laquelle vous souhaitez migrer ou dupliquer la configuration de l'application. Cliquez sur **OK**.

   - **Importer à l'aide des commandes CLI** - Collez la configuration à partir d'un fichier de configuration.
   - **Télécharger le fichier de configuration** - Cliquez sur **Parcourir** pour sélectionner un fichier de configuration depuis votre machine locale.

   Instance cible - Sélectionnez une instance NetScaler ou un groupe Autoscale vers lequel vous souhaitez migrer ou dupliquer la configuration de l'application. Cliquez sur **OK**.

   Cliquez sur **Suivant**.
5. Dans **Configuration de la politique avancée**, en fonction de votre configuration, les scénarios suivants se produisent :

   - Toutes les politiques classiques existantes dans la configuration sont converties en politiques avancées avec succès et sans erreurs. Examinez la configuration mise à jour et sélectionnez l'accusé de réception. Cliquez sur **Suivant**.
   - Toutes les politiques classiques existantes dans la configuration sont converties en politiques avancées avec succès, mais avec des erreurs. Examinez et corrigez les erreurs. Cliquez sur **Précédent**.
   - S'il n'y a pas de politiques classiques, la configuration n'est pas mise à jour. Cliquez sur **OK** pour continuer.

6. Dans **Définir l'application**,

   a. Dans **Nom de l'application**, spécifiez le nom de l'application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Sélectionnez les serveurs virtuels que vous souhaitez migrer.

c. Cliquez sur **Suivant**.

7. Dans **Configuration de l'application**, examinez les commandes de l'application. Ces commandes sont spécifiques à la configuration d'application sélectionnée.

   Activez le **Visualiseur** pour afficher les configurations d'application et leurs entités associées. Le Visualiseur vous permet de voir comment les différents composants sont connectés et vous aide dans votre compréhension et votre prise de décision pendant le processus de migration.

   

   Avec le Visualiseur, vous pouvez :

   - Afficher la hiérarchie des actions et des stratégies associées à un serveur
   - Passez la souris sur un serveur pour obtenir des descriptions détaillées du serveur, y compris les stratégies et les actions liées à un serveur
   - Agrandir et réduire la vue à l'aide du curseur de zoom
   - Réduire ou développer la hiérarchie en cliquant sur le symbole moins (-) ou plus (+) sur une entité

   Cliquez sur **Suivant**.

8. Dans **Informations de déploiement de l'application**, vous pouvez afficher et modifier l'adresse IP, le port, l'état et l'ARP des serveurs virtuels, des services et des membres du groupe de services.

   

   Dans la page **Détails**, vous pouvez modifier l'adresse IP, le port, l'état et le statut ARP de l'entité NSIP.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- L'état de l'entité NSIP pour l'IP du serveur virtuel détermine l'état initial de l'ARP.
- Si l'entité NSIP pour l'IP du serveur virtuel est déjà configurée sur le NetScaler cible, vous ne pouvez pas modifier l'état ARP du serveur virtuel.
- La modification de l'état ARP d'un serveur virtuel modifie l'état ARP de tous les serveurs virtuels ayant la même adresse IP. La modification de l'état du serveur virtuel n'affecte que le serveur virtuel associé.
- L'ARP n'est pas applicable aux serveurs virtuels basés sur des modèles d'IP.
- Si l'état NSIP pour l'IP du serveur virtuel est désactivé dans la configuration source, l'ARP est également automatiquement désactivé, et vous ne pouvez pas modifier l'ARP.

L'onglet **Informations de déploiement d'application** n'apparaît pas si les instances source et cible sont identiques.

9. Dans **Informations de déploiement d'authentification/réseau**, vous pouvez afficher et modifier les attributs des serveurs d'authentification et des profils réseau, si disponibles.

   a. Dans **Informations de déploiement d'authentification**, sélectionnez le serveur d'authentification requis et modifiez l'adresse IP, l'IP du serveur, le nom du serveur et le numéro de port des serveurs.

   b. Dans **Informations NetProfile**, sélectionnez le profil réseau requis et modifiez les détails de **NetProfile** et **IPSET**.

   REMARQUE :

   Les modifications d'adresse NSIP effectuées à cette étape sont prises en compte pour la migration finale et les configurations des étapes précédentes sont mises à jour pour refléter les changements.

10. Dans **Fichiers de ressources/Secrets**, téléchargez les certificats et les clés pour déchiffrer les mots de passe et les certificats. Cliquez sur **Suivant**.
11. Dans **Configuration globale**, affichez les différences dans les paramètres de configuration globale entre la source et la cible. Examinez la configuration à appliquer sur la cible et sélectionnez l'accusé de réception. Cliquez sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Dans **Migrer**, affichez les détails du StyleBook. Cliquez sur **Migrer**.

    REMARQUE :

    Par défaut, NetScaler Console gère le pack de configuration créé lors de la migration d'applications ou de serveurs virtuels vers NetScaler. Décochez la case **Gérer la configuration via NetScaler Console** si vous ne souhaitez pas associer un pack de configuration à la configuration résultante.

13. Dans **Configuration non prise en charge**, affichez toutes les configurations manquantes ou non prises en charge. Pour migrer ces configurations avec succès, vous devez appliquer les configurations manquantes ou non prises en charge séparément sur l'instance cible. Cliquez sur **Suivant**.

Limitations

- Les expressions nommées et `responderhtmlpages` mentionnées dans l'instance source ne sont pas identifiées. Assurez-vous de configurer les expressions nommées et `responderhtmlpages` sur l'instance cible avant la migration.
- Si la source a une configuration pour `servicegroup` et une liaison de moniteur comme suit :

  ```
  bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
  ```

  L'erreur suivante apparaît :

  ```
  CLI Command conversion failed: 100 - No such command [{ "errorcode":
  1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
  ```

  Cette erreur se produit car NetScaler enregistre la liaison entre le groupe de services et le moniteur dans un format non valide. Ce problème est résolu à partir de la version 12.1.52.15 de NetScaler.

StyleBooks d'applications métier

NetScaler Console fournit les StyleBooks qui vous aident à déployer une configuration NetScaler pour des applications métier spécifiques. Pour plus d'informations sur ces StyleBooks, consultez les rubriques suivantes :

- StyleBook SSO Google Apps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StyleBook SSO Office 365
- StyleBook Microsoft Skype Entreprise
- StyleBook Microsoft Exchange
- StyleBook Microsoft SharePoint
- StyleBook de proxy Microsoft ADFS
- StyleBook Oracle e-business

StyleBook SSO Google Apps

Google Apps est une collection d'outils, de logiciels et de produits de cloud computing, de productivité et de collaboration développés par Google. L'authentification unique (SSO) permet aux utilisateurs d'accéder à toutes leurs applications cloud d'entreprise, y compris les administrateurs se connectant à la console d'administration, en se connectant une seule fois pour tous les services à l'aide de leurs informations d'identification d'entreprise.

Le StyleBook SSO Google Apps de NetScaler Console vous permet d'activer l'authentification unique (SSO) pour Google Apps via les instances NetScaler. Le StyleBook configure l'instance NetScaler en tant que fournisseur d'identité SAML pour authentifier les utilisateurs accédant à Google Apps.

L'activation de l'authentification unique (SSO) pour Google Apps dans une instance NetScaler à l'aide de ce StyleBook entraîne les étapes suivantes :

1. Configuration du serveur virtuel d'authentification
2. Configuration d'une stratégie et d'un profil IdP SAML
3. Liaison de la stratégie et du profil au serveur virtuel d'authentification
4. Configuration d'un serveur et d'une stratégie d'authentification LDAP sur l'instance
5. Liaison du serveur et de la stratégie d'authentification LDAP à votre serveur virtuel d'authentification configuré sur l'instance

Détails de la configuration :

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration prend également en charge les versions supérieures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUIT	VERSION MINIMALE REQUISE
NetScaler	Version 11.0, Licence Advanced/Premium

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes ou internes appropriées pour acheminer les requêtes d'authentification vers une adresse IP surveillée par NetScaler.

Déploiement des configurations StyleBook SSO Google apps :

La tâche suivante vous aide à déployer le StyleBook Microsoft SSO Google Apps dans votre réseau d'entreprise.

Pour déployer le StyleBook SSO Google apps

1. Dans NetScaler Console, accédez à **Applications** > **Configurations** > **StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console. Faites défiler vers le bas et recherchez **SSO Google Apps StyleBook**. Cliquez sur **Créer une configuration**.
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.
3. Saisissez les valeurs des paramètres suivants :

    a. **Nom de l'application**. Nom de la configuration SSO Google apps à déployer dans votre réseau.

    b. **Adresse IP virtuelle d'authentification**. Adresse IP virtuelle utilisée par le serveur virtuel d'authentification, d'autorisation et d'audit auquel la stratégie SAML IdP des applications Google est liée.

    c. **Expression de règle SAML**. Par défaut, l'expression de stratégie NetScaler (PI) suivante est utilisée : HTTP.REQ.HEADER("Referrer").CONTAINS("google"). Mettez à jour ce champ avec une autre expression si votre exigence est différente. Cette expression de stratégie correspond au trafic auquel ces paramètres SAML SSO sont appliqués et garantit que l'en-tête Referrer provient d'un domaine Google.

4. La section Paramètres SAML IdP vous permet de configurer votre instance NetScaler en tant que fournisseur d'identité SAML en créant le profil et la stratégie SAML IdP utilisés par le serveur virtuel d'authentification, d'autorisation et d'audit créé à l'étape 3.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Nom de l'émetteur SAML**. Dans ce champ, saisissez le FQDN public de votre serveur virtuel d'authentification. Exemple : `https://<NetScaler Auth VIP>/saml/login`

b. **ID du fournisseur de services (SP) SAML**. (facultatif) Le fournisseur d'identité NetScaler accepte les requêtes d'authentification SAML provenant d'un nom d'émetteur correspondant à cet ID.

c. **URL du service consommateur d'assertions**. Saisissez l'URL du fournisseur de services où le fournisseur d'identité NetScaler doit envoyer les assertions SAML après une authentification utilisateur réussie. L'URL du service consommateur d'assertions peut être initiée sur le site du serveur du fournisseur d'identité ou sur le site du fournisseur de services.

d. Il existe d'autres champs facultatifs que vous pouvez saisir dans cette section. Par exemple, vous pouvez définir les options suivantes :

   i. Profil de liaison SAML (le profil par défaut est « POST »).

   ii. Algorithme de signature pour vérifier/signer les requêtes/réponses SAML (la valeur par défaut est « RSA-SHA1 »).

   iii. Méthode de hachage pour les requêtes/réponses SAML (la valeur par défaut est « SHA-1 »).

   iv. Algorithme de chiffrement (la valeur par défaut est AES256) et autres paramètres.

   REMARQUE

   Nous vous recommandons de conserver les paramètres par défaut, car ils ont été testés et sont compatibles avec Google Apps.

e. Vous pouvez également activer la case à cocher Attributs utilisateur pour saisir les détails de l'utilisateur, tels que :

   i. Nom de l'attribut utilisateur

   ii. Expression NetScaler PI évaluée pour extraire la valeur de l'attribut

   iii. Nom convivial de l'attribut

   iv. Sélectionnez le format de l'attribut utilisateur.

   Ces valeurs sont incluses dans l'assertion SAML émise. Vous pouvez inclure jusqu'à cinq ensembles d'attributs utilisateur dans une assertion émise par NetScaler à l'aide de ce StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Dans la section Paramètres LDAP, entrez les détails suivants pour authentifier les utilisateurs de Google Apps. Pour que les utilisateurs du domaine puissent se connecter à l'instance NetScaler à l'aide de leurs adresses e-mail d'entreprise, vous devez configurer les éléments suivants :

   a. **Base LDAP (Active Directory)**. Entrez le nom de domaine de base du domaine dans lequel résident les comptes d'utilisateurs au sein de l'Active Directory (AD) pour lequel vous souhaitez autoriser l'authentification. Par exemple, `dc=netscaler`, `dc=com`

   b. **DN de liaison LDAP (Active Directory)**. Ajoutez un compte de domaine (en utilisant une adresse e-mail pour faciliter la configuration) qui dispose des droits de navigation dans l'arborescence AD. Par exemple,`cn=Manager,dc=netscaler,dc=com`

   c. **Mot de passe de liaison DN LDAP (Active Directory)**. Saisissez le mot de passe du compte de domaine pour l'authentification.

   d. Voici quelques autres champs que vous devez saisir dans cette section :

      i. Adresse IP du serveur LDAP auquel NetScaler se connecte pour authentifier les utilisateurs

      ii. Nom FQDN du serveur LDAP

      REMARQUE

      Vous devez spécifier au moins l'un des deux éléments ci-dessus : l'adresse IP du serveur LDAP ou le nom FQDN.

      iii. Port du serveur LDAP auquel NetScaler se connecte pour authentifier les utilisateurs (la valeur par défaut est 389).

      iv. Nom d'hôte LDAP. Ceci est utilisé pour valider le certificat LDAP si la validation est activée (par défaut, elle est désactivée).

      v. Attribut de nom d'utilisateur LDAP. L'attribut par défaut utilisé pour extraire les noms d'utilisateur est « sAMAccountName ».

      vi. Autres paramètres LDAP divers facultatifs

6. Dans la section Certificat SSL IdP SAML, vous pouvez spécifier les détails du certificat SSL :

   a. **Nom du certificat**. Saisissez le nom du certificat SSL.

   b. **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local ou sur NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **Format CertKey**. Sélectionnez le format du certificat et des fichiers de clé privée dans la liste déroulante. Les formats pris en charge sont les extensions .pem et .der.

d. **Nom de la clé de certificat**. Saisissez le nom de la clé privée du certificat.

e. **Fichier de clé de certificat**. Sélectionnez le fichier contenant la clé privée du certificat à partir de votre système local ou de NetScaler Console.

f. **Mot de passe de la clé privée**. Si votre fichier de clé privée est protégé par une phrase secrète, saisissez-la dans ce champ.

g. Vous pouvez également activer la case à cocher Paramètres de certificat avancés pour saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

7. Vous pouvez éventuellement sélectionner le certificat CA SSL IdP si le certificat IdP SAML saisi ci-dessus nécessite l'installation d'un certificat public CA sur NetScaler. Assurez-vous de sélectionner « Est un certificat CA » dans les paramètres avancés.
8. Vous pouvez éventuellement sélectionner le certificat SSL SAML SP pour spécifier le certificat SSL Google (clé publique) utilisé pour valider les requêtes d'authentification des applications Google (SAML SP).
9. Cliquez sur **Instances cibles** et sélectionnez la ou les instances NetScaler sur lesquelles déployer cette configuration SSO Google Apps. Cliquez sur **Créer** pour créer la configuration et la déployer sur la ou les instances NetScaler sélectionnées.

REMARQUE

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

Aussi,

CONSEIL

Nous vous recommandons, avant d'exécuter la configuration réelle, de sélectionner **Exécution à blanc** pour confirmer visuellement les objets de configuration créés sur la ou les instances NetScaler cibles par le StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook SSO Office 365

Microsoft Office 365 est une suite d'applications de productivité et de collaboration basées sur le cloud, fournies par Microsoft sur la base d'un abonnement. Elle comprend les applications serveur populaires de Microsoft telles qu'Exchange, SharePoint, Office et Skype Entreprise. L'authentification unique (SSO) permet aux utilisateurs d'accéder à toutes leurs applications cloud d'entreprise :

- Y compris les administrateurs se connectant à la console d'administration
- Connexion unique pour tous les services Microsoft Office 365 à l'aide de leurs informations d'identification d'entreprise.

Le StyleBook SSO Office 365 vous permet d'activer l'authentification unique (SSO) pour Microsoft Office 365 via les instances NetScaler. Vous pouvez désormais configurer l'authentification SAML avec NetScaler en tant que fournisseur d'identité (IdP) SAML et Microsoft Office 365 en tant que fournisseur de services SAML.

L'activation de l'authentification unique (SSO) pour Microsoft Office 365 dans une instance NetScaler à l'aide de ce StyleBook implique les étapes suivantes :

1. Configuration du serveur virtuel d'authentification
2. Configuration d'une stratégie et d'un profil IDP SAML
3. Liaison de la stratégie et du profil au serveur virtuel d'authentification
4. Configuration d'un serveur et d'une stratégie d'authentification LDAP sur l'instance
5. Liaison du serveur et de la stratégie d'authentification LDAP à votre serveur virtuel d'authentification configuré sur l'instance.

Le tableau répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration devrait également fonctionner avec des versions supérieures des mêmes.

PRODUIT	VERSION MINIMALE REQUISE
NetScaler	11.0, licence Advanced/Premium

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées. Ces entrées sont essentielles pour acheminer les requêtes d'authentification vers une adresse IP surveillée par NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les instructions suivantes vous aident à implémenter le StyleBook SSO Office 365 dans votre réseau d'entreprise.

Pour déployer le StyleBook SSO Microsoft Office 365

1. Dans NetScaler Console, accédez à **Applications** > **StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console. Faites défiler vers le bas et recherchez **SSO Office 365 StyleBook**. Cliquez sur **Créer une configuration**.
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.
3. Saisissez les valeurs des paramètres suivants :

   a. **Nom de l'application**. Nom de la configuration SSO Microsoft Office 365 à déployer sur votre réseau.

   b. **Adresse IP virtuelle d'authentification**. Adresse IP virtuelle à utiliser par le serveur virtuel AAA auquel la stratégie SAML IdP de Microsoft Office 365 est liée.

   

4. Dans la section **Paramètres** des **certificats SSL**, saisissez les noms du certificat SSL et de la clé de certificat.

   REMARQUE

   Il ne s'agit pas du certificat du fournisseur de services Office 365. Ce certificat SSL est lié au serveur d'authentification virtuel sur l'instance NetScaler.

5. Sélectionnez les fichiers respectifs dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de la clé privée pour charger des clés privées chiffrées au format PEM.

   

6. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.
7. En option, vous pouvez sélectionner la case à cocher **Certificat CA SSL pour l'IP virtuelle d'authentification** si le certificat SSL nécessite l'installation d'un certificat public CA sur NetScaler. Assurez-vous de choisir « Est un certificat CA » dans la section **Paramètres de certificat avancés** ci-dessus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Dans la section **Paramètres LDAP pour SSO Office 365**, saisissez les détails suivants pour authentifier les utilisateurs d'Office 365. Pour permettre aux utilisateurs de domaine de se connecter à l'instance NetScaler en utilisant leurs adresses e-mail d'entreprise, configurez les éléments suivants :

   - **Base LDAP (Active Directory)**. Saisissez le nom de domaine de base du domaine dans lequel résident les comptes d'utilisateurs au sein de l'Active Directory (AD) pour permettre l'authentification. Par exemple, dc=netscaler®,dc=com
   - **DN de liaison LDAP (Active Directory)**. Ajoutez un compte de domaine (en utilisant une adresse e-mail pour faciliter la configuration) qui a les droits de parcourir l'arborescence AD. Par exemple, cn=Manager,dc=netscaler,dc=com
   - **Mot de passe du DN de liaison LDAP (Active Directory)**. Saisissez le mot de passe du compte de domaine pour l'authentification.
   - Voici quelques autres champs que vous devez saisir dans cette section :
     - Adresse IP du serveur LDAP auquel NetScaler se connecte pour authentifier les utilisateurs.
     - Nom de domaine complet (FQDN) du serveur LDAP.

       REMARQUE

       Vous devez spécifier au moins l'un des deux éléments ci-dessus : l'adresse IP du serveur LDAP ou le nom de domaine complet (FQDN).

     - Port du serveur LDAP auquel NetScaler se connecte pour authentifier les utilisateurs (la valeur par défaut est 389). LDAPS utilise 636.
     - Nom d'hôte LDAP. Le nom d'hôte est utilisé pour valider le certificat LDAP si la validation est activée (par défaut, elle est désactivée).
     - Attribut de nom de connexion LDAP. L'attribut par défaut utilisé pour extraire les noms de connexion est « samAccountname ».
     - Autres paramètres LDAP divers facultatifs.

9. Dans la section **Certificat IdP SAML**, vous pouvez spécifier les détails des certificats SSL utilisés pour l'assertion SAML.

   - **Nom du certificat**. Saisissez le nom du certificat SSL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local.
- **Format de la clé de certificat**. Sélectionnez le format du certificat et des fichiers de clé privée dans la liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.
- **Nom de la clé de certificat**. Saisissez le nom de la clé privée du certificat.
- **Fichier de clé de certificat**. Sélectionnez le fichier contenant la clé privée du certificat depuis votre système local.
- **Mot de passe de la clé privée**. Saisissez la phrase secrète qui protège votre fichier de clé privée.

Vous pouvez également activer la case à cocher **Paramètres avancés du certificat**. Ici, vous pouvez saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

10. Vous pouvez éventuellement sélectionner **Certificat CA SAML IdP** si le certificat SAML IdP saisi ci-dessus nécessite l'installation d'un certificat public CA sur NetScaler. Assurez-vous de sélectionner **Est un certificat CA** dans la section **Paramètres avancés du certificat** ci-dessus.
11. Dans la section **Certificat SAML SP**, saisissez les détails suivants pour le certificat public SSL Office 365. Ce certificat est utilisé par l'instance NetScaler pour vérifier les requêtes d'authentification SAML entrantes.

    - **Nom du certificat**. Saisissez le nom du certificat SSL.
    - **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local.
    - **Format de la clé de certificat**. Sélectionnez le format du certificat et des fichiers de clé privée dans la liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.
    - Vous pouvez également activer la case à cocher **Paramètres avancés du certificat**. Ici, vous pouvez saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

12. La section **Paramètres SAML IdP** vous permet de configurer votre instance NetScaler en tant que fournisseur d'identité SAML en créant le profil et la politique SAML IdP utilisés par le serveur virtuel AAA créé à l'étape 3.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Nom de l'émetteur SAML**. Dans ce champ, saisissez le FQDN public de votre serveur virtuel d'authentification. Exemple : `https://<NetScaler Auth VIP>/saml/login`
- **Expression d'identifiant de nom**. Saisissez l'expression NetScaler qui est évaluée pour extraire le NameIdentifier SAML envoyé dans l'assertion SAML. Exemple : `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
- **Algorithme de signature** : Sélectionnez l'algorithme pour vérifier/signer les requêtes/réponses SAML (la valeur par défaut est « RSA-SHA256 »).
- **Méthode de résumé**. Sélectionnez la méthode de hachage de résumé pour les requêtes/réponses SAML (la valeur par défaut est « SHA256 »).
- **Nom de l'audience**. Saisissez le nom de l'entité ou l'URL qui représente le fournisseur de services (Microsoft Office 365).
- **ID du fournisseur de services (SP) SAML**. (facultatif) Le fournisseur d'identité NetScaler accepte les requêtes d'authentification SAML provenant d'un nom d'émetteur correspondant à cet ID.
- **URL du service consommateur d'assertions**. Saisissez l'URL du fournisseur de services où le fournisseur d'identité NetScaler doit envoyer les assertions SAML après une authentification utilisateur réussie. L'URL du service consommateur d'assertions peut être initiée sur le site du serveur du fournisseur d'identité ou sur le site du fournisseur de services.
- Il existe d'autres champs facultatifs que vous pouvez saisir dans cette section. Par exemple, vous pouvez définir les options suivantes :
  - **Nom de l'attribut SAML**. Nom de l'attribut utilisateur envoyé dans l'assertion SAML.
  - **Nom convivial de l'attribut SAML**. Nom convivial de l'attribut utilisateur envoyé dans l'assertion SAML.
  - **Expression PI pour l'attribut SAML**. Par défaut, l'expression de stratégie NetScaler (PI) suivante est utilisée : HTTP.REQ.USER.ATTRIBUTE(1). Ce champ spécifie le premier attribut utilisateur envoyé par le serveur LDAP (mail) comme attribut d'authentification SAML.
  - Sélectionnez le format de l'attribut utilisateur.

  Ces valeurs sont incluses dans l'assertion SAML émise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONSEIL

Nous vous recommandons de conserver les paramètres par défaut, car ils ont été testés et fonctionnent avec les applications Microsoft Office 365.

13. Cliquez sur **Instances cibles** et sélectionnez la ou les instances NetScaler sur lesquelles déployer cette configuration SSO Microsoft Office 365. Cliquez sur **Créer** pour créer la configuration et la déployer sur la ou les instances NetScaler sélectionnées.

CONSEIL

Nous vous recommandons de sélectionner **Exécution à blanc** avant d'exécuter la configuration réelle, afin de visualiser les objets de configuration créés sur les instances NetScaler cibles par le StyleBook.

StyleBook Microsoft Skype Entreprise

L'application Skype Entreprise 2015 s'appuie sur plusieurs composants externes pour fonctionner. Le réseau Skype Entreprise se compose de divers systèmes, tels que des serveurs et leurs systèmes d'exploitation, des bases de données, des systèmes d'authentification et d'autorisation, des systèmes et infrastructures de réseau, et des systèmes de PBX téléphonique. Skype Entreprise Server 2015 est disponible en deux versions : Standard Edition et Enterprise Edition. La principale différence réside dans la prise en charge des fonctionnalités de haute disponibilité qui ne sont incluses que dans l'Enterprise Edition. Pour implémenter la haute disponibilité, plusieurs serveurs frontaux doivent être déployés dans un pool et les serveurs SQL doivent être mis en miroir.

Un déploiement Enterprise Edition permet la création de plusieurs serveurs avec des rôles différents.

Composants principaux

Les principaux composants de l'application Skype Entreprise 2015 sont :

- Serveurs frontaux
- Serveurs Edge
- Serveurs Director

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Serveurs de base de données (SQL)

Serveurs frontaux

Dans l'application Skype Entreprise, le serveur frontal est le serveur central de votre réseau. Il fournit les liens et les services pour l'authentification des utilisateurs, l'enregistrement, la présence, le carnet d'adresses, la conférence audio/vidéo, le partage d'applications, la messagerie instantanée et la conférence web. Si vous déployez Skype Entreprise 2015 Enterprise Edition, la topologie se compose généralement d'au moins deux serveurs frontaux équilibrés en charge dans un pool frontal avec un serveur de base de données qui héberge l'instance SQL Server contenant la base de données Skype Entreprise.

Serveurs Edge

Le déploiement de serveurs Edge pour Skype Entreprise est nécessaire si des utilisateurs externes qui ne sont pas connectés au réseau interne de votre organisation doivent pouvoir interagir avec des utilisateurs internes. Ces utilisateurs externes peuvent être des utilisateurs distants authentifiés et anonymes, des partenaires fédérés ou d'autres clients mobiles.

Il existe quatre types de rôles dans le serveur Edge de Skype Entreprise :

- Access Edge, qui gère le trafic SIP et authentifie les connexions externes, autorise la connexion à distance et autorise la connexion de fédération
- Conférence Web, qui gère les paquets de conférence de données et permet aux utilisateurs externes d'accéder à Skype Entreprise
- Conférence A/V, qui gère les paquets de conférence A/V et étend l'audio et la vidéo, le partage d'applications et le transfert de fichiers aux utilisateurs externes
- Proxy XMPP, qui gère les paquets XMPP et permet aux serveurs ou clients basés sur XMPP de se connecter à Skype Entreprise.

Serveurs Director

La fonction principale du serveur Director dans Skype Entreprise 2015 est d'authentifier les points de terminaison et de « diriger » les utilisateurs vers le pool qui contient leur compte. Dans Skype Entreprise 2015, bien que le Director soit un rôle entièrement dédié et spécifique sur un serveur autonome, il s'agit d'un serveur facultatif. Cela facilite la sécurité en rendant le déploiement ou la suppression des configurations plus simple.

Les Directors sont très utiles là où plusieurs pools existent, car ils fournissent un point de contact unique pour l'authentification des points de terminaison. De plus, pour les utilisateurs distants, un

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Director sert de saut supplémentaire entre le pool Edge et le pool Front-End, ajoutant une couche de protection supplémentaire contre les attaques.

La figure suivante représente schématiquement le déploiement des serveurs Skype dans le réseau :



Configuration des instances NetScaler dans une entreprise

Le tableau suivant répertorie les adresses IP utilisées dans l'exemple de configuration inclus dans les instructions ci-dessous :

SERVEURS SKYPE ENTREPRISE	ADRESSE IP VIRTUELLE	ADRESSES IP DU SERVEUR	INSTANCE NETSCALER
Serveurs Edge	VIP externe - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	VIP interne - 10.10.10.20	10.10.10.21; 10.10.10.22	
Serveurs frontaux	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Serveur directeur	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

Pour configurer les serveurs frontaux

1. Dans NetScaler Console, accédez à **Applications** > **Configuration**, puis cliquez sur **Créer nouveau**. La page **Choisir un StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console. Faites défiler vers le bas et sélectionnez **Microsoft Skype for Business 2015 StyleBook**. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.
2. Dans la section **Serveur Edge**, entrez les adresses IP virtuelles (VIP) et les adresses IP suivantes de tous les serveurs Edge du réseau.
    a. Adresse VIP externe et adresses IP pour les serveurs Edge qui seront utilisés pour Access Edge, web conferencing Edge et A/V Edge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Adresse VIP interne et adresses IP pour les serveurs Edge qui seront connectés au réseau interne.

c. Deux serveurs Edge externes et deux internes dans votre réseau.

3. Dans la section **Serveur frontal**, entrez l'adresse IP du serveur frontal virtuel (VIP) à créer pour les serveurs frontaux Skype Entreprise. Entrez également les adresses IP de tous les serveurs frontaux Skype Entreprise du réseau.
4. Dans la section **Serveur Director**, entrez l'adresse IP virtuelle (VIP) pour les serveurs Director à créer pour l'application Skype Entreprise. Entrez également les adresses IP de tous les serveurs Director Skype Entreprise du réseau. Créez au moins deux serveurs Director pour la haute disponibilité.
5. La section **Paramètres avancés** répertorie tous les ports par défaut configurés sur les instances NetScaler pour les trois serveurs Skype.

Le tableau suivant vous fournit une liste de tous les ports et protocoles par défaut :

ÉTIQUETTE	PORT	PROTOCOLE	DESCRIPTION
Port HTTP	80	HTTP	Utilisé pour la communication des serveurs frontaux vers les FQDN de la ferme web lorsque HTTPS n'est pas utilisé.
Port HTTPS	443	HTTPS	Utilisé pour la communication des serveurs frontaux vers les FQDN de la ferme web.
Port interne AutoDiscover	4443	HTTPS	HTTPS (depuis le proxy inverse) et communications inter-pools HTTPS frontales pour la connexion AutoDiscover.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTIQUETTE	PORT	PROTOCOLE	DESCRIPTION
Port RPC	135	DCOM et appel de procédure distante (RPC)	Utilisé pour les opérations basées sur DCOM telles que le déplacement d'utilisateurs, la synchronisation du réplicateur d'utilisateurs et la synchronisation du carnet d'adresses.
Port SIP	5061	TCP (TLS)	Utilisé par les serveurs frontaux pour toutes les communications SIP internes.
Port SIP Focus	444	HTTPS, TCP	Utilisé pour la communication HTTPS entre le Focus (le composant qui gère l'état de la conférence Skype) et les serveurs individuels.
Port de groupe SIP	5071	TCP	Utilisé pour les requêtes SIP entrantes de l'application de groupe de réponse.
Port de partage d'applications SIP	5065	TCP	Utilisé pour les requêtes d'écoute SIP entrantes pour le partage d'applications.
Port d'opérateur SIP	5072	TCP	Utilisé pour les requêtes SIP entrantes destinées

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTIQUETTE	PORT	PROTOCOLE	DESCRIPTION
			à l'opérateur (c'est-à-dire pour la conférence téléphonique).
Port d'annonce de conférence SIP	5073	TCP	Utilisé pour les requêtes SIP entrantes destinées au service d'annonce de conférence du serveur Skype for Business (c'est-à-dire pour la conférence téléphonique).
Port SIP CallPark	5075	TCP	Utilisé pour les requêtes SIP entrantes destinées à l'application CallPark.
Port d'admission d'appel SIP	448	TCP	Utilisé pour le contrôle d'admission d'appel par le service de stratégie de bande passante du serveur Skype for Business.
Port TURN d'admission d'appel SIP	5080	TCP	Utilisé pour le contrôle d'admission d'appel par le service de politique de bande passante pour le trafic TURN Audio/ Vidéo Edge.
Port de test audio SIP	5076	TCP	Utilisé pour les requêtes SIP entrantes destinées

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTIQUETTE	PORT	PROTOCOLE	DESCRIPTION
			au service de test audio.
Port externe HTTPS	443	HTTPS	Utilisé pour les ports externes pour la communication SIP/TLS pour l'accès utilisateur à distance, l'accès aux conférences Web internes, et les communications multimédias STUN/TCP entrantes et sortantes pour l'accès aux médias internes et aux sessions A/V.
Port interne HTTPS	443	HTTPS	Utilisé pour les ports internes pour la communication SIP/TLS pour l'accès utilisateur à distance, l'accès aux conférences Web internes et les communications multimédias STUN/TCP entrantes et sortantes pour l'accès aux sessions multimédias et A/V internes.
Port d'accès à distance externe SIP	5061	TCP	Utilisé pour les ports externes pour la communication SIP/MTLS pour l'accès utilisateur à distance ou la fédération.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTIQUETTE	PORT	PROTOCOLE	DESCRIPTION
Port d'accès à distance interne SIP	5061	TCP	Utilisé pour les ports internes pour la communication SIP/MTLS pour l'accès utilisateur à distance ou la fédération.
Port UDP STUN externe SIP	3478	UDP	Utilisé pour les ports externes pour les communications multimédias STUN/UDP entrantes et sortantes.
Port UDP STUN interne SIP	3478	UDP	Utilisé pour les ports internes pour les communications multimédias entrantes et sortantes STUN/UDP.
Port IM interne SIP	5062		Utilisé pour les ports internes pour l'authentification SIP/MTLS des communications de messagerie instantanée sortantes via le pare-feu interne.
Port HTTP	80	TCP	Utilisé pour la communication initiale des directeurs vers les FQDN de la ferme web.
Port HTTPS	443	HTTPS	Utilisé pour la communication des directeurs vers les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTIQUETTE	PORT	PROTOCOLE	DESCRIPTION
			FQDN de la ferme web.
Port interne AutoDiscover	4443	HTTPS	Utilisé pour HTTPS (depuis le proxy inverse) et les communications inter-pools du directeur HTTPS pour la connexion AutoDiscover.
Port interne SIP	5061	TCP	Utilisé pour les communications internes entre les serveurs et pour les connexions client.

```
6.  Dans la section **Instances cibles**, sélectionnez les trois instances NetScaler différentes sur lesquelles déployer les trois serveurs Skype Entreprise.
```

REMARQUE

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

7. Cliquez sur **Créer** pour créer la configuration sur les instances NetScaler sélectionnées.

CONSEIL

Nous vous recommandons de sélectionner **Exécution à blanc** pour vérifier les objets de configuration qui doivent être créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque la configuration est créée avec succès, le StyleBook crée 25 serveurs virtuels d'équilibrage de charge. C'est-à-dire que pour chaque port, un serveur virtuel d'équilibrage de charge est défini avec un groupe de services, et le groupe de services est lié au serveur virtuel d'équilibrage de charge. La configuration ajoute également les serveurs frontaux en tant que membres du groupe de services et les lie au groupe de services. Le nombre de membres du groupe de services créés est égal au nombre de serveurs frontaux créés.

La figure suivante montre les objets créés dans chaque serveur :



StyleBook Microsoft Exchange

Vous pouvez utiliser le StyleBook Microsoft Exchange 2016 pour déployer une configuration NetScaler qui optimise et sécurise une application d'entreprise Microsoft Exchange 2016 dans votre réseau. Microsoft Exchange 2016 est une application d'entreprise clé pour fournir des services de messagerie électronique, de gestion des informations personnelles et de messagerie à vos employés et autres parties prenantes.

Fonctionnalités NetScaler configurées à l'aide du StyleBook Microsoft Exchange

Le StyleBook Microsoft Exchange 2016 active et configure les fonctionnalités NetScaler suivantes pour les serveurs Microsoft Exchange 2016 :

- Équilibrage de charge - Équilibrage de charge de base qui permet l'équilibrage de charge de plusieurs serveurs Exchange
- Commutation de contenu - Commutation de contenu qui permet un accès IP unique et la redirection des requêtes vers les serveurs virtuels d'équilibrage de charge corrects
- Réécriture - Redirige les utilisateurs vers des pages sécurisées
- Déchargement SSL - Décharge le traitement SSL vers le NetScaler, réduisant ainsi la charge sur le serveur Exchange

La figure suivante représente schématiquement le déploiement des serveurs Exchange dans le réseau :



Prérequis

- Pour l'authentification basée sur les certificats, tous les hôtes adressables faisant partie de la configuration réseau doivent avoir des noms de domaine résolvables et pas seulement des adresses IP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Assurez-vous que les ports SIP sont accessibles sur le serveur Microsoft Exchange 2016.

Configuration d'un StyleBook Microsoft Exchange

Configurez le StyleBook Microsoft Exchange dans votre entreprise pour déployer la configuration NetScaler.

Pour configurer une application Microsoft Exchange dans NetScaler Console

1. Dans NetScaler Console, accédez à **Applications** > **StyleBooks**.
2. Recherchez **Microsoft Exchange 2016 StyleBook** et cliquez sur **Créer une configuration**.

   Le StyleBook apparaît sous la forme d'un formulaire d'interface utilisateur dans lequel vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.

   
3. Saisissez les détails pour les paramètres suivants :

   - **Nom de l'application Exchange** - Nom de l'application Microsoft Exchange dans votre réseau
   - **VIP Exchange** - Adresse IP virtuelle sur NetScaler qui reçoit les requêtes client pour l'application Microsoft Exchange
   - **Adresses IP des serveurs Exchange** - Adresses IP de tous les serveurs Exchange du réseau.

     Si vous souhaitez ajouter d'autres adresses IP, cliquez sur l'icône plus (**+**). Généralement, deux serveurs Exchange sont configurés dans le réseau.
4. Dans la section **Certificats Exchange**, téléchargez les certificats Exchange vers NetScaler Console. Saisissez les noms des fichiers de certificat et de clé, puis téléchargez-les depuis le stockage local. Vous pouvez également fournir un mot de passe de clé privée pour chiffrer le fichier de clé.

   REMARQUE

   Assurez-vous que les fichiers de certificat sont au format ".pem" ou ".der". NetScaler Console rejette les fichiers d'autres formats.

   Si vous souhaitez spécifier les détails d'expiration du certificat ou des paramètres avancés, sélectionnez **Paramètres de certificat avancés**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Dans la section **Configuration de l'authentification Exchange Active Directory**, configurez les paramètres AD en saisissant les données.

   - **Active Directory Authentication VIP** - L'adresse IP virtuelle utilisée pour créer et configurer le serveur virtuel AD (LDAP) sur une appliance NetScaler.
   - **Active Directory Server IP** - L'adresse IP de votre contrôleur de domaine Active Directory.
   - **Active Directory Base String** - La chaîne de base LDAP dans Active Directory. Par exemple, CN=Users,DC=CTXNSSFB,DC=COM.
   - **Active Directory LDAP Bind Distinguished Name (DN)** - Le nom distinctif de liaison LDAP (DN) est utilisé pour lier cet objet au serveur LDAP (AD). Par exemple « cn=Administrator,cn=Users,dc=acme,dc=com »
   - **Active Directory LDAP Bind Distinguished Name (DN) Password** - Le mot de passe du nom distinctif de liaison LDAP (DN) est le mot de passe pour l'authentification AD.
   - **Active Directory User Name Attribute** - Attribut AD pour le nom d'utilisateur. Le NetScaler utilise l'attribut LDAP pour interroger les serveurs Active Directory externes. Par exemple, « sAMAccountName »
   - **Active Directory group Attribute Name** - les noms d'attributs de groupe LDAP configurés sur le serveur LDAP. Par exemple, « memberOf » pour l'attribut de groupe dans LDAP.
   - **Active Directory Sub-Attribute Name** - les noms de sous-attributs LDAP configurés sur le serveur LDAP. Par exemple, « cn » pour le sous-attribut dans LDAP.
   - **Active Directory Authentication Domain** - Le nom de domaine AD/LDAP utilisé pour l'authentification. Par exemple, ctxnssfb.com.

6. Dans la section **Target Instances**, sélectionnez l'instance NetScaler sur laquelle déployer cette configuration Exchange.

   REMARQUE

   Si vous souhaitez afficher les instances NetScaler récemment découvertes, cliquez sur l'icône d'actualisation.

7. Cliquez sur **Create** pour créer le fichier de configuration et exécuter la configuration sur l'instance NetScaler sélectionnée.

   Nous vous recommandons de sélectionner d'abord **Dry Run** pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque la configuration a été créée avec succès, le StyleBook a créé un serveur virtuel de commutation de contenu, cinq serveurs virtuels d'équilibrage de charge et une politique LDAP liée à un serveur virtuel d'authentification LDAP. De plus, les groupes de services correspondants ont été créés et liés aux serveurs virtuels d'équilibrage de charge.

StyleBook Microsoft SharePoint

Microsoft SharePoint 2016 est une application d'entreprise clé qui fournit principalement un système de gestion et de stockage de documents, hautement configurable et pris en charge par tous les principaux navigateurs.

Vous pouvez utiliser le StyleBook Microsoft SharePoint 2016 pour déployer une configuration NetScaler qui optimise et sécurise l'application d'entreprise Microsoft SharePoint 2016 dans votre réseau.

Prérequis

- Microsoft SharePoint 2016
- NetScaler Console, version 12.0 et ultérieure
- NetScaler, version 10.5 et ultérieure

Fonctionnalités NetScaler configurées par le StyleBook Microsoft SharePoint 2016

Vous pouvez utiliser le StyleBook Microsoft SharePoint 2016 pour activer et configurer les fonctionnalités NetScaler suivantes pour Microsoft SharePoint 2016 :

- Équilibrage de charge
- Commutation de contenu
- Répondeur
- Réécriture
- Compression
- Mise en cache intégrée

Équilibrage de charge

L'équilibrage de charge NetScaler répartit équitablement les requêtes vers les serveurs SharePoint backend. La surveillance intelligente des serveurs backend empêche l'envoi de requêtes à des serveurs défaillants.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le StyleBook SharePoint configure 12 serveurs virtuels d'équilibrage de charge, chacun dédié à l'équilibrage de charge des requêtes pour un certain type de contenu, tels que les documents, les images, l'audio, la vidéo et d'autres types de fichiers.

Le StyleBook SharePoint prend désormais en charge le mode SSL de l'application SharePoint en configurant des serveurs virtuels d'équilibrage de charge basés sur SSL. Assurez-vous que SSL est sélectionné comme protocole frontal. Notez que le port virtuel est défini sur 443 par défaut. Vous pouvez également sélectionner SSL pour lier des groupes de services (serveurs d'applications SharePoint) aux serveurs virtuels d'équilibrage de charge cibles. Notez que le protocole backend est défini sur HTTP par défaut.

Commutation de contenu

La fonctionnalité de commutation de contenu est utilisée pour distribuer les requêtes client entre plusieurs serveurs virtuels d'équilibrage de charge sur la base de types spécifiques de contenu SharePoint demandé (par exemple, des documents, des images et des fichiers audio ou vidéo). Le module de commutation de contenu dirige le trafic entrant vers un serveur virtuel d'équilibrage de charge correspondant de manière optimale qui peut traiter ce type de contenu. Vous pouvez donc appliquer différentes politiques d'optimisation à différents types de trafic. Par exemple, vous pourriez vouloir utiliser des politiques de compression ou de mise en cache différentes pour la vidéo que pour les documents texte.

Répondeur

La fonctionnalité de répondeur d'une instance NetScaler peut être utilisée pour rediriger de manière transparente les utilisateurs de HTTP vers HTTPS. Le répondeur peut également être configuré pour fournir des pages d'erreur personnalisées. La politique du répondeur détermine les requêtes (trafic) sur lesquelles une action doit être effectuée, et lie chaque politique à un serveur virtuel d'équilibrage de charge. Le StyleBook SharePoint inclut une configuration qui redirige les utilisateurs des URL HTTP vers HTTPS.

Réécriture

Le module de réécriture est utilisé pour modifier les en-têtes de requête/réponse, les URL ou le contenu à la volée. Ce module fonctionne en ligne avec le traitement du trafic et peut donc modifier le flux de trafic selon les besoins pour des cas d'utilisation particuliers. Par exemple, la réécriture peut fournir un accès au contenu demandé sans exposer de détails inutiles sur le serveur du site web.

Dans le StyleBook SharePoint, la fonctionnalité de réécriture est utilisée pour supprimer les en-têtes inutiles des requêtes utilisateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compression

Le moteur de compression NetScaler identifie et compresse le contenu compressible. Ce processus améliore le temps de transmission des données et réduit les exigences de bande passante réseau pour les clients, tout en économisant des cycles CPU sur les serveurs de contenu SharePoint. Une instance NetScaler peut compresser les données statiques et générées dynamiquement. Elle applique l'algorithme de compression GZIP ou DEFLATE pour supprimer les informations superflues et répétitives des réponses du serveur et représenter les informations originales dans un format plus compact et efficace. La capacité du navigateur client à décompresser les données dépend de l'algorithme ou des algorithmes qu'il prend en charge : GZIP, DEFLATE, ou les deux.

Une instance NetScaler est configurée pour compresser le texte dans les documents HTML, XML, texte brut, feuilles de style en cascade (CSS) et Microsoft Office, mais ne compresse pas les images au format GIF ou JPG. Les principaux avantages du trafic compressé incluent la réduction des coûts de bande passante, la réduction de la latence WAN et une meilleure performance du serveur.

Mise en cache intégrée

Le cache en mémoire de NetScaler peut stocker des objets SharePoint afin de fournir rapidement du contenu fréquemment demandé aux utilisateurs. Le contenu mis en cache comprend les documents téléchargés et les fichiers audio, vidéo et image.

La figure suivante représente schématiquement le déploiement de serveurs SharePoint dans un réseau dont l'accès est géré par une instance NetScaler sur laquelle NetScaler Console est utilisée pour déployer une configuration StyleBook SharePoint.



Déploiement des configurations StyleBook SharePoint

La tâche suivante vous aidera à déployer le StyleBook Microsoft SharePoint 2016 dans votre réseau d'entreprise.

Pour déployer le StyleBook Microsoft SharePoint 2016 :

1. Dans NetScaler Console, accédez à **Applications** > **Administration** > **Configuration**, puis cliquez sur **Créer nouveau**.

   La page **Choisir StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console.
2. Faites défiler vers le bas et sélectionnez **Microsoft SharePoint 2016 StyleBook**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Dans NetScaler Console, accédez à **Applications** > **Configurations** > **StyleBooks**. Faites défiler vers le bas pour trouver le **StyleBook Microsoft SharePoint 2016**, puis cliquez sur **Créer une configuration**.

Le StyleBook s'ouvre sous la forme d'un formulaire d'interface utilisateur sur lequel vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.

Saisissez les valeurs pour les paramètres suivants :

a. **Nom de l'application SharePoint**. Nom de la configuration SharePoint à déployer dans votre réseau.

b. **Adresse IP virtuelle SharePoint**. Adresse IP virtuelle à laquelle l'instance NetScaler reçoit les requêtes client pour l'application Microsoft SharePoint.

c. **Port virtuel SharePoint**. Le port TCP à utiliser par les utilisateurs pour accéder à l'application SharePoint

d. **Protocole frontal SharePoint**. Sélectionnez le protocole frontal SharePoint dans la liste déroulante. Les options disponibles sont HTTP ou SSL.

REMARQUE

Si vous sélectionnez SSL, assurez-vous que le paramètre Configuration de réécriture est activé dans la section Paramètres avancés de SharePoint de ce StyleBook.

e. **Adresses IP des serveurs SharePoint**. Adresses IP de tous les serveurs SharePoint du réseau.

f. **Port des serveurs SharePoint**. Numéro de port TCP utilisé par les serveurs SharePoint. Par défaut, il s'agit du port 80. Vous pouvez modifier cette valeur si nécessaire, mais assurez-vous que ce port est accessible sur les serveurs Microsoft SharePoint 2016.

3. Dans la section **Paramètres des certificats SSL**, cliquez sur + pour saisir le nom du certificat SSL, la clé de certificat, et sélectionnez les fichiers correspondants dans votre dossier de stockage local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez éventuellement sur **Paramètres avancés du certificat** pour activer ou désactiver la surveillance de l'expiration du certificat SSL. Si vous activez la surveillance de l'expiration du certificat, définissez le nombre de jours afin que NetScaler Console émette une alarme après ce nombre de jours lorsque le certificat est sur le point d'expirer. Vous avez également la possibilité de faire de la vérification OCSP une fonctionnalité facultative ou obligatoire.

   

5. La section **Paramètres avancés** de SharePoint vous permet d'activer les fonctionnalités NetScaler qui seront configurées sur les instances NetScaler. Bien que les fonctionnalités d'équilibrage de charge et de commutation de contenu soient configurées sur les instances par défaut, vous pouvez choisir les autres fonctionnalités, c'est-à-dire la configuration du répondeur, la configuration de réécriture, la configuration de compression et la configuration de mise en cache intégrée, que vous souhaitez configurer sur l'instance.
6. Cliquez sur **Instances cibles** et sélectionnez l'instance NetScaler sur laquelle déployer cette configuration SharePoint. Cliquez sur **Créer** pour créer la configuration et la déployer sur l'instance NetScaler sélectionnée.

   REMARQUE

   Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.



REMARQUE

Nous vous recommandons de sélectionner **Exécution à blanc** avant d'exécuter la configuration réelle pour vérifier les objets de configuration qui seront créés sur l'instance cible.

Lorsque la configuration est créée et déployée avec succès, le StyleBook SharePoint crée un serveur virtuel de commutation de contenu et 12 serveurs virtuels d'équilibrage de charge. Il crée également des stratégies et des groupes de services et les lie aux serveurs virtuels d'équilibrage de charge. Les stratégies créées dépendent des fonctionnalités sélectionnées dans le StyleBook lors de la création du pack de configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Affichage des objets définis sur l'instance NetScaler

Une fois le pack de configuration créé sur NetScaler Console, vous pouvez afficher tous les objets créés sur l'instance NetScaler pour le StyleBook SharePoint. Accédez à **Applications** > **Administration** > **Configuration**, puis cliquez sur **Afficher les objets créés**. La figure suivante montre certains des objets créés, avec les adresses IP spécifiées dans l'exemple présenté dans « Déploiement des configurations de StyleBook SharePoint à partir de NetScaler Console. »



StyleBook de proxy Microsoft ADFS

Le proxy Microsoft ADFS joue un rôle important en offrant un accès par authentification unique (SSO) aux ressources internes compatibles avec la fédération et aux ressources cloud. Office 365 est un exemple de ressource cloud. Le but du serveur proxy ADFS est de recevoir et de transmettre les requêtes aux serveurs ADFS qui ne sont pas accessibles depuis Internet. Le proxy ADFS est un proxy inverse et réside généralement dans le réseau périmétrique (DMZ) de votre organisation. Le proxy ADFS joue un rôle essentiel dans la connectivité des utilisateurs à distance et l'accès aux applications.

NetScaler dispose de la technologie précise pour permettre une connectivité sécurisée, l'authentification et la gestion de l'identité fédérée. L'utilisation de NetScaler comme proxy ADFS évite de devoir déployer un composant supplémentaire dans la DMZ.

Le StyleBook de proxy Microsoft ADFS dans NetScaler Console vous permet de configurer un serveur proxy ADFS sur une instance NetScaler.

L'image suivante montre le déploiement d'une instance NetScaler en tant que serveur proxy ADFS dans la DMZ de l'entreprise.



Avantages de l'utilisation de NetScaler comme proxy ADFS

1. Répond aux besoins d'équilibrage de charge et de proxy ADFS
2. Prend en charge les scénarios d'accès utilisateur internes et externes
3. Prend en charge des méthodes riches pour la pré-authentification
4. Offre une expérience d'authentification unique aux utilisateurs
5. Prend en charge les protocoles actifs et passifs
    a. Exemples d'applications de protocole actif : Microsoft Outlook, Microsoft Skype Entreprise

© 1997–2026 Citrix Systems, Inc. All rights reserved.

   b. Exemples d'applications de protocole passif : application web Microsoft Outlook, navigateurs web

6. Appareil renforcé pour un déploiement basé sur la DMZ
7. Ajoute de la valeur en utilisant des fonctionnalités NetScaler principales supplémentaires

   a. Commutation de contenu
   b. Déchargement SSL
   c. Réécriture
   d. Sécurité (NetScaler AAA)

Pour les scénarios basés sur un protocole actif, vous pouvez vous connecter à Office 365 et fournir vos informations d'identification. Microsoft Federation Gateway contacte le service ADFS (via le proxy ADFS) au nom du client de protocole actif. La passerelle soumet ensuite les informations d'identification à l'aide de l'authentification de base (401). NetScaler gère l'authentification du client avant l'accès au service ADFS. Après l'authentification, le service ADFS fournit un jeton SAML à la passerelle de fédération. La passerelle de fédération, à son tour, soumet le jeton à Office 365 pour fournir l'accès au client.

Pour les clients passifs, le StyleBook du proxy ADFS crée un compte utilisateur de délégation contrainte Kerberos (KCD). Le compte KCD est nécessaire pour l'authentification SSO Kerberos afin de se connecter aux serveurs ADFS. Le StyleBook génère également une stratégie LDAP et une stratégie de session. Ces stratégies sont ensuite liées au serveur virtuel NetScaler AAA qui gère l'authentification des clients passifs.

Le StyleBook peut également garantir que les serveurs DNS sur le NetScaler sont configurés pour ADFS.

La section de configuration ci-dessous décrit comment configurer NetScaler pour gérer l'authentification client basée sur les protocoles actifs et passifs.

Détails de la configuration

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration soit déployée avec succès.

PRODUIT	VERSION MINIMALE REQUISE
NetScaler	11.0, licence Advanced/Premium

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées.

Déploiement des configurations StyleBook de proxy Microsoft ADFS à partir de NetScaler Console

Les instructions suivantes vous aident lors de la mise en œuvre du StyleBook de proxy Microsoft ADFS dans votre réseau d'entreprise.

Pour déployer le StyleBook de proxy Microsoft ADFS

1. Dans NetScaler Console, accédez à **Applications** \> **StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans NetScaler Console.
2. Faites défiler vers le bas et recherchez le **StyleBook de proxy Microsoft ADFS**. Cliquez sur **Créer une configuration**. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.
3. Saisissez les valeurs pour les paramètres suivants :

   a. **Nom de déploiement du proxy ADFS**. Sélectionnez un nom pour la configuration du proxy ADFS déployée dans votre réseau.

   b. **FQDNs ou adresses IP des serveurs ADFS**. Saisissez les adresses IP ou les FQDN (noms de domaine) de tous les serveurs ADFS du réseau.

   c. **Adresse IP VIP publique du proxy ADFS**. Saisissez l'adresse IP virtuelle publique sur le NetScaler qui agit comme un serveur proxy ADFS.

   ☐

4. Dans la section **Certificats de proxy ADFS**, saisissez les détails du certificat SSL et de la clé de certificat.

   Ce certificat SSL est lié à tous les serveurs virtuels créés sur l'instance NetScaler.

   Sélectionnez les fichiers respectifs dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de la clé privée pour charger les clés privées chiffrées au format .pem.

   ☐

   Vous pouvez également activer la case à cocher **Paramètres avancés du certificat**. Ici, vous pouvez saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Vous pouvez éventuellement cocher la case **Certificat CA SSL** si le certificat SSL nécessite l'installation d'un certificat public d'autorité de certification sur NetScaler. Assurez-vous de sélectionner **Est un certificat CA** dans la section **Paramètres avancés du certificat**.
6. Activez l'authentification pour les clients actifs et passifs. Saisissez le nom de domaine DNS utilisé dans Active Directory pour l'authentification des utilisateurs. Vous pouvez ensuite configurer l'authentification pour les clients actifs, les clients passifs, ou les deux.
7. Saisissez les détails suivants pour activer l'authentification pour les clients actifs :

   REMARQUE

   La configuration de la prise en charge des clients actifs est facultative.

   a. **VIP d'authentification active du proxy ADFS**. Saisissez l'adresse IP virtuelle du serveur d'authentification virtuel sur l'instance NetScaler vers laquelle les clients actifs sont redirigés pour l'authentification.
   b. **Nom d'utilisateur du compte de service**. Saisissez le nom d'utilisateur du compte de service utilisé par NetScaler pour authentifier vos utilisateurs auprès de l'Active Directory.
   c. **Mot de passe du compte de service**. Saisissez le mot de passe utilisé par NetScaler pour authentifier vos utilisateurs auprès de l'Active Directory.

   
8. Configurez l'authentification pour les clients passifs en activant l'option correspondante et en configurant les paramètres LDAP.

   REMARQUE

   La configuration de la prise en charge des clients passifs est facultative.

   Saisissez les détails suivants pour activer l'authentification pour les clients passifs :

   a. **Base LDAP (Active Directory)**. Saisissez le nom de domaine de base du domaine dans lequel résident les comptes d'utilisateur au sein de l'Active Directory (AD) pour permettre l'authentification. Par exemple, dc=netscaler®,dc=com
   b. **DN de liaison LDAP (Active Directory)**. Ajoutez un compte de domaine (en utilisant une adresse e-mail pour faciliter la configuration) qui dispose des privilèges nécessaires pour parcourir l'arborescence AD. Par exemple, cn=Manager,dc=netscaler,dc=com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **Mot de passe du DN de liaison LDAP (Active Directory)**. Saisissez le mot de passe du compte de domaine pour l'authentification.

   Voici quelques autres champs pour lesquels vous devez saisir les valeurs dans cette section :

d. **Adresse IP du serveur LDAP (Active Directory)**. Saisissez l'adresse IP du serveur Active Directory pour que l'authentification AD fonctionne correctement.

e. **Nom de domaine complet (FQDN) du serveur LDAP nom**. Saisissez le nom de domaine complet (FQDN) du serveur Active Directory. Le nom FQDN est facultatif. Indiquez l'adresse IP comme à l'étape 1 ou le nom FQDN.

f. **Port Active Directory du serveur LDAP**. Par défaut, les ports TCP et UDP pour le protocole LDAP sont 389, tandis que le port TCP pour le LDAP sécurisé est 636.

g. **Nom d'utilisateur de connexion LDAP (Active Directory)**. Saisissez le nom d'utilisateur sous la forme "sAMAccountName".

h. **VIP d'authentification passive du proxy ADFS**. Saisissez l'adresse IP du serveur virtuel proxy ADFS pour les clients passifs.

REMARQUE

Les champs marqués d'un "*" sont obligatoires.

9. Vous pouvez également configurer un VIP DNS pour vos serveurs DNS, si vous le souhaitez.

10. Cliquez sur **Instances cibles** et sélectionnez les instances NetScaler sur lesquelles déployer cette configuration de proxy Microsoft ADFS. Cliquez sur **Créer** pour créer la configuration et la déployer sur les instances NetScaler sélectionnées.

REMARQUE

Nous vous recommandons de sélectionner **Exécution à blanc** avant d'exécuter la configuration réelle. Vous pouvez d'abord afficher les objets de configuration créés sur les instances NetScaler cibles par le StyleBook. Vous pouvez ensuite cliquer sur **Créer** pour déployer la configuration sur les instances sélectionnées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Objets créés

Plusieurs objets de configuration sont créés lorsque la configuration du proxy ADFS est déployée sur l'instance NetScaler. L'image suivante affiche la liste des objets créés.



StyleBook Oracle E-Business

Oracle E-Business Suite est la suite la plus complète d'applications métier intégrées et globales. Cette suite permet aux organisations de prendre de meilleures décisions, de réduire les coûts et d'améliorer les performances, et se compose des applications suivantes.

- Planification des ressources d'entreprise (ERP)
- Gestion de la relation client (CRM)
- Gestion de la chaîne d'approvisionnement (SCM)

Ces applications informatiques sont développées ou acquises par Oracle. Le StyleBook Oracle E-Business Suite 12.2 vous permet de déployer la configuration sur les instances NetScaler sélectionnées.

Ce StyleBook crée une configuration d'équilibrage de charge qui comprend un serveur virtuel d'équilibrage de charge, un groupe de services et une liste de services. Il lie également les services au groupe de services et le groupe de services au serveur virtuel. Vous pouvez choisir une communication chiffrée en sélectionnant SSL et en fournissant les fichiers SSL et les fichiers de clés depuis votre système local.

Pour créer une configuration pour Oracle E-Business Suite 12.2

1. Dans NetScaler Console, accédez à **Applications** > **Configuration > StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre NetScaler Console. Faites défiler vers le bas et sélectionnez **Oracle E-Business Suite 12.2**. Vous pouvez également utiliser l'option de recherche pour rechercher le StyleBook.
2. Cliquez sur **Créer une configuration** dans le panneau StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Saisissez le nom de l'application d'équilibrage de charge et l'adresse IP virtuelle dans la section des paramètres de l'équilibreur de charge.
4. Sélectionnez le protocole requis. Vous avez deux options ici : HTTP et HTTPS/SSL. Vous pouvez également saisir le numéro de port.
5. Saisissez les adresses IP de tous les serveurs d'applications Oracle E-Business Suite du réseau qui doivent être équilibrés en charge. Cliquez sur **+** pour ajouter d'autres adresses IP de serveur.
6. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers correspondants depuis votre stockage local. Vous pouvez également activer la case à cocher **Paramètres avancés des certificats**. Ici, vous pouvez configurer plus de détails tels que la période de notification d'expiration du certificat. Vous pouvez également activer ou désactiver le moniteur d'expiration des certificats.

   Sélectionnez l'instance NetScaler cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

   

   CONSEIL

   Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre. L'icône d'actualisation est actuellement disponible uniquement sur NetScaler Console.

Citrix StoreFront™ StyleBooks

StoreFront est un magasin d'applications d'entreprise qui agrège les applications et les bureaux des sites Citrix Virtual Apps and Desktops en un seul magasin pour les utilisateurs. StoreFront authentifie les utilisateurs auprès des sites hébergeant des ressources et gère les magasins d'applications et les bureaux auxquels les utilisateurs accèdent. Il héberge votre magasin d'applications d'entreprise, ce qui vous permet de donner aux utilisateurs un accès en libre-service aux applications et aux bureaux que vous mettez à leur disposition.

Ce StyleBook définit les configurations NetScaler pour les serveurs StoreFront. Avec ce StyleBook, vous pouvez configurer les serveurs StoreFront sur les instances NetScaler souhaitées. Vous pouvez choisir une communication chiffrée en sélectionnant SSL et en fournissant les fichiers SSL et les fichiers de clés depuis votre système local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Créer une configuration pour les applications Citrix StoreFront

1. Dans l'interface graphique de NetScaler Console, accédez à **Applications > StyleBooks**.
2. Dans la barre de recherche, utilisez les propriétés **Nom** et recherchez `Citrix StoreFront`.
3. Sur le StyleBook Citrix StoreFront, cliquez sur Créer une configuration.
4. Spécifiez les détails suivants :

   - **Nom StoreFront** : Spécifiez le nom StoreFront. Le pack de configuration StoreFront est créé avec le même nom StoreFront.
   - **IP virtuelle (VIP)** : Spécifiez l'adresse IP virtuelle à laquelle l'instance NetScaler reçoit les requêtes client.
   - **Serveurs StoreFront** : Spécifiez les adresses IP des serveurs StoreFront que vous souhaitez configurer avec une instance NetScaler.
   - **URL de redirection HTTPS** : Spécifiez l'URL HTTPS vers laquelle les requêtes HTTPS sont redirigées.

   

5. Dans la section **Paramètres des certificats SSL**, saisissez les noms du certificat SSL et de la clé de certificat.
6. Sélectionnez les fichiers respectifs depuis votre dossier de stockage local. Vous pouvez également saisir le mot de passe de la clé privée pour spécifier les clés privées chiffrées au format PEM.

   Spécifier les paramètres du certificat SSL pour les StyleBooks StoreFront(/en-us/netscaler-application-delivery-management-software/media/ssl-cert-sf-stylebooks.png)
7. Vous pouvez également activer la case à cocher **Paramètres avancés du certificat**. Ici, vous pouvez saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.
8. Facultatif, sélectionnez la case à cocher **Certificat CA SSL pour l'adresse IP virtuelle d'authentification** si le certificat SSL nécessite l'installation d'un certificat public CA sur NetScaler. Assurez-vous de choisir **Est un certificat CA** dans la section **Paramètres avancés du certificat**.
9. Cliquez sur **Créer**.
10. Cliquez sur **Instances cibles** et sélectionnez les instances NetScaler sur lesquelles vous souhaitez configurer les serveurs StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances NetScaler sélectionnées.

Créer et utiliser des StyleBooks personnalisés

Vous pouvez écrire votre propre StyleBook pour votre déploiement, l'importer dans NetScaler Console et créer des objets de configuration. Vous pouvez également utiliser l'API pour créer des configurations à partir de vos StyleBooks.

Ce document contient les informations suivantes :

Avant de commencer

Avant de commencer à créer des StyleBooks, assurez-vous d'avoir des connaissances sur les points suivants :

- API NITRO. Pour plus d'informations, consultez la documentation de l'API Nitro
- YAML

Les fichiers StyleBook utilisent le format YAML. Pour plus d'informations sur le format YAML, consultez Syntaxe YAML.

Voici une liste de directives YAML dont vous devez tenir compte lors de la création de StyleBooks :

- YAML est sensible à la casse.
- YAML nécessite une indentation correcte
- Utilisez la touche `<spacebar>` pour créer une indentation correcte. N'utilisez pas la touche `<tab>`. L'utilisation de la touche `<tab>` crée une erreur de compilation lors de l'importation de votre StyleBook dans le service MA.
- N'utilisez pas de chaînes entre guillemets. Incluez la chaîne entre guillemets uniquement si une chaîne contient des signes de ponctuation (tirets, deux-points, etc.). Si vous souhaitez interpréter un nombre comme une chaîne, incluez le nombre entre guillemets ou utilisez la fonction intégrée str() des StyleBooks.
- Les littéraux comme YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off, et TRUE/true/truthy/FALSE/False/false/falsely sont considérés comme des booléens et sont équivalents à true et false respectivement. Pour les interpréter comme des chaînes, incluez-les entre guillemets. Par exemple :
    - "YES"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- "Non"
- "Vrai"
- "Faux" et ainsi de suite.

REMARQUE

Avant d'importer votre fichier StyleBook dans NetScaler Console, il est recommandé de vérifier s'il est conforme au format YAML. Nous vous recommandons d'utiliser le validateur YAML intégré aux StyleBooks pour valider et importer le contenu YAML.

Lors de la configuration des StyleBooks, vous ne pouvez utiliser que les ressources de configuration Nitro qui prennent en charge les opérations **Créer** et **Supprimer** (méthodes HTTP POST et DELETE). Pour plus d'informations, consultez la documentation des API Nitro.

Anatomie d'un StyleBook

La rédaction de StyleBooks nécessite de comprendre la grammaire, la syntaxe et la structure des StyleBooks. Un StyleBook typique comporte les sections suivantes :

- **En-tête** : Cette section vous permet de définir l'identité d'un StyleBook et de décrire ce qu'il fait. C'est une section obligatoire.
- **Importer des StyleBooks** : Cette section vous permet de déclarer à quel autre StyleBook vous souhaitez faire référence depuis votre StyleBook actuel. L'importation de StyleBooks de configuration NetScaler NITRO ou d'autres StyleBooks est nécessaire pour écrire un StyleBook. C'est une section obligatoire.
- **Paramètres** : Cette section vous permet de définir les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Elle décrit l'entrée que votre StyleBook prend. C'est une section facultative.
- **Composants** : Cette section vous permet de définir les entités (objets de configuration) créées par le StyleBook pour une configuration spécifique. Cette section est considérée comme le cœur d'un StyleBook. Les composants utilisent généralement l'entrée fournie dans la section des paramètres pour adapter la configuration générée par le StyleBook. C'est une section facultative.

  Un StyleBook peut avoir une section de paramètres, ou une section de composants, ou les deux. Un StyleBook avec seulement la section des paramètres est utile pour définir une liste de paramètres qui peuvent être utilisés par d'autres StyleBooks. Cela favorise la réutilisabilité des groupes de paramètres à travers un ensemble de StyleBooks. Un StyleBook avec seulement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

une section de composants peut être utilisé lorsque vous souhaitez spécifier les valeurs des attributs dans le StyleBook au lieu de définir des paramètres pour prendre l'entrée utilisateur.

- **Sorties** : Alors que la section des paramètres définit les entrées du StyleBook, cette section facultative définit ses sorties. Dans cette section de sorties facultative, vous pouvez spécifier les composants que vous souhaitez exposer aux utilisateurs créant une configuration à partir de ce StyleBook et aux autres StyleBooks qui importent ce StyleBook. Les utilisateurs et les StyleBooks importateurs peuvent alors référencer les propriétés des composants exposés.
- **Opérations** : Un StyleBook peut contenir une section facultative pour activer l'analyse dans NetScaler Console sur tout serveur virtuel faisant partie du StyleBook.

La figure suivante montre un aperçu simple d'un StyleBook.



Les exemples suivants vous aident à comprendre la grammaire et la structure d'un StyleBook et à écrire des StyleBooks avec des niveaux de complexité croissants.

- StyleBook pour créer un serveur virtuel d'équilibrage de charge
- StyleBook pour créer une configuration d'équilibrage de charge de base
- Créer un StyleBook composite
- Personnaliser votre StyleBook à l'aide d'attributs d'interface graphique

StyleBook pour créer un serveur virtuel d'équilibrage de charge

Dans cet exemple, vous concevez un StyleBook de base qui crée un serveur virtuel d'équilibrage de charge de type protocole HTTP et écoutant sur le port 80. Les paramètres du nom du serveur virtuel, de l'adresse IP et de la méthode d'équilibrage de charge acceptent des valeurs définies par l'utilisateur, c'est-à-dire qu'ils sont les paramètres du StyleBook.

En-tête

Les six premières lignes d'un StyleBook constituent la section d'en-tête. Dans cet exemple, la section d'en-tête est rédigée comme suit :

```
name: lb-vserver

description: This StyleBook defines a load balancing virtual server
configuration.

display-name: Load Balancing Virtual Server (HTTP)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"
```

La section d'en-tête comprend les détails suivants :

- **name** : Un nom pour ce StyleBook.
- **description** : Une description définissant ce que fait ce StyleBook. Cette description apparaît sur NetScaler Console.
- **display-name** : Un nom descriptif pour le StyleBook qui apparaît sur NetScaler Console.
- **namespace** : Un espace de noms fait partie d'un identifiant unique pour un StyleBook afin d'éviter les conflits de noms.
- **schema-version** : Prend toujours la valeur « 1.0 » dans cette version.
- **version** : Le numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour le StyleBook.

La combinaison de **name**, **namespace** et **version** identifie de manière unique un StyleBook dans le système. Vous ne pouvez pas avoir deux StyleBooks avec la même combinaison de nom, d'espace de noms et de version dans NetScaler Console. Cependant, vous pouvez avoir deux StyleBooks avec le même nom et la même version mais des espaces de noms différents, ou avec le même espace de noms et la même version mais des noms différents.

REMARQUE

Considérez que vous avez mis à jour votre StyleBook et que vous avez un numéro de version mis à jour. Maintenant, si vous faites référence à (c'est-à-dire, si vous importez) ce StyleBook dans d'autres StyleBooks, assurez-vous de mettre à jour le numéro de version dans les autres StyleBooks également, afin qu'ils utilisent la version correcte du StyleBook importé.

Importer des StyleBooks

La section après l'en-tête est appelée « import-stylebooks ». Dans cette section, vous devez déclarer l'espace de noms et le numéro de version de tout autre StyleBook auquel vous souhaitez faire référence dans votre StyleBook actuel. Cela vous permet d'importer et de réutiliser d'autres StyleBooks au lieu de reconstruire la même configuration dans votre propre StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, la section import-stylebooks est écrite comme suit :

```
import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"
```

Chaque StyleBook doit faire référence à l'espace de noms netscaler.nitro.config s'il utilise directement l'un des objets de configuration NITRO. Cet espace de noms contient tous les types NetScaler NITRO, tels que lbvserver. Les versions logicielles 10.5 et ultérieures étant prises en charge, vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur toute instance NetScaler exécutant la version 10.5 ou ultérieure.

Le préfixe utilisé dans la section import-stylebooks est un raccourci pour faire référence à la combinaison de l'espace de noms et de la version. Dans ce cas, ns fait référence à netscaler.nitro.config de la version 10.5. Dans les sections ultérieures de votre StyleBook, au lieu d'utiliser l'espace de noms et la version pour faire référence au StyleBook importé, vous pouvez utiliser la chaîne de préfixe choisie, par exemple, ns, dans l'exemple ci-dessus.

La version utilisée dans les StyleBooks est la version NetScaler NITRO. Un StyleBook basé sur la version Nitro X peut être utilisé pour configurer tout NetScaler de version X ou supérieure.

REMARQUE

Pour vous assurer que vos StyleBooks peuvent être utilisés pour configurer toute instance NetScaler de version 10.5 ou ultérieure, nous recommandons, pour une compatibilité maximale, d'importer l'espace de noms Nitro 10.5 dans vos StyleBooks qui utilisent directement les StyleBooks intégrés de Nitro (espace de noms : netscaler.nitro.config, version : 10.5).

Il est important qu'un StyleBook qui importe d'autres StyleBooks soit basé sur une version Nitro égale ou supérieure à celle des StyleBooks qu'il importe. Par exemple, un StyleBook basé sur la version Nitro 10.5 ne peut pas dépendre, utiliser ou importer un StyleBook basé sur la version

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11.1. Mais un StyleBook basé sur la version 11.1 peut importer un StyleBook basé sur toute version inférieure à 11.1.

Il est également possible qu'un StyleBook n'importe pas du tout l'espace de noms Nitro. Cela signifie qu'un StyleBook n'a pas besoin de définir directement des composants Nitro, mais peut importer (dépendre de) des StyleBooks qui définissent des composants Nitro. Le StyleBook qui importe d'autres StyleBooks acquiert toujours la version Nitro la plus élevée dans la hiérarchie de ses dépendances et pourrait donc être utilisé pour configurer des NetScalers de cette version ou d'une version supérieure.

Paramètres

La section des paramètres vous permet de déclarer tous les paramètres dont vous avez besoin dans votre StyleBook. En tant que développeur de StyleBook, vous devez décider quelle est l'entrée que vous souhaitez que les utilisateurs de votre StyleBook spécifient. Dans cet exemple, vous avez construit votre StyleBook de manière à ce que ses utilisateurs doivent fournir le nom du serveur virtuel, son adresse IP et la méthode d'équilibrage de charge.

La section des paramètres se présenterait comme suit :

```
parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Name of the application configuration.

  required: true



 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  description: Application VIP that the clients access.

  required: true



-

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the load balancing algorithm (method) used for load
balancing client request between the application servers.

  allowed-values:

   - ROUNDROBIN

   - LEASTCONNECTION

   default: ROUNDROBIN
```

REMARQUE

Si vous ne fournissez pas l'étiquette d'un paramètre, NetScaler Console utilise l'attribut de nom lors de l'affichage de ce paramètre. Vous devez toujours définir une étiquette pour vos paramètres afin de pouvoir contrôler la façon dont ils apparaissent dans NetScaler Console.

Cependant, lors de l'utilisation des API, le paramètre est désigné par son nom.
Dans cette section, vous avez déclaré trois paramètres indiqués par les valeurs de leur attribut **name** : **name** pour le nom du serveur virtuel, **ip** pour l'adresse IP du serveur virtuel et **lb-alg** pour la méthode d'équilibrage de charge.

- **type**. Type de valeur que ces paramètres peuvent prendre. Par exemple, name et lb-alg peuvent prendre une valeur de type chaîne de caractères et la valeur ip doit être de type adresse IP. Les paramètres d'un StyleBook peuvent être de l'un des types intégrés suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **string**. Un tableau de caractères. Si une longueur n'est pas spécifiée, la valeur de la chaîne peut prendre n'importe quel nombre de caractères. Cependant, vous pouvez limiter la longueur d'un type de chaîne en utilisant les attributs min-length et max-length.
- **number**. Un nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs min-value et max-value.
- **boolean**. Peut être vrai ou faux. Notez également que tous les littéraux sont considérés par YAML comme des booléens (par exemple, Yes ou No).
- **ipaddress**. Une chaîne qui représente une adresse IPv4 ou IPv6 valide.
- **tcp-port**. Un nombre entre 0 et 65535 qui représente un port TCP ou UDP.
- **password**. Une valeur de chaîne opaque/secrète. Lorsque NetScaler Console affiche une valeur pour ce paramètre, elle est représentée par des astérisques (*****).
- **certfile**. Fichier de certificat.
- **keyfile**. Fichier de clé privée de certificat.
- **file**. Un paramètre de ce type exige que l'utilisateur télécharge un fichier, par exemple, un certificat ou un fichier de clé.
- **object**. Se compose de plusieurs éléments et chacun de ces éléments est un paramètre. Ce type peut être utilisé pour regrouper plusieurs paramètres liés sous un seul paramètre parent.
- **required**. Indique si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création de configurations à l'aide de ce StyleBook. Par défaut, tous les paramètres sont facultatifs. Dans cet exemple, **name** et **ip** sont des paramètres obligatoires, tandis que **lb-alg** est un paramètre facultatif, dont la valeur par défaut est "ROUNDROBIN".

Utilisez l'attribut **default** pour attribuer une valeur par défaut à un paramètre facultatif. Lors de la création d'une configuration, si un utilisateur ne spécifie pas de valeur, la valeur par défaut est utilisée. Par exemple, pour le paramètre **lb-alg**, la valeur par défaut est ROUNDROBIN.

Utilisez l'attribut **allowed-values** pour définir des valeurs spécifiques qu'un utilisateur peut choisir lors de la création d'une configuration. Dans cet exemple, vous avez spécifié deux valeurs pour le paramètre **lb-alg** : ROUNDROBIN et LEASTCONNECTION.

Lorsque vous importez votre StyleBook et l'utilisez, NetScaler Console affiche un formulaire avec ces trois paramètres. Les champs affichés pour le nom et l'adresse IP permettent de saisir des valeurs de type chaîne de caractères et adresse IP, et le champ lb-alg est affiché sous forme de liste déroulante avec ROUNDROBIN sélectionné comme valeur par défaut.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

En plus des types intégrés, un paramètre peut avoir un autre StyleBook comme type. C'est un moyen de réutiliser les paramètres définis dans d'autres StyleBooks.

Composants

La dernière section de ce StyleBook est appelée la section des composants et est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration qui doivent être créés par le StyleBook.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: HTTP

   ipv46: $parameters.ip

   port: 80

   lbmethod: $parameters.lb-alg
```

Cet exemple ne contient qu'un seul composant. Les principaux attributs d'un composant sont le nom, le type et les propriétés. Le type d'un composant détermine les propriétés qu'il fournit. Les composants sont de deux types :

- **Type intégré**. Ce type est fourni par le système et vous n'avez pas à le définir, par exemple, les types d'entités NITRO « lbvserver » ou « servicegroup ». Dans cet exemple, vous utilisez un type de composant intégré.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Type composite**. Ce type est le StyleBook que vous avez créé et importé dans NetScaler Console, ou le StyleBook par défaut fourni avec NetScaler Console. Vous pouvez en savoir plus sur les StyleBooks composites dans Créer un StyleBook composite.

Dans cet exemple, vous avez défini un composant appelé **lbvserver-comp**. Ce composant est de type **ns::lbvserver** (un type Nitro intégré), où « ns » est le préfixe qui fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5 que vous aviez spécifiés dans la section import-stylebooks, et « lbvserver » est une ressource Nitro dans cet espace de noms.

Les **propriétés** définies ici sont les attributs de la ressource « lbvserver ». Pour en savoir plus sur toutes les ressources NetScaler Nitro disponibles et leurs attributs, consultez la documentation de l'API REST NetScaler NITRO.

Les propriétés de cette section incluent les attributs obligatoires de la ressource « lbvserver » et vous permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour servicetype et port, tandis que les propriétés name, ipv46 et lbmethod obtiennent leurs valeurs des paramètres d'entrée. Dans le reste du StyleBook, vous pouvez faire référence aux noms de paramètres définis dans la section des paramètres en utilisant l'expression **$parameters.\<parameter-name\>**, par exemple, **$parameters.ip**.

REMARQUE

Par convention, le préfixe « ns » est toujours utilisé pour désigner un espace de noms NetScaler Nitro dans la section « import-stylebooks ». Bien que cela ne soit pas obligatoire, Citrix recommande d'utiliser la même convention dans vos propres StyleBooks pour des raisons de cohérence.

Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, rassemblez-les toutes pour créer votre premier StyleBook. Copiez et collez le contenu du StyleBook dans un éditeur de texte, puis enregistrez le fichier sous le nom **lb-vserver.yaml**. Nous vous recommandons d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier lb-vserver.yaml est reproduit ci-dessous :

```
name: lb-vserver

namespace: com.example.stylebook
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

 -

  namespace: com.citrix.adc.stylebooks

  version: "1.0"

  prefix: stlb



parameters:

 -

  name: name

  label: "Application Name"

  description: "Give a name to the application configuration."

  type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  required: true

 -

  name: vip-ipaddress

  label: "Load Balancer IP Address"

  description: "The Application VIP that clients access"

  type: ipaddress

  required: true

 -

  name: lb-alg

  label: LB Algorithm

  description: Load Balancing Algorithm

  type: string

  default: ROUNDROBIN

  allowed-values:

   - ROUNDROBIN

   - LEAST-CONNECTION



components:

 -

  name: lbvserver-comp

  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler load balancing virtual server configuration object.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: ns::lbvserver

properties:

 name: $parameters.name

 ipv46: $parameters.vip-ipaddress

 lbmethod: $parameters.lb-alg

 servicetype: HTTP

 port: 80
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans NetScaler Console, puis l'utiliser. Pour plus d'informations, consultez Comment utiliser les StyleBooks définis par l'utilisateur.

Vous pouvez également importer ce StyleBook dans d'autres StyleBooks (en utilisant la construction import-stylebooks). Ou, vous pouvez modifier ce StyleBook pour inclure davantage de paramètres et de composants, comme décrit dans la section suivante.

StyleBook pour créer une configuration de répartition de charge de base

Dans l'exemple précédent, vous avez créé un StyleBook de base pour créer un serveur virtuel de répartition de charge. Vous pouvez enregistrer ce StyleBook sous un nom différent, puis le mettre à jour pour inclure des paramètres et des composants supplémentaires pour une configuration de répartition de charge de base. Enregistrez ce fichier StyleBook sous le nom **basic-lb-config.yaml**.

Dans cette section, vous allez concevoir un nouveau StyleBook qui crée une configuration de répartition de charge comprenant un serveur virtuel de répartition de charge, un groupe de services et une liste de services. Il lie également les services au groupe de services et lie le groupe de services au serveur virtuel.

En-tête

Pour créer ce StyleBook, vous devez commencer par mettre à jour la section d'en-tête. Cette section est similaire à celle que vous avez créée pour le StyleBook du serveur virtuel de répartition de charge. Dans la section d'en-tête, modifiez la valeur de **name** en basic-lb-config. Mettez également à jour **description** et **display-name** pour décrire ce StyleBook de manière appropriée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous n'avez pas à modifier les valeurs de **namespace** et **version**. Étant donné que vous avez modifié le nom, la combinaison du nom, de l'espace de noms et de la version crée un identifiant unique pour ce StyleBook dans le système.

```
name: basic-lb-config

description: This StyleBook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"
```

Importer des StyleBooks

La section import-stylebooks reste la même. Elle fait référence à l'espace de noms netscaler.nitro.config pour utiliser les objets de configuration Nitro.

```
import-stylebooks:

 -

 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

Paramètres

Vous devez mettre à jour la section des paramètres pour ajouter deux paramètres supplémentaires afin de définir la liste des services ou des serveurs et le port sur lequel les services écoutent. Les trois premiers paramètres, name, ip et lb-alg, restent les mêmes.

```
parameters:

 -

 name: name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 type: string

 label: Application Name

 description: Name of the application configuration

 required: true

  -

   name: ip

   type: ipaddress

   label: Application Virtual IP (VIP)

   description: Application VIP that the clients access

   required: true

  -

   name: lb-alg

   type: string

   label: LoadBalancing Algorithm

   description: Choose the load balancing algorithm used for load
balancing client requests between the application servers.

     allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

      default: ROUNDROBIN

  -

   name: svc-servers
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ipaddress\[\]

    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true

   -

    name: svc-port

    type: tcp-port

    label: Server Port

    description: The TCP port open on the application servers to receive
requests.

    default: 80
```

Dans cet exemple, le paramètre **svc-servers** est ajouté pour accepter une liste d'adresses IP des services qui représentent les serveurs backend de l'application. Il s'agit d'un paramètre obligatoire, comme indiqué par **required: true**. Le second paramètre, **svc-port**, indique le numéro de port sur lequel les serveurs écoutent. Le numéro de port par défaut est 80 pour le paramètre svc-port, s'il n'est pas spécifié par l'utilisateur.

Composants

Vous devez également mettre à jour la section des composants pour définir des composants supplémentaires afin qu'ils utilisent les deux nouveaux paramètres et construisent la configuration complète de répartition de charge.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg


components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP


components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver\_servicegroup\_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

 name: members-svcg-comp

 type: ns::servicegroup\_servicegroupmember\_binding

 repeat: $parameters.svc-servers

 repeat-item: srv

 properties:

  ip: $srv

  port: str($parameters.svc-port)

  servicegroupname: $parent.properties.name
```

Dans cet exemple, le composant original **lbvserver-comp** (de l'exemple précédent) a maintenant un composant enfant appelé **svcg-comp**. Et le composant **svcg-comp** contient deux composants enfants. L'imbrication d'un composant dans un autre permet au composant imbriqué de créer des objets de configuration en se référant aux attributs du composant parent. Le composant imbriqué peut créer un ou plusieurs objets pour chaque objet créé dans le composant parent.

Le composant **svcg-comp** est utilisé pour créer un groupe de services sur l'instance NetScaler en utilisant les valeurs fournies pour les attributs de la ressource « servicegroup ». Dans cet exemple, vous spécifiez une valeur statique pour servicetype, tandis que name obtient sa valeur du paramètre d'entrée. Vous faites référence au paramètre **name** défini dans la section des paramètres en utilisant la notation **$parameters.name + "-svcgrp"**, où **-svcgrp** est ajouté (concaténé) au nom défini par l'utilisateur.

Le composant **svcg-comp** a deux composants enfants, **lbvserver-svg-binding-comp** et **members-svcg-comp**.

Le premier composant enfant, **lbvserver-svg-binding-comp**, est utilisé pour lier un objet de configuration entre le groupe de services créé par son composant parent et le serveur virtuel d'équilibrage de charge (lbvserver) créé par le composant parent du parent. La notation $parent, également appelée référence parent, est utilisée pour faire référence aux entités dans les composants parents. Par exemple, **servicegroupname: $parent.properties.name** fait référence au groupe de services créé par le composant parent **svcg-comp**, et **name:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

$parent.parent.properties.name fait référence au serveur virtuel créé par le composant parent du parent **lbvserver-comp**.

Le composant **members-svcg** est utilisé pour lier des objets de configuration entre la liste des services et le groupe de services créé par le composant parent. La création de plusieurs objets de configuration de liaison est réalisée en utilisant la construction **repeat** de StyleBook pour itérer sur la liste des serveurs spécifiés dans le paramètre **svc-servers**. Pendant l'itération, ce composant StyleBook crée un objet de configuration Nitro de type **servicegroup_servicegroupmember_binding** pour chaque service (appelé srv dans la construction **repeat-item**) dans le groupe de services, et il définit l'attribut **ip** dans chaque objet de configuration Nitro sur l'adresse IP du serveur correspondant.

Généralement, vous pouvez utiliser les constructions **repeat** et **repeat-item** dans un composant pour que ce composant crée plusieurs objets de configuration du même type. Vous pouvez attribuer un nom de variable à la construction **repeat-item**, par exemple, srv, pour désigner la valeur actuelle dans l'itération. Ce nom de variable est référencé dans les propriétés du même composant ou dans les composants enfants comme **$\<varname\>**, par exemple $srv.

Dans l'exemple ci-dessus, vous avez utilisé l'imbrication de composants les uns dans les autres pour construire facilement cette configuration. Dans ce cas particulier, l'imbrication de composants n'était pas la seule façon de construire la configuration. Vous auriez pu obtenir le même résultat sans imbrication, comme indiqué ci-dessous :

```
components:

 -

  name: members-svcg-comp

  type: ns::servicegroup\_servicegroupmember\_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

   ip: $srv

   port: str($parameters.svc-port)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  servicegroupname: $components.svcg-comp.properties.name
-
 name: lbvserver-svg-binding-comp
 type: ns::lbvserver\_servicegroup\_binding
 properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.name
-
 name: lbvserver-comp
 type: ns::lbvserver
 properties:
  name: $parameters.name + "-lb"
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg
-
 name: svcg-comp
 type: ns::servicegroup
 properties:
 name: $parameters.name + "-svcgrp"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  servicetype: HTTP
```

Ici, tous les composants sont au même niveau (c'est-à-dire qu'ils ne sont pas imbriqués) mais le résultat obtenu (la configuration NetScaler générée) est le même que celui des composants imbriqués utilisés précédemment. De plus, l'ordre dans lequel les composants sont déclarés dans le StyleBook n'a pas d'impact sur l'ordre de création des objets de configuration. Dans cet exemple, les composants **svcg-comp** et **lbvserver-comp**, bien que déclarés en dernier, doivent être construits avant de construire le deuxième composant **lbvserver-svg-binding-comp** car il existe des références anticipées à ces composants dans le deuxième composant.

REMARQUE

Par convention, les noms des StyleBooks, des paramètres, des substitutions, des composants et des sorties sont en minuscules. Lorsqu'ils contiennent plusieurs mots, ils sont séparés par un caractère « - ». Par exemple, « lb-bindings », « app-name », « rewrite-config », etc. Une autre convention consiste à suffixer les noms de composants avec la chaîne « -comp ».

Sorties

La dernière section que vous pouvez ajouter au nouveau StyleBook est la section des sorties, où vous spécifiez ce que ce StyleBook expose à ses utilisateurs (ou à d'autres StyleBooks) après avoir été utilisé pour créer une configuration. Par exemple, vous pouvez spécifier dans la section des sorties d'exposer les objets de configuration lbvserver et servicegroup qui seraient créés par ce StyleBook.

```
outputs:

 -

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

La section des sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer de sorties. Cependant, en renvoyant certains composants internes comme sorties, il offre plus de flexibilité à tout StyleBook qui importe ce StyleBook, comme vous pouvez le constater lors de la création d'un StyleBook composite.

REMARQUE

Il est recommandé d'exposer un composant entier du StyleBook dans la section des sorties, plutôt qu'une seule propriété d'un composant (par exemple, exposez l'ensemble de $components.lbvserver-comp plutôt que seulement le nom $components.lbvserver-comp.properties.name). Ajoutez également une description à la sortie expliquant ce que représente la sortie spécifique.

Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, rassemblez-les toutes pour construire votre deuxième StyleBook. Vous avez déjà enregistré ce fichier StyleBook sous le nom **basic-lb-config.yaml**. Nous vous recommandons d'utiliser le validateur YAML intégré dans la page StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier **basic-lb-config.yaml** est reproduit ci-dessous :

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.

schema-version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true



components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP

   ipv46: $parameters.ip
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  port: 80
  lbmethod: $parameters.lb-alg
-
 name: svcg-comp
 type: ns::servicegroup
 properties:
   servicegroupname: $parameters.name + "-svcgrp"
   servicetype: HTTP


-
 name: lbvserver-svg-binding-comp
 type: ns::lbvserver_servicegroup_binding
 properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.servicegroupname
-
 name: members-svcg-comp
 type: ns::servicegroup_servicegroupmember_binding
 repeat: $parameters.svc-servers
 repeat-item: srv
 properties:
  ip: $srv
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname

outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans NetScaler Console, puis l'utiliser. Pour plus d'informations, consultez Comment utiliser les StyleBooks définis par l'utilisateur.

Vous pouvez également importer ce StyleBook dans d'autres StyleBooks et utiliser ses propriétés comme décrit dans la section suivante.

Créer un StyleBook composite

Une caractéristique importante et puissante des StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Un StyleBook peut être importé dans un autre StyleBook et il peut être désigné comme un **type** utilisé par les composants du second StyleBook, de manière similaire à un StyleBook intégré Nitro.

Par exemple, vous pouvez utiliser le StyleBook **basic-lb-config** que vous avez créé dans la section précédente, pour créer un autre StyleBook appelé **composite-example**. Pour utiliser le

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook « basic-lb-config », vous devez l'importer dans le nouveau StyleBook dans la section import-stylebooks.

Créez votre StyleBook

Le nouveau StyleBook se présenterait comme suit :

```
name: composite-example

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (HTTP/RoundRobin)

description: This StyleBook defines a RoundRobin load balancing
configuration with a monitor.

schema-version: "1.0"

import-stylebooks:

  -

   namespace: netscaler.nitro.config

   version: "10.5"

   prefix: ns

  -

   namespace: com.example.stylebooks

   version: "0.1"

   prefix: stlb

parameters:

  -

    name: name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true


  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response codes
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
in integer.



components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config

    description: This component's type is another StyleBook that builds
the NetScaler lbvserver, servicegroups and services configuration objects.

    properties:

     name: $parameters.name

     ip: $parameters.ip

     svc-servers: $parameters.svc-servers

  -

     name: monit-comp

     type: ns::lbmonitor

     description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.

     properties:

       monitorname: $parameters.name + "-mon"

       type: HTTP

       respcode: $parameters.response-code

       httprequest: "'GET /'"

       lrtm: ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      secure: "YES"



    components:

       -

         name: monit-svcgrp-bind-comp

         type: ns::servicegroup_lbmonitor_binding

         properties:

           servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname

           monitor_name: $parent.properties.monitorname
```

Dans la section import-stylebooks, vous importez le StyleBook basic-lb-config en utilisant son espace de noms et sa version, désignés par le préfixe « stlb ».

Dans la section des composants, deux composants sont définis. Le premier composant est de type **stlb::basic-lb-config**, où « basic-lb-config » est le nom du StyleBook que vous avez créé dans StyleBook pour créer une configuration d'équilibrage de charge de base. Les propriétés définies pour ce composant correspondent aux paramètres obligatoires déclarés dans le StyleBook basic-lb-config. Vous pouvez, cependant, utiliser n'importe quel paramètre du StyleBook (obligatoire et facultatif). Au lieu de reconstruire un lbvserver, un groupe de services et des liaisons de services et de groupes de services, vous importez le StyleBook qui fait tout cela en tant que composant et l'utilisez pour créer ces objets de configuration dans le nouveau StyleBook.

StyleBook ajoute un second composant « monit-comp » qui utilise les attributs de la ressource Nitro « lbmonitor » (un StyleBook intégré) pour créer un objet de configuration de moniteur. Il dispose également d'un sous-composant « monit-svcgrp-bind-comp » pour créer l'objet de configuration de liaison qui lie le moniteur au groupe de services créé dans le premier composant. Étant donné que le composant de groupe de services créé dans le StyleBook « basic-lb-config » est exposé en tant que sortie, ce StyleBook peut y accéder à l'aide de l'expression **$components.basic-lb-comp.outputs.servicegroup-comp**. Ceci est un exemple de la façon

© 1997–2026 Citrix Systems, Inc. All rights reserved.

dont la section des sorties peut être utilisée par les StyleBooks importateurs pour avoir accès aux composants des StyleBooks importés auxquels ils n'auraient pas pu accéder autrement.

Ensuite, copiez et collez le contenu du StyleBook dans un éditeur de texte, puis enregistrez le fichier sous le nom **composite-example.yaml**. Assurez-vous de valider le contenu YAML avant d'importer le fichier dans NetScaler Console. Ensuite, importez-le dans NetScaler Console et créez une ou plusieurs configurations à l'aide de ce StyleBook.

Nous vous recommandons d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Utiliser les attributs d'interface graphique dans un StyleBook personnalisé

Vous pouvez ajouter des attributs d'interface graphique dans la section des paramètres de votre StyleBook pour rendre les champs intuitifs lorsqu'ils sont affichés sur NetScaler Console.

Exemple. Vous pouvez ajouter un nom descriptif pour le paramètre en utilisant l'attribut label, et ajouter une info-bulle pour ce paramètre en utilisant l'attribut description.

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.

type: ipaddress

required: true
```

Exemple. Si vous avez un paramètre de type objet, vous pouvez définir la mise en page en utilisant l'attribut **gui**. Dans cet exemple, la mise en page est un objet réductible où les champs sont affichés en deux colonnes.

```
name: svcg-advanced

label: Advanced Application Server Settings

type: object
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
required: false

gui:

 collapse_pane: true

 columns: 2
```

Exemple. Certains StyleBooks sur NetScaler Console sont utilisés uniquement comme blocs de construction pour d'autres StyleBooks. Et, vous ne voudrez peut-être pas que les utilisateurs créent des configurations directement à partir de ces StyleBooks. Car ces StyleBooks doivent être utilisés dans le cadre d'autres StyleBooks. Marquez le StyleBook comme privé pour vous assurer qu'il n'est pas utilisé directement pour créer des configurations dans l'interface graphique de NetScaler Console.

```
name: basic-lb-config

description: This stylebook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

private: true

schema-version: "1.0"

version: "0.1"
```

Importer des StyleBooks personnalisés

Après avoir créé votre StyleBook, vous devez l'importer dans NetScaler Console pour l'utiliser. NetScaler Console vous permet d'importer un seul StyleBook au format YAML ou plusieurs fichiers YAML de StyleBook sous forme de bundle dans un format .zip, .tgz ou .gz. Le système NetScaler Console valide vos StyleBooks lors de l'importation. Le StyleBook est maintenant prêt à être utilisé pour créer des configurations.

NetScaler Console dispose également d'un éditeur YAML intégré que vous pouvez utiliser pour composer le contenu YAML du StyleBook. L'éditeur YAML vous permet de valider vos constructions YAML directement depuis l'interface graphique de NetScaler Console. Vous n'avez

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pas besoin d'utiliser un outil séparé pour ces vérifications de validation. Le contenu est validé par rapport aux normes YAML et toute déviation est mise en évidence. Vous pouvez ensuite corriger le contenu et tenter d'importer le StyleBook dans NetScaler Console. L'éditeur YAML intégré offre deux avantages lors de la rédaction de votre propre StyleBook.

- **Code couleur**. L'éditeur affiche le contenu du StyleBook analysé selon les directives YAML, et le code couleur vous aide à différencier facilement les clés et les valeurs définies dans le contenu YAML.
- **Validation YAML**. Le contenu est validé pour détecter toute erreur YAML au fur et à mesure que vous tapez, et toute déviation est immédiatement mise en évidence. Cette validation vous permet d'écrire du texte conforme aux directives YAML avant même d'importer le StyleBook dans NetScaler Console.

REMARQUE :

Actuellement, l'éditeur valide le contenu selon les directives YAML. Il ne valide pas la correction du code ni les erreurs typographiques.

Pour importer votre StyleBook

1. Dans NetScaler Console, accédez à **Applications** > **Configuration** > **StyleBooks**, puis cliquez sur **Importer un nouveau StyleBook**.
2. Cliquez sur l'une des options suivantes pour importer un StyleBook.

   - **Fichier** - sélectionnez le fichier requis ou le bundle de fichiers depuis votre stockage local.

     REMARQUE :

     Dans cet exemple, importez le StyleBook `lb-vserver.yml` que vous avez créé dans StyleBook pour créer un serveur virtuel d'équilibrage de charge.

     

   - **Bundle** - NetScaler Console vous permet d'importer plusieurs StyleBooks au format YAML. Vous pouvez importer plusieurs fichiers StyleBook YAML compressés au format zip (.zip) ou tarball (.tgz, .gz).

     

     Vous pouvez maintenant inclure des icônes à chaque StyleBook du bundle. Assurez-vous d'avoir le dossier de ressources qui contient des icônes aux formats PNG, GIF ou JPEG. Si

© 1997–2026 Citrix Systems, Inc. All rights reserved.

le nom du fichier d'icône correspond au nom du StyleBook, les icônes sont automatiquement mappées aux StyleBooks. Sinon, procédez comme suit :

a. Ajoutez le fichier `icon_mapping.json` dans le dossier des ressources.

b. Mappez les StyleBooks et les icônes dans le fichier `icon_mapping.json` comme suit :

```
<StyleBook file name> : <icon file name>
```

Voici un exemple de bundle StyleBook :

- [ ] Le dossier `resources` contient les icônes requises.

- [ ] Dans cet exemple, les fichiers `sharepoint.yaml` et `skype.yaml` sont automatiquement mappés à `sharepoint.jpeg` et `skype.png` respectivement.

Pour mapper `exchange.yaml` à `exch.png`, spécifiez ce qui suit dans le fichier `icon_mapping.json` :

```
{

"exchange.yaml":"exch.png"

}
```

Si vous spécifiez l'entrée `defaulticon`, les StyleBooks sont mappés à l'icône par défaut, sauf s'ils sont mappés à une icône différente.

```
defaulticon: <icon file name>
```

Dans **Applications > StyleBooks**, les StyleBooks importés apparaissent avec les icônes mappées.

- **Brut** - Composez le contenu de votre StyleBook dans l'éditeur YAML.

  Vous pouvez valider le contenu du StyleBook pour vérifier les erreurs de grammaire du StyleBook. Pour valider le contenu du StyleBook, cliquez sur **Valider le contenu**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Lors de la composition d'un StyleBook, assurez-vous de connaître les concepts suivants :

- NITRO API
- YAML

Pour plus d'informations sur la façon de créer vos propres StyleBooks, consultez Comment créer vos propres StyleBooks.

- **Synchroniser le référentiel** - Cette option répertorie les référentiels ajoutés à NetScaler Console. Sélectionnez le référentiel que vous souhaitez synchroniser avec NetScaler Console.

REMARQUE :

Vous pouvez également copier-coller le contenu d'un fichier YAML StyleBook dans l'éditeur YAML.

3. Facultatif, sélectionnez une icône pour un StyleBook.

   Dans **Applications > StyleBook**, le StyleBook importé apparaît avec cette icône.

4. Cliquez sur **Créer**.

   NetScaler Console valide maintenant votre StyleBook pour toutes les erreurs syntaxiques et sémantiques conformément à la grammaire StyleBook. Votre StyleBook n'est pas importé dans NetScaler Console s'il y a des erreurs.

   S'il n'y a pas d'erreurs, le StyleBook est importé avec succès et répertorié sur la page **StyleBooks**. Vous pouvez identifier le StyleBook par le nom d'affichage que vous avez défini dans la section d'en-tête du StyleBook.

REMARQUE :

Si vous importez un ensemble de fichiers, NetScaler Console décompresse le dossier compressé et valide tous les StyleBooks. Le bundle n'est pas importé même si un seul fichier StyleBook échoue au test de validation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations sur la grammaire et la syntaxe des différentes constructions et attributs de StyleBook, consultez Grammaire StyleBook.

5. Cliquez sur le lien **Créer une configuration** pour créer des configurations à partir de ce StyleBook.

   Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.

6. Spécifiez les valeurs requises pour les paramètres.

   Dans l'exemple suivant,

   a. Spécifiez les champs obligatoires **nom de l'application** et **adresse IP de l'équilibreur de charge**.

   b. Sélectionnez l'**algorithme d'équilibrage de charge** dans la liste. Par défaut, **ROUNDROBIN** est sélectionné.

7. Sous **Instances cibles**, sélectionnez l'adresse IP de l'instance NetScaler sur laquelle vous souhaitez déployer la configuration.

   Vous pouvez également déployer la configuration sur plusieurs NetScaler, en spécifiant autant d'instances cibles que nécessaire.

8. Si vous souhaitez tester les objets de configuration NetScaler (NITRO) avant de déployer la configuration, cliquez sur **Exécution à blanc**.

   Si la configuration est valide, les objets de configuration sont créés en fonction des valeurs spécifiées.

   Dans cet exemple, le StyleBook ne crée qu'un seul objet de type `lbvserver`. Ce serveur d'équilibrage de charge était le seul composant défini dans cet exemple de StyleBook de base.

   Ensuite, cliquez sur **Créer** pour déployer la configuration sur les instances NetScaler sélectionnées.

Après avoir déployé la configuration avec succès, un nouveau pack de configuration apparaît dans la page **Configurations**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

Rechercher des StyleBooks personnalisés

NetScaler Console vous permet désormais de rechercher des StyleBooks en fonction de leur type. Autrement dit, vous pouvez désormais rechercher des StyleBooks par défaut ou des StyleBooks personnalisés. Cette option est particulièrement utile lorsque vous devez rechercher vos StyleBooks définis par l'utilisateur parmi de nombreux StyleBooks par défaut.

Pour rechercher des StyleBooks personnalisés

1. Dans NetScaler Console, accédez à **Applications** > **Configurations** > **StyleBooks**.
2. Cliquez sur l'icône de recherche en haut à droite.
3. Dans la barre de recherche, sélectionnez **Type**, puis sélectionnez **Personnalisé** dans la sous-liste.
4. NetScaler Console affiche uniquement les StyleBooks définis par l'utilisateur.

Créer et modifier un pack de configuration

Dans NetScaler Console, vous pouvez créer un pack de configuration à partir d'un StyleBook. Le pack de configuration est lié au StyleBook à partir duquel il est créé. Les mises à jour du pack de configuration sont effectuées via le StyleBook auquel il est lié.

Créer un pack de configuration

Effectuez les opérations suivantes pour créer un pack de configuration à partir d'un StyleBook :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Cliquez sur **Ajouter**.
3. Dans **Choisir des StyleBooks**, sélectionnez les StyleBooks requis à partir desquels vous souhaitez créer un pack de configuration.

   Cette page classe les StyleBooks en StyleBooks par défaut et StyleBooks personnalisés. Sélectionnez les onglets respectifs pour trouver les StyleBooks requis.
4. Spécifiez les détails requis tels que le nom de l'application, l'adresse IP, le port ou le type de protocole.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les champs de l'interface graphique diffèrent d'un StyleBook à l'autre.

5. Dans **Instances cibles**, sélectionnez les instances ou les groupes d'instances sur lesquels vous souhaitez exécuter la configuration.

   REMARQUE :

   Vous pouvez déployer la configuration sur plusieurs NetScaler, en spécifiant autant d'instances cibles que nécessaire.

6. Cliquez sur **Exécution à blanc**.

   La page **Objets** affiche les objets qui sont créés, modifiés ou supprimés des instances NetScaler.

7. Cliquez sur **Create**

   Le pack de configuration apparaît dans la page **StyleBook > Configurations**.

Si vous souhaitez modifier les packs de configuration existants, sélectionnez le pack de configuration et cliquez sur **Edit**.

Réutiliser les configurations créées en dehors des StyleBooks et partager les configurations entre les ConfigPacks

Il peut arriver que vous ayez créé des configurations NetScaler® en dehors des Stylebooks, que ce soit en raison de besoins opérationnels spécifiques ou de configurations héritées. Vous pouvez désormais intégrer et gérer ces configurations préexistantes dans le cadre des packs de configuration Stylebook, permettant une gestion plus flexible et centralisée.

Par exemple, avant cette fonctionnalité, si NetScaler est déjà configuré avec un profil SSL, et si l'opération de pack de configuration de StyleBook tente de créer un profil SSL portant le même nom, l'opération de pack de configuration aurait échoué avec l'erreur « Resource Already Exists ». Maintenant, avec cette fonctionnalité activée, l'opération de pack de configuration réussit et le profil SSL existant portant le même nom peut être réutilisé dans le nouveau pack de configuration.

De même, vous pourriez également être confronté à des scénarios où des ressources telles que les paramètres réseau, les politiques de sécurité ou une partie des configurations d'application sont requises pour plusieurs applications ou configurations. Cette fonctionnalité vous permet de partager les configurations entre plusieurs packs de configuration.

Pour activer cette fonctionnalité, suivez ces étapes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à Applications > Configuration > Stylebooks.
2. Sur la page Stylebooks, sélectionnez le Stylebook que vous utiliserez pour créer un nouveau pack de configuration ou celui associé au pack de configuration que vous modifiez.
3. Dans Sélectionner l'action, cliquez sur Configurer les paramètres.
4. Ajustez les paramètres en choisissant une ou les deux options suivantes :
   - Pour permettre la réutilisation des ressources existantes sur le NetScaler lors de la création de configurations, sélectionnez l'option **Allow reuse of existing resources on the NetScaler while creating configuration(s)**.
   - Pour conserver les ressources réutilisées sur le NetScaler lors de la suppression de configurations, sélectionnez l'option **Retain reused resources on the NetScaler when deleting configuration(s)?**. Cette option conserve les ressources initialement créées en dehors des Stylebooks sur le NetScaler, même si le dernier pack de configuration les référençant est supprimé, assurant leur disponibilité continue.
5. Cliquez sur **OK**.

Modifier le StyleBook d'un pack de configuration

Parfois, vous devez mettre à jour le StyleBook pour ajouter des fonctionnalités ou corriger un problème. Si vous avez déjà créé des packs de configuration à l'aide de l'ancien StyleBook, vous souhaiterez peut-être les mettre à jour pour utiliser le nouveau StyleBook mis à jour. Pour utiliser un nouveau StyleBook, modifiez le StyleBook existant du pack de configuration.

Prenons l'exemple d'un StyleBook **example-lb** qui déploie une configuration de base d'équilibreur de charge sur une instance NetScaler. Et, vous créez un pack de configuration CP1 à partir de ce StyleBook.

Lorsque vous souhaitez configurer des moniteurs avec la configuration de base de l'équilibreur de charge, vous avez besoin d'un nouveau StyleBook. Par conséquent, créez le StyleBook **example-lb-mon** qui inclut la possibilité de configurer des moniteurs en plus de la configuration de base de l'équilibreur de charge.

Après avoir créé un StyleBook, mettez à jour le pack de configuration existant CP1 pour ajouter des moniteurs. Pour ce faire, procédez comme suit :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez le pack de configuration pour lequel vous souhaitez modifier le StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, sélectionnez CP1 dans la liste.

3. Cliquez sur **Modifier le StyleBook**.
4. Sélectionnez le StyleBook requis dans la liste. Ensuite, cliquez sur **Enregistrer la sélection**.
5. Cliquez sur **Modifier**.

   Dans cet exemple, sélectionnez **example-lb-mon** dans la liste.

   Lorsque vous modifiez le StyleBook d'un pack de configuration, les paramètres du nouveau StyleBook peuvent avoir une structure différente de celle du StyleBook existant. Si la structure des paramètres est similaire à celle du StyleBook précédent, les valeurs des paramètres sont automatiquement conservées dans leurs champs respectifs. Sinon, seuls les paramètres ayant la même structure entre les deux StyleBooks sont transférés. Par exemple, le même nom de paramètre, le même type, le même parent de paramètre, et plus encore.

   Si de nouveaux paramètres obligatoires sont ajoutés dans le nouveau StyleBook, après avoir modifié le StyleBook, vous devez spécifier manuellement les valeurs de ces paramètres.

   Dans cet exemple, les paramètres qui apparaissent sur la page de configuration pour le StyleBook **example-lb** sont les suivants :

   Exemple de pack de configuration d'équilibrage de charge(/en-us/netscaler-application-delivery-management-software/media/nmas-migrate-configpack-3.png)

   Les paramètres qui apparaissent sur la page de configuration pour le nouveau StyleBook **example-lb-mon** sont les suivants :

   Exemple de paramètres après la migration du pack de configuration(/en-us/netscaler-application-delivery-management-software/media/nmas-migrate-configpack-4.png)

   Dans ce cas, les StyleBooks conservent les anciennes valeurs pour la configuration de base de l'équilibreur de charge car le nouveau StyleBook n'a pas modifié les paramètres existants. Et, il ajoute uniquement les nouveaux paramètres. Pour les paramètres de moniteur, spécifiez manuellement les valeurs requises.
6. Dans **Instances cibles**, examinez les instances sélectionnées et mettez à jour la liste si nécessaire.
7. Cliquez sur **Exécution à blanc**.

   La page **Objets** affiche les objets qui sont créés, modifiés ou supprimés des instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Cliquez sur **OK**.

   Dans la page **StyleBook > Configurations**, la colonne **Nom du StyleBook** affiche le nouveau nom du StyleBook pour le pack de configuration sélectionné. Dans ce cas, il affiche **example-lb-mon**.

Modifier le StyleBook qui contient plusieurs packs de configuration

Lorsque vous modifiez un StyleBook existant qui contient plusieurs packs de configuration, procédez comme suit :

1. Importez un nouveau StyleBook dans NetScaler Console.

   Généralement, le nouveau StyleBook a le même nom et le même espace de noms avec une version supérieure à celle du StyleBook existant. Cependant, vous pouvez ignorer cette étape si le nom, l'espace de noms ou la version sont différents.
2. Modifier le StyleBook pour les packs de configuration associés au StyleBook existant.

   Vous ne pouvez sélectionner **Modifier le StyleBook** que lorsque les packs de configuration sélectionnés sont associés au même StyleBook.

   Pour les packs de configuration sélectionnés, NetScaler Console modifie le StyleBook avec succès lorsque les conditions suivantes sont remplies :

   - Tous les paramètres de configuration du StyleBook existant doivent être présents dans le StyleBook sélectionné.
   - Les nouveaux paramètres du StyleBook sélectionné sont facultatifs.

   Pour afficher la progression des packs de configuration sélectionnés, sélectionnez **Configurations en cours/échouées** dans la page **Configurations**.
3. Supprimez l'ancien StyleBook de NetScaler Console une fois que tous les packs de configuration sont liés au nouveau StyleBook.

Exporter ou importer des packs de configuration

Vous pouvez exporter ou importer un pack de configuration comme les StyleBooks. Grâce à cette fonctionnalité, vous pouvez facilement partager la configuration du StyleBook avec une autre NetScaler Console. Lorsque vous exportez un pack de configuration, un bundle `tgz` ou `zip` est téléchargé sur votre ordinateur local. Ce bundle comprend un fichier JSON avec tous les paramètres définis dans un pack de configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exporter la configuration

Procédez comme suit pour exporter un pack de configuration :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez un pack de configuration que vous souhaitez exporter.
3. Dans **Sélectionner une action**, sélectionnez **Exporter la configuration**.

   
4. Dans le volet **Exporter la configuration**, spécifiez les éléments suivants :

   - **Informations sur l'instance ou les instances cibles sur lesquelles la configuration est déployée** : Sélectionnez cette option pour inclure les informations des instances cibles dans le bundle d'exportation.
   - **StyleBook associé à la configuration** : Sélectionnez cette option pour inclure le StyleBook dans le bundle d'exportation.
   - **Phrase secrète pour protéger les données de configuration d'exportation** : Spécifiez une phrase secrète pour chiffrer le bundle d'exportation. Cette phrase secrète sécurise les données sensibles d'un pack de configuration.
   - **Type de fichier compressé** : Sélectionnez le type de fichier **ZIP** ou **TGZ**.

   
5. Cliquez sur **Exporter**.

   Enregistrez le bundle d'exportation sur votre ordinateur local.

Importer la configuration

Vous pouvez importer un pack de configuration de votre ordinateur local vers une autre console NetScaler. Pour importer un pack de configuration, procédez comme suit :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez **Importer la configuration**.
3. Choisissez le bundle de fichiers d'importation depuis votre ordinateur.
4. Utilisez la phrase secrète que vous avez spécifiée lors de l'exportation.
5. Facultatif, dans Options avancées, sélectionnez **Autoriser uniquement la création d'une nouvelle configuration si tous les objets de configuration existent déjà sur NetScaler**.

   Cette option ne modifie pas les objets déjà créés sur l'instance NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considérez que vous avez ajouté la même instance NetScaler dans deux serveurs NetScaler Console. Et vous souhaitez migrer un pack de configuration d'un serveur NetScaler Console vers un autre serveur. Utilisez cette option pour importer un pack de configuration sans modifier ses objets de configuration sur une instance NetScaler.

IMPORTANT

Pour utiliser cette option, assurez-vous que le bundle de configuration spécifié contient les informations des instances cibles. Voir, Exporter la configuration.

Cette option ne migre la configuration que si tous les objets sont présents sur l'instance cible.

6. Cliquez sur **Importer**.

Lorsque vous importez un pack de configuration, NetScaler Console vérifie les éléments suivants :

- **StyleBook associé** : Si le StyleBook associé ne se trouve pas dans NetScaler Console, il importe le StyleBook avec le pack de configuration.
- **Instances cibles** : Vérifie les instances cibles et déploie la configuration sur les instances cibles spécifiées. Si les instances NetScaler mentionnées sont absentes dans NetScaler Console, le pack de configuration est importé sans instances cibles.
- **NetScaler Console source** : Si vous importez un pack de configuration sur le même serveur NetScaler Console, le bundle sélectionné met à jour le pack de configuration existant.

Enregistrer un pack de configuration en tant que brouillon

L'option **Enregistrer en tant que brouillon** dans les packs de configuration vous permet d'enregistrer vos modifications de configuration en tant que brouillons. Cette fonctionnalité enregistre les modifications sans les déployer immédiatement sur une instance NetScaler.

Pour enregistrer un pack de configuration en tant que brouillon :

1. Accédez à **Applications > Configuration > Packs de configuration**.
2. Sur la page **Configurations**, cliquez sur **Ajouter**.
3. Sélectionnez le stylebook souhaité et cliquez sur **Sélectionner**.
4. Sur la page **Créer une configuration**, cliquez sur **Enregistrer comme brouillon**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Une fois le pack de configuration enregistré comme brouillon, vos modifications de configuration ne sont pas déployées directement sur l'instance NetScaler. Au lieu de cela, les packs de configuration sont stockés comme brouillons dans l'onglet **Configurations de brouillon** sous **Configurations en attente**.

Dans l'onglet **Configurations de brouillon**, sélectionnez le pack de configuration pour effectuer les opérations suivantes :

- Modifier la configuration d'un pack de configuration.
- Déployer la configuration sur une instance NetScaler.
- Supprimer le brouillon pour supprimer la configuration sans la déployer.

Vous pouvez également planifier le moment du déploiement de vos brouillons enregistrés.

Pour plus d'informations, consultez Planifier un pack de configuration.

Créer un calendrier pour un pack de configuration

Lorsque vous créez un pack de configuration, celui-ci est automatiquement déployé sur une instance NetScaler par défaut. Grâce à cette fonctionnalité, vous pouvez planifier le moment du déploiement du pack de configuration.

Pour créer un calendrier pour un pack de configuration :

1. Accédez à **Applications > Configuration > Packs de configuration**.
2. Sur la page **Configurations**, cliquez sur **Ajouter**.
3. Sélectionnez le StyleBook et cliquez sur **Sélectionner**.
4. Sur la page **Créer une configuration**, sous **Exécution**, sélectionnez **Plus tard** dans la liste **Mode d'exécution**.
5. Sélectionnez l'heure et la date souhaitées pour la planification, puis cliquez sur **Soumettre**.

Toutes les configurations planifiées sont stockées dans l'onglet **Configurations planifiées** sous **Configurations en attente**. Vous pouvez sélectionner la planification créée pour la modifier, la déployer ou l'annuler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour un pack de configuration déployé

Vous pouvez également créer une planification pour modifier et supprimer un pack de configuration déployé.

PLANIFIER UNE OPÉRATION DE MODIFICATION POUR UN PACK DE CONFIGURATION

Pour créer une planification afin de modifier le pack de configuration déployé :

1. Accédez à **Applications > Configuration > Packs de configuration**.
2. Sur la page **Configurations**, sélectionnez un StyleBook et cliquez sur **Modifier**.
3. Sur la page **Modifier la configuration**, modifiez le pack de configuration.
4. Dans la liste **Mode d'exécution**, sélectionnez **Plus tard**.
5. Sélectionnez l'heure et la date souhaitées pour la planification et cliquez sur **Soumettre**.

PLANIFIER UNE OPÉRATION DE SUPPRESSION POUR UN PACK DE CONFIGURATION

Pour créer une planification pour supprimer le pack de configuration déployé :

1. Accédez à **Applications > Configuration > Packs de configuration**.
2. Sur la page **Configurations**, sélectionnez un StyleBook et cliquez sur **Supprimer**.
3. Dans la liste **Mode d'exécution**, sélectionnez **Plus tard**.
4. Sélectionnez l'heure et la date souhaitées pour la planification et cliquez sur **Soumettre**.

Détacher une instance cible d'un pack de configuration

Pour détacher une instance cible d'un pack de configuration, procédez comme suit :

1. Accédez à **Applications > Configuration > Packs de configuration**.
2. Sélectionnez le pack de configuration avec une instance cible que vous souhaitez supprimer.
3. Dans **Sélectionner une action**, sélectionnez **Détacher les cibles**.
4. Dans le volet **Détacher les cibles**, sélectionnez l'instance cible que vous souhaitez supprimer du pack de configuration.

   

5. Cliquez sur **OK**.

Un message s'affiche, confirmant la création d'un pack de configuration en double avec l'instance cible désormais supprimée.

Créez vos StyleBooks

Le contenu complet du StyleBook **example-lb** est fourni à titre de référence comme suit :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

Le contenu complet du StyleBook **example-lb-mon** est fourni à titre de référence comme suit :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

  -

    namespace: com.citrix.adc.commontypes

    prefix: cmtypes

    version: "1.0"

parameters-default-sources:

  - stlb::lb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: monitors

    label: "List of Monitors"

    description: "List of Monitors to monitor Application Servers"

    type: cmtypes::monitor[]

substitutions:

  mon-name(appname, monname): $appname + "-mon-" + $monname

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

Créer un StyleBook pour télécharger des fichiers vers NetScaler Console

Les StyleBooks de NetScaler Application Delivery Management (NetScaler Console) vous permettent de créer des configurations NetScaler qui peuvent inclure, entre autres, le téléchargement de fichiers de tout type depuis votre système de fichiers local vers l'instance NetScaler, en utilisant l'interface graphique de NetScaler Console ou les API. Ces fichiers peuvent être des exemples de fichiers de certificat ou des fichiers de géolocalisation. Vous pouvez également spécifier le répertoire de téléchargement de ces fichiers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration StyleBook

Voici un exemple de StyleBook qui décrit comment télécharger un fichier de géolocalisation sur l'instance NetScaler. Les fichiers géographiques sont généralement utilisés dans les configurations GSLB pour définir la proximité statique basée sur la géolocalisation :

Créez votre StyleBook -1

```
name: upload-geolocations

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

-

 namespace: netscaler.nitro.config

 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Console

 type: file

 required: true



components:

-

 name: upload-file-comp

 type: ns::systemfile

 properties:

    filename: $parameters.locationfile.filename

    filelocation: "/var/netscaler/inbuilt_db/"

    filecontent: base64.encode($parameters.locationfile.contents)
```

REMARQUE

Le paramètre utilisé dans cet exemple est de type fichier. Vous pouvez importer ce StyleBook dans NetScaler Console et l'utiliser pour télécharger des fichiers de géolocalisation.

Ce StyleBook exige que le fichier soit déjà présent dans NetScaler Console (par exemple, vous l'auriez déjà copié dans NetScaler Console à l'aide d'un utilitaire comme scp). Si vous souhaitez télécharger un fichier vers des NetScalers via NetScaler Console sans le copier d'abord dans le système de fichiers de NetScaler Console, vous pouvez créer un StyleBook qui comporte deux paramètres de type "chaîne", l'un pour spécifier le nom du fichier à utiliser sur le NetScaler et l'autre pour spécifier le contenu du fichier, et utiliser ces deux paramètres dans les composants upload-file-comp. Voici un StyleBook alternatif pour télécharger un fichier de géolocalisation :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Créez votre StyleBook - 2

```
name: upload-geolocations-alt

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "11.1"

  prefix: ns



parameters:

 -

  name: filename

  label: Location Filename

  description: The name of the location file on the NetScaler

  type: string

  required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -

  name: filecontents

  label: Location File Contents

  description: The contents of the location file

  type: string

  required: true



components:

 -

  name: upload-file-comp

  type: ns::systemfile

  properties:

   filename: $parameters.filename

   filelocation: "/var/NetScaler/inbuilt_db/"

   filecontent: base64.encode($parameters.filecontents)
```

Création de configurations pour télécharger des fichiers

La procédure suivante crée une configuration sur une instance NetScaler sélectionnée qui téléchargerait un fichier de géolocalisation en utilisant le premier StyleBook décrit ci-dessus.

Pour créer une configuration pour le téléchargement de fichiers :

1. Dans NetScaler Console, accédez à **Applications** > **Configuration**, puis cliquez sur **Créer nouveau**. La page Choisir StyleBook affiche tous les StyleBooks disponibles dans votre NetScaler Console. Faites défiler vers le bas et sélectionnez le StyleBook que vous avez importé.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les paramètres StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet de saisir les valeurs de tous les paramètres définis dans ce StyleBook.

2. Saisissez le nom de l'équilibreur de charge et l'adresse IP virtuelle dans la section des paramètres de base de l'équilibreur de charge.
3. Dans la section **Fichier d'emplacement**, saisissez le nom ou l'emplacement du fichier.

   REMARQUE

   Assurez-vous que dans NetScaler Console, le fichier se trouve uniquement dans le dossier du locataire actuel. Utilisez n'importe quel protocole de transfert de fichiers pour copier le fichier vers le système de fichiers de NetScaler Console.

4. Il peut vous être demandé de fournir vos informations d'identification d'utilisateur avant d'accéder aux instances cibles.
5. Sélectionnez l'instance NetScaler cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

REMARQUE

Nous vous recommandons de sélectionner **Exécution à blanc** pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la création du pack de configuration est réussie, le fichier est enregistré sur le système de fichiers de l'instance NetScaler à l'emplacement : /var/netscaler/inbuilt_db/

REMARQUE

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

Utilisation de l'API NetScaler Console pour créer un pack de configuration

Vous pouvez également utiliser l'API NetScaler Console pour créer un pack de configuration qui télécharge des fichiers vers l'instance NetScaler sélectionnée. Pour plus d'informations sur l'utilisation des API, consultez Comment utiliser l'API pour créer des configurations afin de télécharger n'importe quel type de fichier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Créer un StyleBook pour télécharger des fichiers de certificat SSL et de clé de certificat vers NetScaler Console

Lors de la création d'une configuration StyleBook qui utilise le protocole SSL, vous devez télécharger les fichiers de certificat SSL et les fichiers de clé de certificat comme requis par les paramètres StyleBook. StyleBook vous permet de télécharger directement les fichiers SSL et les fichiers de clé depuis votre système local en utilisant l'interface graphique de NetScaler Console. Vous pouvez également utiliser les API de NetScaler Console pour télécharger des fichiers de certificat et des fichiers de clé qui sont déjà gérés par NetScaler Console.

Configuration StyleBook

Ce document vous aide à créer votre propre StyleBook - **Serveur virtuel d'équilibrage de charge (SSL)** avec des composants pour télécharger des certificats SSL et des fichiers de clé. Le StyleBook fourni ici à titre d'exemple crée une configuration de serveur virtuel d'équilibrage de charge de base sur l'instance NetScaler sélectionnée. La configuration utilise le protocole SSL. Pour créer une configuration à l'aide de ce StyleBook, vous devez fournir le nom et l'adresse IP du serveur virtuel, sélectionner les paramètres de la méthode d'équilibrage de charge, et télécharger le fichier de certificat et le fichier de clé de certificat pour le serveur virtuel, ou utiliser un fichier de certificat et un fichier de clé de certificat déjà présents dans NetScaler Console. Ceux-ci sont spécifiés dans la section "parameters", comme indiqué ci-dessous :

```
parameters:

 -

  name: name

  type: string

  required: true

 -

  name: ip

  type: ipaddress

  required: true

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: lb-alg

  type: string

  allowed-values:

    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile
```

Deux composants sont ensuite créés dans la section des composants du StyleBook, comme indiqué ci-dessous. Le composant "my-lbvserver-comp" est de type ns::lbvserver, où :

- "ns" est le préfixe qui fait référence à l'espace de noms intégré netscaler.nitro.config et à la version 10.5 que vous aviez spécifiée dans la section import-stylebooks.
- "lbvserver" est un StyleBook intégré dans cet espace de noms. Il correspond à la ressource de serveur virtuel d'équilibrage de charge NetScaler NITRO du même nom.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le deuxième composant "lbvserver-certificate-comp" est de type stlb::vserver-certs-binds. Le préfixe "stlb" fait référence à l'espace de noms "com.citrix.adc.stylebooks" et à la version 1.0 spécifiée dans la section import-stylebooks du StyleBook. Si l'espace de noms "com.citrix.adc.stylebooks" peut être considéré comme un dossier, "vserver-certs-binds" est un autre StyleBook (ou un fichier) dans ce dossier. Les StyleBooks qui se trouvent dans l'espace de noms "com.citrix.adc.stylebooks" sont livrés avec NetScaler Console.

Le StyleBook "vserver-certs-binds" utilisé par les StyleBooks définis par l'utilisateur vous permet de configurer facilement les certificats en téléchargeant les fichiers de certificat et de clé vers l'instance NetScaler cible, et en configurant la liaison des fichiers de certificat et de clé aux serveurs virtuels appropriés. Les propriétés de ce composant sont : le nom du serveur virtuel lb et les noms des certificats SSL que vous fournissez lors de la création du pack de configuration.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
vserver-name: $components.my-lbvserver-comp.properties.name

certificates:

 -

  cert-name: $parameters.name + "-lb-cert"

  cert-file: $parameters.certificate

  ssl-inform: PEM

  key-name: $parameters.name + "-key"

  key-file: $parameters.key
```

Lorsque vous utilisez l'API pour créer une configuration à partir d'un tel StyleBook, utilisez uniquement les noms de fichiers (pas le chemin complet du fichier). Ces fichiers sont censés être déjà disponibles dans les dossiers de fichiers de certificat et de clé sur NetScaler Console. Le fichier de certificat SSL téléchargé est stocké sur NetScaler Console dans le répertoire /var/mps/tenants/.../ns_ssl_certs, et le fichier de clé de certificat SSL est stocké dans le répertoire /var/mps/tenants/.../ns_ssl_keys dans NetScaler Console.

Création de configurations pour télécharger des fichiers SSL

La procédure suivante crée une configuration de serveur virtuel d'équilibrage de charge de base sur une instance NetScaler sélectionnée en utilisant le protocole SSL à partir du StyleBook spécifié ci-dessus. Vous pouvez utiliser cette procédure pour télécharger les fichiers de certificat SSL et les fichiers de clés de certificat dans NetScaler Console.

Pour créer une configuration pour le téléchargement de fichiers

1. Dans NetScaler Console, accédez à **Applications** > **Configuration > StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre NetScaler Console.
2. Faites défiler vers le bas et sélectionnez **Serveur virtuel d'équilibrage de charge (SSL)** ou tapez **Serveur virtuel d'équilibrage de charge (SSL)** dans le champ de recherche et appuyez sur la touche **Entrée**.
3. Cliquez sur le lien **Créer une configuration** dans le panneau StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les paramètres StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet de saisir les valeurs de tous les paramètres définis dans ce StyleBook.

4. Saisissez le nom de l'équilibreur de charge et l'adresse IP virtuelle dans la section des paramètres de base de l'équilibreur de charge.
5. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également sélectionner les fichiers présents sur la console NetScaler elle-même.
6. Sélectionnez l'instance NetScaler cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

REMARQUES :

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter les instances NetScaler récemment découvertes dans NetScaler Console à la liste des instances disponibles dans cette fenêtre.

Dans NetScaler Console, les StyleBooks par défaut suivants, fournis avec NetScaler Console, vous permettent de créer un support SSL en téléchargeant les certificats et clés SSL.

- StyleBook d'équilibrage de charge HTTP/SSL (lb)
- StyleBook d'équilibrage de charge HTTP/SSL (avec moniteurs) (lb-mon)
- Application à commutation de contenu HTTP/SSL avec moniteurs (cs-lb-mon)
- Exemple de StyleBook d'application utilisant les fonctionnalités CS, LB et SSL (sample-cs-app)

Vous pouvez également créer vos propres StyleBooks qui utilisent des certificats SSL de la même manière que celle décrite dans le StyleBook ci-dessus.

Créez votre StyleBook

Le contenu complet du fichier lb-vserver-ssl.yaml est affiché ci-dessous :

```
name: lb-vserver-ssl

description: "This stylebook defines a load balancing virtual server
configuration."

display-name: "Load Balancing Virtual Server (SSL)"

namespace: com.example.ssl.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"

version: "0.1"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"

 -

  namespace: com.citrix.adc.stylebooks

  prefix: stlb

  version: "1.0"



parameters:

 -

  name: name

  type: string

  required: true

 -

  name: ip

  type: ipaddress

  required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -

  name: lb-alg

  type: string

  allowed-values:

    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile



components:

 -

  name: my-lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 type: ns::lbvserver
 properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
-
 name: lbvserver-certificate-comp
 type: stlb::vserver-certs-binds
 description: Binds lbvserver with server certificate
 properties:
  vserver-name: $ components.my-lbvserver-comp.properties.name
  certificates:
   -
    cert-name: $parameters.name + "-lb-cert"
    cert-file: $parameters.certificate
    ssl-inform: PEM
    key-name: $parameters.name + "-key"
    key-file: $parameters.key
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utilisation de l'API NetScaler Console pour créer un pack de configuration

Vous pouvez également utiliser l'API NetScaler Console pour créer un pack de configuration qui télécharge les fichiers de certificat et de clé vers l'instance NetScaler sélectionnée. Pour plus d'informations sur l'utilisation des API, consultez Comment utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificat et de clé.

Affichage des objets définis sur l'instance NetScaler

Une fois le pack de configuration StyleBook créé sur NetScaler Console, cliquez sur **Afficher les objets créés** pour afficher tous les objets NetScaler créés sur l'instance NetScaler cible



Gérer les certificats SSL depuis le magasin de certificats à l'aide de StyleBooks

Le magasin de certificats NetScaler Console vous aide à stocker et à gérer vos certificats SSL en un seul endroit. Ainsi, vous pouvez stocker des certificats SSL dans NetScaler Console et les réutiliser lors de la configuration de NetScaler.

Cet article explique comment créer une définition StyleBook qui vous permet de télécharger et de réutiliser des certificats SSL depuis le magasin de certificats NetScaler Console.

Paramètres

La définition **StyleBook** prend en charge `certkey` comme nouveau type de paramètre intégré. Utilisez ce type de paramètre pour réutiliser les certificats SSL du magasin de certificats NetScaler Console.

```
parameters:

-

    name: certificate

    label: Certificate

    description: "Certificate to be bound to this virtual load balanced
application"

    type: certkey
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    required: true
```

Dans cet exemple, le paramètre de certificat fait référence à un certificat SSL ou à une chaîne de certificats du magasin de certificats NetScaler Console.

Dans la définition **StyleBook**, vous pouvez faire référence aux propriétés suivantes pour un paramètre `certkey` :

- `certkeyname` – Nom de la clé de certificat SSL que vous souhaitez configurer sur une instance.
- `cert_filename` – Nom de fichier d'un certificat SSL.
- `password` – Mot de passe requis pour accéder à un certificat SSL si nécessaire.
- `key_filename` – Nom de fichier d'une clé de certificat SSL.
- `keyfile_contents` – Contenu d'un certificat SSL.
- `subject` – Sujet mentionné dans un certificat SSL.
- `issuer` – Autorité ayant émis le certificat SSL.
- `certchain_certkeyname` – Nom de la chaîne de certificats.

REMARQUE :

Parfois, de nombreuses autorités de certification (CA) hiérarchiques signent les certificats de serveur, ce qui signifie que les certificats forment une chaîne. Utilisez cette propriété lorsque le magasin de certificats contient une chaîne de certificats. Cela vous aide à référencer et à lier les certificats entre eux. Lorsque vous créez un pack de configuration, la chaîne de certificats apparaît sous forme de liste.

Ces propriétés vous aident à créer les composants requis dans la définition du **StyleBook**.

Composants

Lorsqu'un StyleBook possède un paramètre `type: certkey`, vous pouvez fournir un certificat pour ce paramètre à partir du magasin de certificats NetScaler Console. Dans ce flux de travail, en plus de visualiser et de sélectionner des certificats à partir du magasin de certificats NetScaler Console, vous pouvez également effectuer les opérations suivantes :

- Télécharger de nouveaux certificats.
- Mettre à jour les certificats existants. Par exemple, les certificats expirés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Supprimer les certificats.

REMARQUE :

- Vous pouvez également gérer les certificats dans le magasin de certificats NetScaler Console à l'aide du tableau de bord SSL de NetScaler Console.
- Après avoir mis à jour un certificat SSL dans le magasin de certificats NetScaler Console, vous devez mettre à jour les packs de configuration associés au certificat SSL. Pour en savoir plus sur la mise à jour des packs de configuration, consultez Utiliser les API pour mettre à jour un pack de configuration existant ou Créer et modifier un pack de configuration.

Créez votre StyleBook

La définition de StyleBook suivante utilise des certificats SSL du magasin de certificats NetScaler Console. Ce StyleBook inclut des composants qui téléchargent le certificat principal et les fichiers de clé vers l'instance NetScaler. Si ces fichiers sont déjà présents sur l'instance NetScaler, NetScaler Console ignore les étapes de téléchargement et ces composants n'ont aucun effet.

```
name: lb-with-cert-from-certstore

namespace: com.example.stylebooks

version: "1.0"

display-name: Application using a CertStore certificate

description: This StyleBook defines a simple SSL Vserver.

schema-version: "1.0"



import-stylebooks:

 -

    namespace: netscaler.nitro.config

    version: "13.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    prefix: ns


parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: certificate
  label: Application Certificate
  description: Certificate chain and key to be bound to this application
  type: certkey
  required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
 -
    name: pem-cert-files-comp
    type: ns::systemfile
    description: This component uploads the PEM certificate file onto the
NetScaler
    condition: $parameters.certificate
    properties:
      filename: $parameters.certificate.cert_filename
      filelocation: /nsconfig/ssl
      filecontent: base64($parameters.certificate.certfile_contents)
      fileencoding: BASE64
 -
    name: pem-KEY-files-comp
    type: ns::systemfile
    description: This component uploads the PEM key file onto the
NetScaler.
    condition: $parameters.certificate
    properties:
      filename: $parameters.certificate.key_filename
      filelocation: /nsconfig/ssl
      filecontent: base64($parameters.certificate.keyfile_contents)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      fileencoding: BASE64

 -

    name: cert-files-comp

    type: ns::sslcertkey

    description: This component creates the certkey on the NetScaler using
the uploaded files.

    condition: $parameters.certificate

    properties:

      certkey:  $parameters.certificate.certkeyname

      cert: $parameters.certificate.cert_filename

      key: $parameters.certificate.key_filename

 -

  name: lbvserver-comp

  type: ns::lbvserver

  description: This component creates the lbvserver of the application.

  properties:

   name: $parameters.name + "-lbvserver"

   servicetype: SSL

   ipv46: $parameters.ip

   port: 443

   lbmethod: ROUNDROBIN

  components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
  name: sslvserver-comp
  type: ns::sslvserver
  description: This component configures SSL settings on the vserver
  properties:
    vservername: $parent.properties.name
    ssl3?: ENABLED
    tls1?: ENABLED
    tls11?: ENABLED
-
 name: cert-bindings-adv-comp
 type: ns::sslvserver_sslcertkey_binding
 description: This component binds the certkey to the vserver
 condition: $parameters.certificate
 properties:
   vservername: $parent.properties.name
   certkeyname: $parameters.certificate.certkeyname
```

Activer l'analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook

Vous pouvez utiliser le constructeur d'opérations pour configurer l'analyse NetScaler Console afin de collecter des enregistrements appflow sur tout ou partie des transactions de trafic gérées par tout composant de serveur virtuel faisant partie d'un StyleBook. Vous pouvez également utiliser ce

© 1997–2026 Citrix Systems, Inc. All rights reserved.

constructeur pour configurer des alarmes afin d'obtenir des informations sur le trafic géré par le serveur virtuel.

L'exemple suivant montre une section d'opérations d'un StyleBook :

```
operations:

  analytics:

   -

    name: lbvserver-ops

    properties:

    target: $components.basic-lb-comp.outputs.lbvserver

    filter: HTTP.REQ.URL.CONTAINS("catalog")

   -

    alarms:

     -

      name: lbvserver-alarm

      properties:

      target: $outputs.lbvserver

      email-profile: $parameters.emailprofile

      sms-profile: "NetScalerSMS"



    rules:

     -

      metric: "total_requests"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      operator: "greaterthan"

      value: 25

      period-unit: $parameters.period

    -

      metric: "total_bytes"

      operator: "lessthan"

      value: 60

      period-unit: "day"
```

Les attributs de la section d'analyse sont utilisés pour indiquer à la fonction d'analyse de NetScaler Console de collecter des enregistrements appflow sur un composant de serveur virtuel identifié par la propriété cible. Vous pouvez également spécifier facultativement une propriété de filtre qui accepte une expression de stratégie NetScaler pour filtrer les requêtes pour lesquelles les enregistrements appflow sont collectés sur le serveur virtuel.

Lorsqu'un pack de configuration est créé à partir de ce StyleBook, la fonction d'analyse de NetScaler Console est configurée pour collecter des enregistrements appflow sur les serveurs virtuels qui ont été spécifiés lors de leur création dans le processus de création d'un pack de configuration.

Les attributs de la section des alarmes sont utilisés pour définir des seuils afin de générer des alarmes et d'envoyer des notifications sur le serveur virtuel identifié par la propriété cible. Dans l'exemple ci-dessus, les propriétés email-profile et sms-profile sont utilisées pour spécifier où les notifications doivent être envoyées. La section des règles définit les seuils. Par exemple, si le nombre total de requêtes traitées par le serveur virtuel est supérieur à 25 et pendant une période définie par l'utilisateur, une alarme est déclenchée et une notification est envoyée. Le "period-unit" spécifie la fréquence à laquelle une alarme est déclenchée. Il peut prendre la valeur jour, heure ou semaine.

Vous pouvez utiliser les opérateurs suivants lors de la comparaison de la valeur de la métrique à la valeur de seuil :

- "greaterthan" pour ">"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- "lessthan" pour "<"
- "greaterthanequal" pour ">="
- "lessthanequal" pour "<="

Notez que les StyleBooks utilisent les noms d'API pour les métriques et non les noms affichés sur l'interface graphique d'analyse de NetScaler Console.

Pour savoir comment afficher et analyser les données collectées sur les serveurs virtuels créés dans le cadre d'un pack de configuration, consultez la documentation d'analyse de NetScaler Console.

Rôles d'instance

Dans NetScaler Console, il peut y avoir un scénario où vous devez configurer plusieurs instances NetScaler pour une seule application, mais aussi où chaque instance NetScaler nécessite une configuration différente à déployer. Un exemple d'un tel cas est le StyleBook par défaut de Microsoft Skype for Business.

Les StyleBooks prennent actuellement en charge la possibilité de créer un pack de configuration et d'appliquer la même configuration sur plusieurs instances NetScaler. Un tel scénario, où la configuration est identique sur toutes les instances NetScaler, peut être qualifié de configuration symétrique.

Désormais, avec la fonctionnalité « rôles d'instance » des StyleBooks, vous pouvez créer une configuration asymétrique, c'est-à-dire un pack de configuration qui peut être appliqué sur plusieurs instances NetScaler, mais avec des configurations différentes sur différentes instances NetScaler.

Lorsqu'un StyleBook avec la fonctionnalité de rôles d'instance est utilisé pour créer un pack de configuration, chaque instance NetScaler dans un pack de configuration peut se voir attribuer un rôle différent. Ce rôle détermine les objets de configuration du pack de configuration que l'instance NetScaler recevra.

Points à noter :

- L'ensemble des rôles d'instance dans un StyleBook est défini lors de la création du StyleBook.
- Les rôles sont attribués à une instance NetScaler spécifique lors de la création ou de la mise à jour du pack de configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Section « target-roles »

Une nouvelle section dans un StyleBook, appelée « target-roles », est introduite, où tous les rôles pris en charge par le StyleBook sont déclarés.

Cette section est généralement placée après la section « import-StyleBooks » d'un StyleBook, et avant la section des paramètres.

Dans l'exemple de StyleBook suivant, deux rôles sont définis dans la section « target-roles » : A et B.

```
target-roles:



  -

   name: A

   name: B

     min-targets: 2

     max-targets: 5
```

Vous pouvez voir que le rôle B définit également deux sous-propriétés facultatives : min-targets et max-targets.

Bien que ces deux sous-propriétés soient facultatives, min-targets spécifient le nombre minimum obligatoire d'instances NetScaler qui doivent se voir attribuer ce rôle lors de la création d'un pack de configuration à partir de ce StyleBook, et max-targets spécifient le nombre maximum d'instances NetScaler qui peuvent se voir attribuer ce rôle lors de la création d'un pack de configuration à partir de ce StyleBook.

Si ces sous-propriétés ne sont pas spécifiées, alors il n'y a pas de limite sur le nombre d'instances NetScaler pouvant être configurées pour ce rôle. Si min-targets = 0, la configuration associée à ce rôle est facultative et si min-targets = 1, alors cette configuration est obligatoire et au moins une instance NetScaler doit être configurée pour ce rôle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rôle « default »

En plus des rôles explicitement définis, il existe un rôle implicite que tous les StyleBooks possèdent, et ce rôle est appelé rôle par défaut. Ce rôle peut être utilisé comme n'importe quel autre rôle dans un StyleBook. Lors de la création d'un pack de configuration, si une instance NetScaler n'est pas associée à un rôle spécifique, l'instance est implicitement associée au rôle « default ». L'instance recevra alors tous les objets de configuration générés par les composants qui ont le rôle « default ».

Composants avec des rôles

Une fois les rôles qu'un StyleBook peut prendre en charge (y compris le rôle « default ») définis, les rôles peuvent être utilisés dans la section des composants d'un StyleBook. Si vous souhaitez qu'un composant soit déployé uniquement sur les instances NetScaler qui jouent un certain rôle, vous pouvez spécifier l'attribut de rôles dans le cadre du composant, comme illustré dans l'exemple de composant suivant :

```
-

  name: C1

  type: ns::lbvserver

  roles:

    - A

  properties:

    name: lb1

    servicetype: HTTP

    ipv46: 1.1.1.1

    port: 80
```

Dans l'exemple ci-dessus, le composant génère un « lbvserver » qui sera déployé sur les instances jouant le rôle A. Notez que l'attribut de rôles d'un composant est une liste, et qu'un composant peut se voir attribuer plusieurs rôles. Ces rôles auraient été déclarés dans la section « target-roles » du StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque : Si un composant dans un StyleBook ne spécifie pas d'attribut de rôle, les objets de configuration générés par le composant sont créés sur toutes les instances NetScaler, quel que soit leur rôle. Vous pouvez utiliser cette fonctionnalité efficacement pour créer des objets de configuration qui peuvent être appliqués à toutes les instances d'un pack de configuration.

Supposons qu'il existe un StyleBook avec deux rôles définis - A et B, et qui contient quatre composants.

- Le composant C1 a les rôles A et B
- Le composant C2 a le rôle B
- Le composant C3 n'a aucun rôle défini
- Le composant C4 a le rôle « default »

La section des composants de ce StyleBook est reproduite ci-dessous :

```
components:

  -

    name: C1

    type: ns::lbvserver

    roles:

      - A

      - B

    properties:

      name: lb1

      servicetype: HTTP

      ipv46: 1.1.1.1

      port: 80

  -

    name: C2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      name: lb4

      servicetype: HTTP

      ipv46: 14.14.14.14

      port: 80
```

Notez que le composant C3 n'a pas de rôle défini, ce qui signifie que le composant est déployé sur toutes les instances, quel que soit leur rôle. D'autre part, le composant C4 a le rôle « default », ce qui signifie qu'il est appliqué à toute instance à laquelle aucun rôle explicite n'est attribué.

Maintenant, imaginez que vous souhaitez créer un pack de configuration à l'aide de ce StyleBook, et le déployer sur cinq instances NetScaler. À ce stade, vous pouvez attribuer les rôles aux instances de la manière suivante :

- Le rôle A est attribué aux instances T1, T2, T3 et T4
- Le rôle B est attribué aux instances T2, T3 et T4
- Aucun rôle n'est attribué à l'instance T5

L'image suivante récapitule les attributions de rôles et montre la configuration résultante que chaque instance NetScaler recevra :



Notez que le composant C3 est déployé sur toutes les instances, quel que soit le rôle, car ce composant n'avait pas d'attribut de rôles.

Vous pouvez également utiliser la fonctionnalité « Dry Run » lors de la création d'un pack de configuration pour afficher et vérifier l'attribution correcte des rôles et les objets de configuration qui seront créés sur chaque instance NetScaler.

Créez votre StyleBook

Le contenu complet du StyleBook « demo-target-roles » est fourni ci-dessous :

```
---

name: demo-target-roles

namespace: com.example.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
```

L'image suivante montre les objets créés pour un exemple de pack de configuration :



Utilisation des API

Lorsque vous utilisez l'API REST, vous pouvez spécifier des rôles pour chaque instance NetScaler lors de la création ou de la mise à jour du pack de configuration comme suit. Dans le bloc « targets », spécifiez l'UUID de l'instance NetScaler spécifique sur laquelle vous souhaitez déployer les composants individuels.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"targets": [

            {

             "id": "<ADC-UUID>",

             "roles": ["A"]

            },

           ]
```

Un exemple complet d'API REST est fourni pour votre référence.

POST /`<Console-IP`>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]

        },

        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",

          "roles": ["A", "B"]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        {
          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
        },
        {
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```

Créer un StyleBook pour effectuer des opérations non-CRUD

Les StyleBooks gèrent les configurations NetScaler en calculant les objets de configuration nécessaires sur les instances NetScaler. Ces objets sont ajoutés, mis à jour ou supprimés de l'instance chaque fois que vous créez ou mettez à jour un ConfigPack. C'est à ce moment-là que vous spécifiez l'« état souhaité ».

Cependant, certains objets de configuration NetScaler prennent en charge quelques opérations autres que la création, la mise à jour ou la suppression (opérations CRUD). Par exemple, un objet d'équilibrage de charge (lbvserver) ou un objet de fonctionnalité NetScaler (nsfeature) peut

© 1997–2026 Citrix Systems, Inc. All rights reserved.

prendre en charge l'opération « activer » ou « désactiver ». De même, les certkeys NetScaler prennent en charge l'opération « lier » et « délier » pour lier ou délier un certificat à un autre certificat. Ces opérations sur les objets NetScaler sont appelées opérations non-CRUD. Cette section décrit comment effectuer des opérations non-CRUD sur les objets de configuration qui les prennent en charge à l'aide de StyleBooks.

REMARQUE

La liaison entre les objets de configuration (par exemple, lier une certkey à un lbvserver) n'est pas considérée comme une opération non-CRUD. En effet, les liaisons Nitro sont représentées comme des objets de configuration à part entière. Ces objets sont créés et supprimés comme tout autre objet de configuration NetScaler.

Prise en charge des opérations non-CRUD

Une nouvelle construction appelée « meta-properties » est ajoutée dans le composant au même niveau que la construction « properties ». Le seul attribut pris en charge dans cette construction est actuellement appelé « action ». Cet attribut peut prendre des valeurs telles que « enable » ou « disable » qui sont prises en charge par cet objet de configuration.

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  meta-properties

   action: enable

  properties:

    name: $parameters.name

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    lbmethod: $parameters.lb-alg
```

Dans l'exemple ci-dessus, le composant « my-lbvserver-comp » est de type « ns::lbvserver ». Le « ns » est le préfixe qui fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5 que vous aviez spécifiés dans la section import-stylebooks. Le « lbvserver » est une ressource NITRO dans cet espace de noms. En tant qu'action implicite, le lbvserver est d'abord créé par le StyleBook ; puis l'opération « enable » est effectuée sur celui-ci.

L'action spécifiée dans les méta-propriétés est effectuée sur l'objet de configuration uniquement lors de la création du ConfigPack. Les mises à jour du ConfigPack n'effectuent pas d'actions non-CRUD.

REMARQUE

La valeur de l'attribut d'action ne peut pas être une expression StyleBook évaluée dynamiquement.

Migrer les packs de configuration d'un StyleBook vers un autre StyleBook

Dans NetScaler Console, les packs de configuration sont toujours liés au StyleBook à partir duquel ils sont créés. Toute mise à jour du pack de configuration ne peut être effectuée qu'à travers le StyleBook auquel le pack de configuration est lié. NetScaler Console vous permet désormais de migrer un pack de configuration existant vers un nouveau StyleBook. Le nouveau StyleBook peut être une version plus originale du StyleBook actuel auquel le pack de configuration est lié. Ou, vous pouvez également migrer le pack de configuration vers un StyleBook entièrement différent.

Par exemple, vous avez créé un StyleBook appelé **example-lb**. Ce StyleBook est utilisé pour déployer une configuration de base d'équilibreur de charge sur une instance NetScaler. Vous avez créé un pack de configuration CP1 à partir de ce StyleBook sur une instance NetScaler. Plus tard, vous avez réalisé que votre StyleBook n'incluait pas de configuration de surveillance. Vous avez donc créé un StyleBook appelé **example-lb-mon**. Ce StyleBook a la même configuration d'équilibreur de charge que le StyleBook example-lb, mais ajoute la possibilité de configurer des moniteurs.

Vous souhaitez maintenant mettre à jour votre configuration existante, créée dans le pack de configuration CP1, pour ajouter des moniteurs. Auparavant, vous deviez supprimer le pack de configuration CP1 et créer un pack de configuration CP2 à partir du nouveau StyleBook pour

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ajouter des moniteurs à votre configuration. La suppression de CP1 entraîne la suppression de toute la configuration créée dans le pack de configuration CP1 sur une ou plusieurs instances NetScaler. Auparavant, vous deviez recréer un nouveau pack de configuration via le nouveau StyleBook en saisissant les valeurs de tous les paramètres.

Au lieu de cela, vous pouvez maintenant migrer le pack de configuration existant CP1 vers le nouveau StyleBook example-lb-mon. Votre nouveau StyleBook peut configurer les détails des moniteurs. Seuls les objets de configuration liés aux moniteurs sont ajoutés aux instances NetScaler où le pack de configuration a été déployé. Vous devez maintenant fournir uniquement les détails du moniteur. La configuration existante déployée sur les instances NetScaler qui n'a pas été modifiée reste inchangée.

Migrer les packs de configuration

Pour migrer un pack de configuration créé à l'aide du StyleBook example-lb vers le StyleBook example-lb-mon

1. Dans NetScaler Console, accédez à **Applications** \> **Configurations**. La page **Configurations** affiche tous les packs de configuration présents dans le système.
2. Faites défiler vers le bas pour trouver le pack de configuration **example-lb** que vous auriez créé précédemment, et cliquez sur **Migrer le pack de configuration**.
3. La page **Choisir le StyleBook cible pour la migration** s'ouvre et répertorie tous les StyleBooks disponibles dans NetScaler Console. Faites défiler vers le bas pour trouver le StyleBook **example-lb-mon** et cliquez sur **Sélectionner le StyleBook**. Vous pouvez également rechercher le StyleBook en tapant example-lb-mon.

   Si vous migrez d'un StyleBook à un autre, tous les paramètres des deux StyleBooks peuvent ne pas avoir la même structure. Si la structure des paramètres est similaire, les valeurs précédentes sont automatiquement conservées dans les champs de paramètres. Certains des paramètres du nouveau StyleBook peuvent être nouveaux, ou leur structure peut avoir changé. Dans un tel cas, vous devez saisir manuellement les valeurs des paramètres du StyleBook. Par exemple, l'image suivante montre les paramètres du StyleBook example-lb.

   

   L'image suivante montre les paramètres après la migration du pack de configuration vers le StyleBook example-lb-mon.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans ce cas, vous pouvez voir que les StyleBooks conservent les anciennes valeurs pour la configuration de base de l'équilibreur de charge. Mais vous devez saisir manuellement les valeurs des paramètres du moniteur.

4. Saisissez les valeurs des nouveaux paramètres utilisés pour créer des moniteurs sur l'instance.
5. Sous **Instances cibles**, cliquez et sélectionnez l'adresse IP de l'instance NetScaler sur laquelle vous souhaitez exécuter la configuration. Notez que vous pouvez déployer la configuration sur plusieurs NetScaler, en spécifiant autant d'instances cibles que nécessaire.
6. Cliquez sur **Exécution à blanc**. La page **Objets** affiche les objets qui seraient nouvellement créés, modifiés ou supprimés de l'instance (ou des instances) NetScaler.
7. Cliquez sur **Créer** pour créer ou mettre à jour la configuration des instances sélectionnées. Le pack de configuration est créé si les instances cibles sont nouvelles. Sinon, les configurations existantes déployées sur les instances sont mises à jour.

REMARQUE :

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances NetScaler récemment découvertes. Ainsi, ces instances sont instantanément disponibles dans la liste des instances de cette fenêtre. L'icône d'actualisation est actuellement disponible uniquement sur NetScaler Console.

Vous pouvez également migrer un pack de configuration d'une version d'un StyleBook vers la version suivante. Ici aussi, vous devrez peut-être saisir les valeurs de tous les nouveaux paramètres requis présents dans la nouvelle version. Vous pouvez également migrer le pack de configuration vers une version antérieure du StyleBook. Dans ce cas, les paramètres supplémentaires qui ne sont pas présents dans l'ancien StyleBook sont supprimés. La page **Objets** affiche tous les objets qui sont supprimés de la configuration.

Après une migration réussie, le ConfigPack est lié au nouveau StyleBook.

Vous pouvez constater que le nom du pack de configuration et l'ID du pack de configuration sont les mêmes qu'auparavant. Mais NetScaler Console met à jour le nom du StyleBook de example-lb à example-lb-mon.

Créez vos StyleBooks

Le contenu complet du StyleBook **example-lb** est fourni ci-dessous pour votre référence :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

Le contenu complet du StyleBook **example-lb-mon** est fourni ci-dessous pour votre référence :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

  -

    namespace: com.citrix.adc.commontypes

    prefix: cmtypes

    version: "1.0"

parameters-default-sources:

  - stlb::lb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: monitors

    label: "List of Monitors"

    description: "List of Monitors to monitor Application Servers"

    type: cmtypes::monitor[]

substitutions:

  mon-name(appname, monname): $appname + "-mon-" + $monname

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

Gérer les sources de données

La définition d'une source de données dans NetScaler Console vous aide à utiliser les données de sources externes comme entrée lors de la création ou de la mise à jour des configurations StyleBook. Sinon, vous devez fournir explicitement chaque entrée requise par le StyleBook. Dans NetScaler Console, vous pouvez utiliser n'importe quelle instance NetScaler gérée comme source de données pour l'entrée d'une configuration StyleBook. Vous pouvez également définir des sources de données personnalisées qui peuvent servir d'entrée lors de la création ou de la mise à jour des configurations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collections : Tout comme une base de données peut avoir plusieurs tables, une source de données peut contenir plusieurs collections. Chaque collection a un nom et contient une liste de tuples similaires, où chaque tuple est un ensemble de paires clé-valeur. Par exemple, une collection peut être composée de tuples où chaque tuple a (`<name>: <value>, <virtualip>:<value>`).

Type de source de données : Un type de source de données distingue le type de source à partir de laquelle les données sont récupérées. NetScaler Console prend en charge deux types de sources de données.

- **managed-adc** - Il s'agit d'une source de données intégrée. Et, elle est utilisée pour récupérer des données de tout NetScaler existant géré par NetScaler Console. Pour plus d'informations, consultez Utiliser une instance NetScaler comme source de données.

  Vous pouvez également utiliser l'instance NetScaler cible comme source de données. Pour plus d'informations, consultez Utiliser les instances NetScaler cibles comme sources de données.
- **Type de source de données personnalisée** - Vous pouvez définir des types de sources de données personnalisées où les données sont renseignées localement sur NetScaler® Console.

  Considérez un type de source de données `Environment`. Ce type de source de données a deux sources de données `Production` et `Staging`. Lors de la création d'une configuration StyleBook, l'utilisateur StyleBook peut sélectionner n'importe quelle source de données de type `Environment`. Selon la sélection, les valeurs de données de `Production` ou `Staging` sont utilisées comme entrée pour le StyleBook.

  Pour plus d'informations, consultez Utiliser des sources de données personnalisées

Schéma de collection : Il décrit le type de données pouvant être stockées dans un tuple de collection. Le schéma de collection décrit le nom de chaque clé dans le tuple et son type attendu. Dans une analogie avec une base de données, un schéma de collection est similaire à un schéma de base de données pour une table où chaque colonne a un nom bien défini et un type de support.

Le diagramme suivant est une représentation générale des différents composants des sources de données et de leurs relations :



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser une instance NetScaler comme source de données

Vous pouvez utiliser les instances NetScaler gérées comme sources de données. Le `managed-adc` est un type de source de données intégré qui peut être facilement utilisé comme source de données dans NetScaler Console. Chaque instance NetScaler gérée dans NetScaler Console est une source de données par défaut. Vous pouvez commencer à utiliser ces sources de données dans vos StyleBooks si vous avez besoin de données d'un NetScaler existant géré par NetScaler Console lors de la création de packs de configuration.

Dans la définition du StyleBook, spécifiez le paramètre de type intégré `datum`. Vous pouvez utiliser les types de sources de données dans votre StyleBook. Les utilisateurs de StyleBook peuvent sélectionner une source de données qui peut être utilisée pour récupérer des données de cette source.

Utilisation de la source de données intégrée sans collection

```
parameters:

  - name: selected-adc

    label: Select an existing NetScaler

    type: datum

    required: true

    data-source:

      type: managed-adc
```

Dans l'exemple, le paramètre `datum` est utilisé pour sélectionner n'importe quelle instance NetScaler gérée par NetScaler Console. La source de données intégrée `managed-adc` vous permet de récupérer des données de n'importe quelle instance NetScaler gérée par NetScaler Console.

Dans votre StyleBook, vous pouvez accéder à n'importe quelle configuration de l'instance NetScaler sélectionnée. Et vous pouvez utiliser cette configuration lors de la création ou de la mise à jour de configurations sur la même instance NetScaler ou sur une instance NetScaler différente ; cela dépend de l'instance NetScaler cible sélectionnée.

Accéder à la collection à partir d'une source de données :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans l'instance NetScaler sélectionnée, pour accéder à une collection, utilisez l'expression suivante :

```
$parameters.selected-adc.collections.<collection-name>
```

Exemple :

```
$parameters.selected-adc.collections.lbvserver
```

Cette expression renvoie la liste des entités `lbvserver` sur l'instance NetScaler sélectionnée. Par exemple, vous pouvez parcourir cette liste pour sélectionner un `lbvserver` spécifique qui répond à une certaine condition.

Exemple de StyleBook sans collection

```
name: add-vservers-from-managed-adc-instances

namespace: com.citrix.adc.stylebooks

version: "1.0"

schema-version: "1.0"



import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

    -

      name: selected-adc
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      label: Select a NetScaler instance
      type: datum
      required: true
      data-source:
        type: "managed-adc"


components:
  -
    name: sslvserver-comp
    type: ns::sslvserver
    repeat: $parameters.selected-adc.collections.lbvserver
    repeat-item: lbvs
    repeat-condition: $lbvs.attributes.servicetype == "SSL"
    properties:
      name: $lbvs.attributes.name
      ssl2: DISABLED
      ssl3: DISABLED
      tls1: DISABLED
      tls11: ENABLED
      tls12: ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'interface graphique du pack de configuration affiche les instances NetScaler gérées par NetScaler Console et les utilisateurs de StyleBook peuvent sélectionner n'importe quel NetScaler lors de la création ou de la mise à jour du pack de configuration.

Ce StyleBook utilise le NetScaler sélectionné et itère sur toutes les entités `lbvserver`. Il sélectionne les serveurs virtuels SSL et définit les versions de protocole SSL autorisées sur chaque serveur virtuel.

L'expression suivante vous permet de parcourir la liste des entités `lbvserver` dans l'instance NetScaler.

```
repeat: $parameters.selected-adc.collections.lbvserver
```

- `collections` : Fait référence à tous les types d'entités sur l'instance NetScaler. Par exemple `csvserver`, `lbmonitor`, `servicegroup`, etc.
- `lbvserver` : Fait référence à la liste des entités de serveur virtuel d'équilibrage de charge dans l'instance NetScaler.

Utilisation de la source de données intégrée avec collection

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

Dans cet exemple, le paramètre `datum` est utilisé pour permettre à un utilisateur de sélectionner à la fois l'instance NetScaler et un `lbvserver` spécifique à partir du type de source de données `managed-adc`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque vous définissez un type de collection dans la section `parameters`, les utilisateurs de StyleBook peuvent sélectionner l'instance NetScaler et une entité spécifique à partir d'une collection sur cette instance.

Accéder à un attribut de l'élément sélectionné :

Lorsque l'utilisateur StyleBook sélectionne un serveur virtuel, l'expression suivante dans votre StyleBook peut accéder à n'importe quel attribut de l'élément sélectionné.

```
$parameters.selected-lbvserver.attributes.<attribute-name>
```

Dans cet exemple, le `datum` sélectionné est `lbvserver`. Ainsi, vous pouvez accéder à n'importe quel attribut de l'entité NetScaler `lbvserver` tel que `name`, `servicetype`, `ipv46`, et ainsi de suite.

Exemple :

```
$parameters.selected-lbvserver.attributes.ipv46
```

Cette expression récupère l'adresse IP du serveur virtuel d'équilibrage de charge sélectionné. Pour plus d'informations sur les entités NetScaler (collections) et leurs attributs, consultez la référence de l'API NetScaler NITRO.

Sélectionner plusieurs éléments d'une collection :

La section des paramètres suivante permet aux utilisateurs de StyleBook de sélectionner plusieurs éléments d'une collection.

```
parameters:

  - name: selected-lbvservers

    label: Select existing lbvservers

    type: datum[]

    required: true

    data-source:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: managed-adc

      collection: lbvserver
```

Dans cet exemple, le paramètre datum est utilisé pour définir le tableau de sources de données. L'utilisateur peut sélectionner un ou plusieurs lbvservers à partir d'une seule instance NetScaler® ou de plusieurs instances NetScaler.

L'extrait de code ci-dessous décrit la manière d'accéder aux éléments sélectionnés et à leurs attributs.

```
components:

  - name: sslvserver-comp

    type: ns::sslvserver

    repeat:

      repeat-list: $parameters.selected-lbvservers

      repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.name

      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

Accéder à une collection par la référence de l'élément sélectionné :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

En plus de permettre à un utilisateur de StyleBook de sélectionner une entité spécifique sur une instance NetScaler gérée, vous pouvez également accéder à n'importe quelle entité provenant de collections identiques ou différentes sur l'instance NetScaler sélectionnée. Pour accéder à une autre collection sur cette instance NetScaler, utilisez l'expression suivante dans la section `components` :

```
$parameters.selected-lbvserver.datasource.collections.<collection-name>
```

Exemple :

```
$parameters.selected-lbvserver.datasource.collections.csvserver
```

Cette expression renvoie la liste des serveurs virtuels de commutation de contenu de l'instance NetScaler sélectionnée.

Et l'expression suivante renvoie une liste de toutes les liaisons entre `lbvservers` et `servicegroups` :

```
$parameters.selected-
lbvserver.datasource.collections.lbvserver_servicegroup_binding
```

Exemple de StyleBook avec une collection

Voici un exemple de StyleBook pour montrer comment utiliser l'instance NetScaler gérée comme source de données :

```
name: bind-lb-to-servicegroup-using-ADC-as-datasource

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration where we allow the user to select an existing lbvserver on
the NetScaler using datum type parameter. Then a servicegroup for the
selected lb is created if it does not exist on the NetScaler. Finally, the
selected lbvserver is bound to the service "
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

  -

    name: selected-vserver

    label: "Select an Existing VServer"

    description: "Load Balancing Application Vservers to be bound to
service on the ADC"

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver



components:

  -

    name: servicegroup-discovery-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: object

    repeat: $parameters.selected-
vserver.datasource.collections.servicegroup

    repeat-item: svcgrp

    repeat-condition: $svcgrp.attributes.servicegroupname ==
 $parameters.selected-vserver.attributes.name + "-svcgrp"

    properties:

      servicegroupname: $svcgrp.attributes.servicegroupname

  -

    name: servicegroup-creation-if-not-exists-comp

    type: ns::servicegroup

    condition: not exists($components.servicegroup-discovery-comp)

    properties:

      servicegroupname: $parameters.selected-vserver.attributes.name + "-
svcgrp"

      servicetype: $parameters.selected-vserver.attributes.servicetype

    components:

      -

        name: lbvserver-servicegroup-binding

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parameters.selected-vserver.attributes.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        servicegroupname: $parent.properties.servicegroupname
```

Dans ce StyleBook, la section `components` vérifie le nom du groupe de services qui correspond au nom du serveur virtuel d'équilibrage de charge sélectionné, concaténé avec `svcgrp`.

Si le nom du serveur virtuel d'équilibrage de charge sélectionné est `lbv1`, ce StyleBook recherche le groupe de services portant le nom `lbv1-svcgrp`. S'il n'est pas trouvé, il crée un groupe de services `lbv1-svcgrp` et le lie au serveur virtuel `lbv1`.

L'expression suivante récupère la liste des groupes de services dans l'instance NetScaler.

```
repeat: $parameters.selected-vserver.datasource.collections.servicegroup
```

Dans cette expression :

- `datasource` : Fait référence à l'instance NetScaler sélectionnée gérée par NetScaler Console.
- `collections` : Fait référence à toutes les entités de l'instance NetScaler.
- `servicegroup` : Fait référence aux groupes de services dans l'instance NetScaler.

Filtrage des données de collection :

La section des paramètres suivante explique comment spécifier des filtres sur une collection de source de données intégrée dans la définition StyleBook. Elle permet aux utilisateurs de StyleBook de sélectionner un élément spécifique parmi une collection filtrée.

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
collection: lbvserver

collection-filters:

  protocol: SSL
```

Dans cet exemple, le paramètre datum est utilisé pour permettre à un utilisateur de sélectionner à la fois l'instance NetScaler et un lbvserver spécifique ayant le protocole SSL à partir du type de source de données managed-adc.

Une fois que l'utilisateur StyleBook a sélectionné un serveur virtuel, tout attribut de l'élément sélectionné peut être accédé de la même manière que celle expliquée dans la section précédente.

Utiliser les instances NetScaler cibles comme sources de données

Vous pouvez également utiliser le NetScaler cible de votre configuration comme entrée de source de données pour votre configuration. Dans ce scénario, vous pourriez vouloir vous référer à la configuration existante sur le NetScaler cible pour créer de nouvelles configurations sur ce NetScaler.

Pour utiliser les instances cibles comme sources de données, vous n'avez pas besoin d'utiliser le paramètre de type intégré `datum`, car aucune instance NetScaler n'a besoin d'être sélectionnée par l'utilisateur StyleBook. Vous pouvez directement écrire des expressions dans la section `components` de votre StyleBook qui récupèrent des données de l'instance NetScaler cible.

Utilisez l'expression suivante pour récupérer les éléments suivants des instances NetScaler cibles :

- Collections :

  ```
  $current-target-as-datasource.collections.<collection-name>
  ```

  Exemple :

  ```
  $current-target-as-datasource.collections.lbvserver
  ```

- Attributs :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$current-target-as-datasource.collections.attributes.<attribute>
```

Exemple de StyleBook pour utiliser l'instance NetScaler cible comme source de données

Voici un exemple de StyleBook pour démontrer comment utiliser l'instance NetScaler cible comme source de données :

```
---

name: lb-add-service-with-target-adc

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration."

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



components:

  -

    name: servicegroup-comp

    type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
properties:
  servicegroupname: "lb-demo-svcgrp"
  servicetype: "HTTP"


components:
  -
    name: lbvserver-svg-binding
    type: ns::lbvserver_servicegroup_binding
    repeat: $current-target-as-datasource.collections.lbvserver
    repeat-item: lbvsrvr
    repeat-condition: $lbvsrvr.attributes.name == "lb-demo-lb"
    properties:
      name: $lbvsrvr.attributes.name
      servicegroupname: $parent.properties.servicegroupname
```

Dans cet exemple, le pack de configuration vérifie les serveurs virtuels d'équilibrage de charge dans les instances NetScaler cibles. Et, si l'adresse IP du serveur virtuel d'équilibrage de charge donnée correspond, il récupère le nom et le nom du groupe de services.

Utiliser des sources de données personnalisées

En plus des instances NetScaler gérées en tant que source de données, vous pouvez définir et utiliser des sources de données personnalisées si les données d'entrée sont utilisées de manière répétée pour créer plusieurs configurations. Vous pouvez enregistrer les données d'entrée dans NetScaler Console en tant que source de données. Et vous pouvez modifier les StyleBooks pour

© 1997–2026 Citrix Systems, Inc. All rights reserved.

consommer ces données sans obliger les utilisateurs de StyleBook à fournir des entrées de manière répétée.

Avant d'utiliser une source de données personnalisée dans votre définition StyleBook, procédez comme suit pour définir une source de données personnalisée :

1. Ajouter un type de source de données.
2. Ajouter un schéma de collection sous le type de source de données.
3. Ajouter une source de données.
4. Ajouter des données de collection.

Après avoir ajouté une source de données, vous pouvez l'utiliser dans la définition StyleBook. Pour plus d'informations, consultez Utiliser des sources de données personnalisées dans la définition StyleBook.

Ajouter un type de source de données

Spécifiez un type de source de données pour distinguer la source à partir de laquelle les données sont récupérées.

1. Dans **Applications > Configuration > Sources de données**.
2. Sélectionnez **Type de source de données** et cliquez sur **Ajouter**.
3. Spécifiez le **Nom** et la **Description** du type de source de données.
4. Cliquez sur **Continuer** pour enregistrer le **Type de source de données**. Cliquez sur **Fermer** pour quitter le workflow sans enregistrer les modifications.



Dans cet exemple, le type de source de données est défini sur **Environnement**. Ce type peut être utilisé pour définir les environnements d'application comme sources de données.

Ajouter un schéma de collection sous le type de source de données

Après avoir ajouté le **Type de source de données**, un écran permettant d'ajouter des **Schémas de collection** pour le ""Type de source de données** s'affiche.

1. Cliquez sur **Ajouter**.
2. Spécifiez le **Nom de la collection** pour un schéma de collection.
3. Saisissez la **Description**.
4. Ajoutez des attributs (nom et son type) sous **Détails des attributs** selon les besoins.
5. Cliquez sur **Créer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Dans cet exemple, le schéma de collection **App-virtual-servers** comporte quatre attributs. Par conséquent, la collection que vous souhaitez stocker doit avoir ces attributs des types de données définis.

Ajouter une source de données

Définissez une source de données pour un type de source de données spécifique.

1. Accédez à **Applications > Configuration > Sources de données**.
2. Sélectionnez l'onglet **Sources de données** et cliquez sur **Ajouter**.
3. Spécifiez le **Nom**.
4. Sélectionnez le **Type de source de données**, et entrez la **Description**.
5. Cliquez sur **Continuer** pour enregistrer la **Source de données**. Cliquez sur **Fermer** pour quitter le workflow sans enregistrer les modifications.



Dans cet exemple, l'**environnement de production** est ajouté en tant que source de données.

Ajouter des données de collection

Après avoir ajouté la **Source de données**, un écran permettant de saisir les données de la **Source de données** s'affiche. Vous pouvez voir une liste de **Schémas de collection**.

1. Sélectionnez le **Schéma de collection** auquel vous souhaitez ajouter des données de collection.
2. Cliquez sur **Gérer les données de collection**.
3. Ajoutez des données à la collection. Vous pouvez ajouter des données une par une ou télécharger un fichier CSV. Lorsque vous téléchargez un fichier CSV, assurez-vous que les noms de colonnes correspondent aux noms d'attributs du schéma de collection.
4. Cliquez sur **OK**.



Utiliser une source de données personnalisée sans collection

La section `parameters` suivante explique comment définir une source de données personnalisée dans la définition StyleBook sans collection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

    - name: selected-environment

      label: Select a custom datasource environment

      type: datum

      required: true

      data-source:

        type: "Environment"
```

L'interface graphique du pack de configuration affiche les sources de données applicables et les utilisateurs de StyleBook peuvent en sélectionner une pour créer un pack de configuration.

Dans cet exemple, il utilise la source de données `Production` pour récupérer des données.

Dans le type de source de données `Environment`, pour accéder au type de collection `App-virtual-servers`, utilisez l'expression suivante :

```
$parameters.selected-environment.collections.App-virtual-servers
```

Extrait d'exemple :

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    repeat: $parameters.selected-environment.collections.App-virtual-
servers

    repeat-item: app

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: $app.attributes.Name + "-lb"
    ipv46: ip($app.attributes.IPv46 )
    port: $app.attributes.Port
    servicetype: $app.attributes.Protocol
  components:


    -
      name: servicegroup-comp
      type: ns::servicegroup
      properties:
        servicegroupname: $parent.properties.name + "-svcgrp"
        servicetype: $parent.properties.servicetype


      components:
        -
          name: lbvserver-svg-binding
          type: ns::lbvserver_servicegroup_binding
          properties:
            name: $parent.parent.properties.name
            servicegroupname: $parent.properties.servicegroupname
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser des sources de données personnalisées avec une collection

La section `parameters` suivante explique comment définir une source de données personnalisée dans la définition StyleBook. Elle permet aux utilisateurs de StyleBook de sélectionner un élément spécifique d'une collection.

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

Dans cet exemple, le paramètre `datum` est utilisé pour définir la source de données personnalisée. Il utilise la source de données `Production` pour récupérer des données du schéma de collection `App-virtual-servers`.

Dans le type de source de données `Environment`, pour accéder au protocole de la collection `App-virtual-servers`, utilisez l'expression suivante :

```
$parameters.selected-app-vserver.attributes.Protocol
```

Extrait d'exemple :

```
components:

  - name: lbvserver-comp

    type: ns::lbvserver

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      name: $parameters.selected-app-vserver.attributes.Name

      ipv46: $parameters.selected-app-vserver.attributes.IPv46

      port: $parameters.selected-app-vserver.attributes.Port

      servicetype: $parameters.selected-app-vserver.attributes.Protocol
```

Lorsque vous définissez un type de collection dans la section `parameters`, les utilisateurs de StyleBook peuvent sélectionner la source de données et la collection.

Sélection de plusieurs éléments d'une collection :

La section des paramètres suivante permet aux utilisateurs de StyleBook de sélectionner plusieurs éléments d'une collection.

```
parameters:

  - name: selected-app-vservers

    label: Select app-vservers from the collection

    type: datum[]

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

Dans cet exemple, le paramètre datum est utilisé pour définir le tableau de sources de données personnalisées. L'utilisateur peut sélectionner un ou plusieurs éléments de la collection « App-virtual-servers » à partir d'une seule source de données ou de plusieurs sources de données.

L'extrait de code ci-dessous décrit la manière d'accéder aux éléments sélectionnés et à leurs attributs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

   name: lbvserver-comp

   type: ns::lbvserver

   repeat:

   repeat-list: $parameters.selected-app-vservers

   repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.Name

      ipv46: $vserverObj.attributes.IPv46

      port: $vserverObj.attributes.Port

      servicetype: $vserverObj.attributes.Protocol
```

Filtrage des données de collection :

La section des paramètres suivante explique comment spécifier des filtres sur une collection de sources de données personnalisées dans la définition StyleBook. Elle permet aux utilisateurs de StyleBook de sélectionner un élément spécifique d'une collection filtrée.

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: Environment

      collection: App-virtual-servers

      collection-filters:

        Protocol: SSL
```

Dans cet exemple, le paramètre datum est utilisé pour définir la source de données personnalisée. Il utilise la source de données de type Environnement pour récupérer les données filtrées du schéma de collection App-virtual-servers.

Une fois que l'utilisateur StyleBook a sélectionné un serveur virtuel, tout attribut de l'élément sélectionné est accessible de la même manière que celle expliquée dans la section précédente.

Utiliser les API pour créer des configurations à partir de StyleBooks

Après avoir créé votre StyleBook, vous devez l'importer soit en utilisant l'interface graphique de NetScaler Console, soit en utilisant les API de NetScaler Console. NetScaler Console valide votre StyleBook lors de l'importation. Si la validation est réussie, votre StyleBook apparaît dans le catalogue de StyleBooks de NetScaler Console, prêt à être utilisé pour créer des configurations.

Vous pouvez maintenant utiliser les API StyleBook pour créer des configurations basées sur ce StyleBook. Vous pouvez utiliser n'importe quel outil, tel que l'outil de ligne de commande cURL ou l'extension de navigateur Chrome Postman, pour envoyer des requêtes HTTP à NetScaler Console.

Exemple 1

Considérez le StyleBook lb-vserver que vous avez créé dans StyleBook pour créer un serveur virtuel d'équilibrage de charge. Utilisez les API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

MÉTHODE HTTP: POST **URL**: `https://<IP>/stylebook/nitro/v2/config/configpacks`

En-têtes de requête:

Content-Type: application/json

Accept: application/json

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CHARGE UTILE DU CORPS DE LA REQUÊTE:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Dans cette requête HTTP, le serveur virtuel d'équilibrage de charge `lb1` avec l'adresse IP 10.102.117.31 est créé sur l'instance NetScaler avec un ID d'instance de "deecee30-f478-4446-9741-a85041903410". L'ID d'instance de l'instance NetScaler est récupéré depuis NetScaler Console.

Pour obtenir l'ID d'une instance gérée par NetScaler Console, vous pouvez utiliser les API NetScaler Console. Par exemple, pour récupérer l'ID d'instance ou une instance NetScaler dont l'adresse IP est 192.168.153.160, vous pouvez utiliser l'API suivante :

MÉTHODE HTTP: GET

URL: `https://<IP>/nitro/v2/config/ns?filter=ip_address:192.168.153.160`

EN-TÊTES DE REQUÊTE:

Accept: application/json

La réponse contient l'ID dans la charge utile JSON :

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{
  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "resourceName": "",
  "ns":
  [
    {
    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
   }
 ]
}
```

Si la configuration (pack de configuration) est créée avec succès, vous recevez la réponse HTTP suivante :

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès) :

202 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{
  "job":
  {
    "job_id": "1460806080"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  }

}
```

Vous avez créé votre premier travail, identifié de manière unique par l'ID 1460806080. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration.

Vous pouvez utiliser l'URL suivante pour interroger l'état du travail :

`https://<IP>/stylebook/nitro/v2/config/jobs/<jobid>`.

Exemple 2

Vous pouvez utiliser le même StyleBook pour créer un autre pack de configuration et l'exécuter sur les mêmes instances NetScaler ou sur des instances différentes. Dans cet exemple, créez une autre configuration et fournissez un nom et une adresse IP différents pour le serveur virtuel. Spécifiez LEASTCONNECTION comme méthode d'équilibrage de charge. Déployez cette configuration sur deux instances NetScaler.

La requête HTTP est la suivante :

MÉTHODE HTTP : POST

URL : `https://<IP>/stylebook/nitro/v2/config/configpacks`

EN-TÊTES DE REQUÊTE :

Content-Type: application/json

Accept: application/json

CHARGE UTILE DU CORPS DE LA REQUÊTE :

```
{

  "configpack":

  {

    "parameters": {

      "name": "lb1",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "vip-ipaddress": "10.102.117.31",
      "lb-alg": "LEASTCONNECTION"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "instance_id": "abcdee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

Dans cette requête HTTP, le serveur virtuel d'équilibrage de charge lb1 avec l'adresse IP 10.102.117.31 est créé sur les deux instances NetScaler avec les ID d'instance « deecee30-f478-4446-9741-a85041903410 » et « abcdee30-f478-4446-9741-a85041903410 ».

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lors de la création réussie du pack de configuration, la réponse HTTP suivante est reçue :

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès) :

202 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

    "job": {

        "job_id": "165769629"

    }

}
```

Ce nouveau pack de configuration a un ID différent, 1657696292. Vous pouvez mettre à jour ou supprimer cette configuration en utilisant cet ID.

Exemple 3

Considérez le StyleBook « basic-lb-config » que vous avez créé dans StyleBook pour créer une configuration d'équilibrage de charge de base. Utilisez les API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

MÉTHODE HTTP : POST

URL : `https://<IP>/stylebook/nitro/v2/config/configpacks`

EN-TÊTES DE REQUÊTE :

Content-Type: application/json

Accept: application/json

CHARGE UTILE DU CORPS DE LA REQUÊTE :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Content-Type: application/json

Accept: application/json

{

  "configpack":

  {

    "parameters":

    {

      "name": "myapp",

      "ip": "10.70.122.25",

      "svc-servers": ["192.168.100.11","192.168.100.12"],

       "svc-port": 8080

    },

    "targets":

    [

     {

      "instance_id": "deecee30-f478-4446-9741-a85041903410"

     },

     {

      "instance_id": "abcdefgi-d589-4557-8632-a74032802412"

     }

    ],

    "stylebook": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "name": "basic-lb-config",

            "namespace": "com.example.stylebooks",

            "version": "0.1"

        }

  }

}
```

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès) :

202 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Dans cette requête HTTP, la configuration d'équilibrage de charge s'exécute sur deux instances NetScaler. Vous pouvez vous connecter à ces instances NetScaler pour vérifier si un serveur virtuel et un groupe de services avec deux services liés sont créés.

Exemple 4

Considérez le StyleBook composite **composite-example** que vous avez créé dans Créer un StyleBook composite. Utilisez les API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

MÉTHODE HTTP: POST

© 1997–2026 Citrix Systems, Inc. All rights reserved.

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

EN-TÊTES DE REQUÊTE:

Content-Type: application/json

Accept: application/json

CHARGE UTILE DU CORPS DE LA REQUÊTE:

```
{
  "configpack":
  {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
    },
    "targets":
    [
     {
      "id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "id": "abcdefgg-d589-4557-8632-a74032802412"
     }
    ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "stylebook": {

            "name": "composite-example",

            "namespace": "com.example.stylebooks",

            "version": "0.1"

        }

  }
```

Dans cette requête HTTP, la configuration est créée sur deux instances NetScaler représentées par leurs identifiants. Si vous vous connectez aux instances NetScaler, vous pouvez afficher les objets de configuration créés par le StyleBook « basic-lb-config » qui a été importé dans le StyleBook « composite-example ». Vous pouvez également voir un nouveau moniteur HTTP appelé myapp-mon qui faisait partie du StyleBook « composite-example ».

Après la création réussie du pack de configuration, la réponse HTTP suivante est reçue :

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès):

202 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mise à jour d'une configuration

Considérez une configuration que vous souhaitez mettre à jour avec un nouveau serveur back-end ayant l'adresse IP 10.102.29.54. Pour ajouter le serveur au serveur virtuel d'équilibrage de charge myapp, utilisez l'API suivante :

MÉTHODE HTTP: PUT

URL : `https://<IP>/stylebook/nitro/v2/config/configpacks/<configpackid>`

EN-TÊTES DE REQUÊTE :

Content-Type: application/json

Accept: application/json

CHARGE UTILE DU CORPS DE LA REQUÊTE :

```
{
  "configpack": {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
  },
  "targets":
   [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "instance_id": "abdcedff-d589-4557-8632-a74032802412"
     }
   ]
  }
}
```

Lors de la mise à jour réussie du pack de configuration, la réponse HTTP suivante est reçue :

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès) :

202 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{
    "job": {
        "job_id": "3628681382"
    }
}
```

Suppression d'une configuration

Pour supprimer cette configuration (de toutes les instances NetScaler), vous pouvez utiliser l'API de suppression d'un pack de configuration comme suit :

Lors de la suppression réussie du pack de configuration, la réponse HTTP suivante est reçue :

MÉTHODE HTTP : DELETE

URL : `https://<DNS-or-IP>//stylebook/nitro/v2/config/configpacks/<configpackid>`

EN-TÊTES DE REQUÊTE:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accept: application/json

EN-TÊTES DE RÉPONSE ATTENDUS (en cas de succès):

202 OK

Content-Type: application/json

CHARGE UTILE DE RÉPONSE ATTENDUE (en cas de succès):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Connectez-vous à l'instance NetScaler et vérifiez que tous les objets de configuration faisant partie de ce pack de configuration ont été supprimés.

Pour supprimer la configuration d'une instance NetScaler spécifique au lieu de toutes les instances, utilisez l'opération de mise à jour du pack de configuration dans Mise à jour d'une configuration. Modifiez l'attribut targets dans la charge utile JSON pour supprimer les ID d'instance NetScaler spécifiques.

Utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificat et de clé

Utilisez les API StyleBook pour créer des configurations basées sur ce StyleBook. Vous pouvez utiliser n'importe quel outil, tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman, pour envoyer des requêtes HTTP à NetScaler Console.

Considérez l'exemple de StyleBook que vous avez créé pour télécharger les fichiers de certificat et de clé dans Comment créer un StyleBook pour télécharger des fichiers de certificat SSL et de clé de certificat vers NetScaler Console. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
POST


https://<MAS_IP_Address>/stylebook/nitro/v2/config/configpacks?mode=async
```

```
Content-Type: application/jsonAccept: application/json


{
    "configpack": {
        "stylebook": {
            "name": "lb-mon_test",
            "namespace": "com.citrix.adc.stylebooks",
            "version": "2.0"
        },
        "parameters": {
            "lb-service-type": "SSL",
            "ip-address-type": "IP Address",
            "lb-appname": "testvip",
            "lb-virtual-port": 80,
            "svc-service-type": "SSL",
            "lb-virtual-ip": "10.10.20.11",
            "certificates": [
                {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    "ssl-inform": "PEM",
                    "certkey-param": {
                        "id": "d0982579-42a9-417a-b24e-1f9ae5592f1d",
                        "name": "testcertkey"
                    }
                }
            ]
        },
        "targets": [
            {
                "instance_id": "f383b454-b777-454a-8c17-c477f0bad21e"
            }
        ]
    }
}
```

Ce pack de configuration est identifié de manière unique par l'ID f383b454-b777-454a-8c17-c477f0bad21e. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration. Lors de la mise à jour réussie du pack de configuration, les fichiers de certificat et de clé sont téléchargés dans le système de fichiers de NetScaler Console.

Utiliser l'API pour créer des configurations afin de télécharger n'importe quel type de fichier

Vous pouvez également utiliser l'API NetScaler Console pour créer un pack de configuration qui télécharge des fichiers vers l'instance NetScaler sélectionnée. Reportez-vous à l'exemple de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

téléchargement de fichiers de tout type dans Comment créer un StyleBook pour télécharger des fichiers vers le service NetScaler MA. Comme expliqué dans l'exemple, créez un pack de configuration et définissez la valeur du paramètre 'locationfile' sur le chemin de fichier du fichier d'emplacement sur NetScaler Console. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

```
POST



https://<mas_ip>/stylebook/nitro/v2/config/configpacks?mode=sync
```

```
Content-Type: application/json

Accept: application/json

{

    "configpack": {

        "stylebook": {

            "name": "upload-geolocations",

            "namespace": "com.citrix.adc.stylebooks.samples",

            "version": "1.0"

        },

        "parameters": {

            "locationfile": {

                "name": "servercert1.key",

                "contents": "<base64-contents>",

                "encoding_type": "base64"

            }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        "targets": [
            {
                "instance_id": "d9dca475-abde-47ef-bf99-8434fe6ad886"
            }
        ]
    }
}
```

Utiliser l'API pour importer des StyleBooks personnalisés

Vous pouvez désormais utiliser les API StyleBook pour importer des StyleBooks personnalisés dans NetScaler Console. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook, comme suit, dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman. Par exemple, vous pouvez importer un StyleBook nommé example-lb qui peut être utilisé pour créer une configuration d'équilibreur de charge sur une instance NetScaler.

```
HTTP Method: POST

URL: http://<mas-ip>/stylebook/nitro/v2/config/stylebooks/actions/import?
mode=sync

Headers:

Content-Type: application/json

Accept: application/json

RequestBody:

{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "import": {
        "file_name": "example-lb.yaml",
        "source": "<base64-contents>",
        "encoding": "base64"
    }
}
```

où la valeur de l'attribut « source » est l'encodage base64 du contenu de votre fichier StyleBook. Vous pouvez coller le contenu YAML de votre fichier StyleBook dans un outil en ligne, par exemple, `<https://www.browserling.com/tools/file-to-base64>` pour obtenir la chaîne base64 que vous pourrez ensuite utiliser comme valeur pour l'attribut « source » ci-dessus.

En utilisant cet appel d'API, vous pouvez également télécharger un fichier tarball compressé (fichier .tgz) contenant plusieurs fichiers StyleBook en une seule opération d'API. Pour ce faire, il suffit de modifier l'attribut file_name pour qu'il corresponde au nom du fichier .tgz et la valeur de l'attribut source pour qu'elle corresponde à l'encodage base64 du contenu de votre fichier .tgz.

Une fois l'API exécutée avec succès dans l'outil, vous obtenez la réponse suivante qui indique que le StyleBook a été importé dans NetScaler Console.

```
200 OK
```

Corps de la réponse :

```
{
    "import": {
        "name": "example-lb",
        "namespace": "com.citrix.adc.stylebooks",
        "version": "2.0"
    }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Utiliser l'API pour télécharger des StyleBooks personnalisés

Vous pouvez télécharger un StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

```
POST

http://<MAS_IP>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>/actions/actions/download?dependencies=true



payload



dependencies=true
```

Vous pouvez exécuter l'API dans n'importe quel outil, tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman, après avoir apporté des modifications aux champs d'adresse IP, de nom, de version et d'espace de noms.

```
POST



http://10.102.201.246/stylebook/nitro/v2/config/stylebooks/
com.samples.adc.stylebooks/1.2/lb-mon/actions/download?dependencies=true



payload

dependencies=true
```

Le StyleBook au format .yaml est téléchargé.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser l'API pour supprimer des StyleBooks personnalisés

Vous pouvez supprimer le StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

```
DELETE



http://<MAS_IP>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>?dependencies=true
```

Si le paramètre de requête des dépendances dans l'URL n'est pas fourni ou si sa valeur est définie sur false, alors les dépendances du StyleBook ne sont pas supprimées (seul le StyleBook lui-même est supprimé).

Lorsque vous recevez un code d'état de réponse HTTP de 200, cela signifie que le StyleBook personnalisé et ses dépendances ont été supprimés avec succès de NetScaler Console.

REMARQUE :

Vous ne pouvez pas supprimer un StyleBook personnalisé qui a d'autres StyleBooks dans le service MA qui en dépendent.

Par exemple, supposons que vous ayez créé un StyleBook nommé « lb-virtual-ssl-extended » dans NetScaler Console. Vous avez ensuite décidé de supprimer ce StyleBook.

Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman après avoir apporté des modifications aux champs d'adresse IP, de nom, de version et d'espace de noms.

DELETE `<http://10.102.201.246/stylebook/nitro/v2/config/stylebooks/com.citrix.adc.stylebooks/2.0/lb-mon_delete?dependencies=false>`

Le StyleBook est supprimé de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Grammaire des StyleBooks

Vous pouvez concevoir vos propres StyleBooks, les importer dans NetScaler Console, puis les utiliser pour créer des configurations, soit à l'aide de l'interface graphique de NetScaler Console, soit à l'aide d'API. Pour pouvoir créer vos propres StyleBooks, vous devez d'abord comprendre la grammaire et la syntaxe des différentes constructions et attributs que vous pouvez utiliser.

Ce document décrit les différentes constructions et références que vous pouvez utiliser lors de la création de StyleBooks.

Cliquez sur une section, une construction ou un nom de référence dans le tableau ci-dessous pour afficher les détails.

En-tête	Importer des StyleBooks
Paramètres	Construction des sources par défaut des paramètres
Substitutions	Composants
Propriétés facultatives	Composants d'aide
Sources par défaut des propriétés	Composants imbriqués
Construction de condition	Construction de répétition(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/repeat-construct.html)
Construction de répétition conditionnelle(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	Sorties(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/outputs.html)
Répétitions imbriquées(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/nested-repeats.html)	Référence parente(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/parent-reference.html)
Référence de paramètre(/fr-fr/netscaler-application-delivery-management-software/	Référence de substitutions(/fr-fr/netscaler-application-delivery-management-software/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

current-release/stylebooks/stylebooks-grammar/parameter-reference.html)	current-release/stylebooks/stylebooks-grammar/substitutions-reference.html)
Référence de composants(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/components-reference.html)	Opérations(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/operations.html)
Référence de variable(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/variable-reference.html)	Alarmes(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/alarms.html)
Analytique(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/analytics.html)	Fonctions intégrées(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/built-in-functions.html)
Expressions(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/expressions.html)	Détection de dépendances(/fr-fr/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/dependency-detection.html)
Interpolations sur place	

REMARQUE

Lors de la définition de repeat-item, repeat-index ou d'arguments pour les fonctions de substitution, n'utilisez pas les mots réservés suivants pour nommer une variable définie par l'utilisateur, $`<var-name>`

- stylebook, paramètres, substitutions, composants, propriétés, sorties, parent, soi, opérations, analyses, alarmes
- repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
- repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
- par défaut
- rôles, rôle, cibles, cible
- contexte, contexte parent, contexte parent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations et des exemples sur la conception de vos propres StyleBooks, consultez Comment créer vos propres StyleBooks.

En-tête

Les six premières lignes d'un StyleBook constituent la section d'en-tête. Cette section vous permet de définir l'identité d'un StyleBook et de décrire ce qu'il fait. C'est une section obligatoire.

Le tableau suivant décrit les attributs de la section d'en-tête :

ATTRIBUT	DESCRIPTION
nom	Un nom pour identifier le StyleBook. Cet attribut est obligatoire.
display-name	Un nom descriptif pour le StyleBook. Ce nom apparaît dans l'interface graphique de NetScaler Console. C'est un attribut facultatif.
Description	Un texte de description définit ce que fait ce StyleBook. Cette description apparaît dans l'interface graphique de NetScaler Console. C'est un attribut facultatif. **Remarque :** Il s'agit d'un fragment HTML et vous pouvez utiliser des balises HTML pour personnaliser les titres ou insérer des images à l'aide de la balise `<img>` avec des URL ou des images intégrées.
auteur	La personne ou l'organisation auteur qui crée le StyleBook. C'est un attribut facultatif.
espace de noms	Un espace de noms fait partie d'un identifiant unique pour un StyleBook afin d'éviter les conflits de noms. Un espace de noms peut être n'importe quelle chaîne de caractères, mais une bonne pratique consiste à l'utiliser pour nommer l'entreprise, le département ou l'unité qui a créé ou possède un ensemble de StyleBooks. Par exemple, vous pouvez utiliser le format suivant : `<company>.<department>.<unit>.stylebooks`. Cet attribut est obligatoire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	DESCRIPTION
Version	Le numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour un StyleBook. Les StyleBooks de différentes versions peuvent coexister. Il s'agit d'un attribut obligatoire.
schema-version	La version du schéma des StyleBooks. Elle prend la valeur « 1.0 » dans la version actuelle de NetScaler Console. Il s'agit d'un attribut obligatoire.
privé	Si cet attribut est défini sur true, le StyleBook n'est pas affiché sur l'interface graphique de NetScaler Console. Il s'agit d'un paramètre utile pour les StyleBooks qui sont des blocs de construction pour d'autres StyleBooks et qui ne sont pas destinés à être utilisés directement par les utilisateurs. Il s'agit d'un attribut facultatif. Sa valeur par défaut est false.

Exemple :

```
    name: lb

    description: "This stylebook defines a sample load balancing
 configuration."

    display-name: "Load Balancing StyleBook (HTTP)"

    author: Mike Smith (ACME Infra team)

    namespace: com.example.stylebooks

    schema-version: "1.0"

    version: "0.1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La combinaison du nom, de l'espace de noms et de la version identifie de manière unique un StyleBook dans le système. Vous ne pouvez pas avoir deux StyleBooks avec la même combinaison de nom, d'espace de noms et de version dans NetScaler Console. Cependant, vous pouvez avoir deux StyleBooks avec le même nom et la même version mais des espaces de noms différents, ou avec le même espace de noms et la même version mais des noms différents.

Importer des StyleBooks

Ceci est la deuxième section de votre StyleBook et vous permet de déclarer à quel autre StyleBook vous souhaitez faire référence depuis votre StyleBook actuel. Cela vous permet d'importer et de réutiliser d'autres StyleBooks au lieu de reconstruire la même configuration dans votre propre StyleBook. Cette section est obligatoire.

Vous devez déclarer le **namespace** et le numéro de **version** du ou des StyleBook(s) auxquels vous souhaitez faire référence dans votre StyleBook actuel. Chaque StyleBook doit faire référence au namespace netscaler.nitro.config s'il utilise directement l'un des objets de configuration NITRO. Ce namespace contient tous les types NetScaler NITRO, tels que le service lbvserver ou le moniteur. Les StyleBooks pour les versions 10.5 et ultérieures de NetScaler sont pris en charge, ce qui signifie que vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur toute instance NetScaler exécutant la version 10.5 ou ultérieure.

L'attribut **prefix** utilisé dans la section import-stylebooks est un raccourci pour faire référence à la combinaison du namespace et de la version. Par exemple, le préfixe « ns » peut être utilisé pour faire référence au namespace netscaler.nitro.config avec la version 10.5. Dans les sections ultérieures de votre StyleBook, au lieu d'utiliser le namespace et la version chaque fois que vous souhaitez faire référence à un StyleBook avec ce namespace et cette version, vous pouvez simplement utiliser la chaîne de préfixe choisie avec le nom du StyleBook pour l'identifier de manière unique.

Exemple :

```
import-stylebooks:
 -
   namespace: netscaler.nitro.config
   version: "10.5"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    prefix: ns

-

 namespace: com.acme.stylebooks

  version: "0.1"

  prefix: stlb
```

Dans l'exemple ci-dessus, le premier préfixe défini est appelé ns et fait référence au namespace netscaler.nitro.config et à la version 10.5. Le second préfixe défini est appelé stlb et fait référence au namespace com.acme.stylebooks et à la version 0.1.

Après avoir défini un préfixe, chaque fois que vous souhaitez faire référence à un type ou à un StyleBook appartenant à un certain namespace et à une certaine version, vous pouvez utiliser la notation **\<raccourci-namespace\>::\<nom-type\>**. Par exemple, **ns::lbvserver** fait référence au type lbvserver défini dans le namespace netscaler.nitro.config, version 10.5.

De même, si vous souhaitez faire référence à un StyleBook avec la version « 0.1 » dans le namespace com.acme.stylebooks, vous pouvez utiliser la notation **stlb::\<nom-stylebook\>**.

REMARQUE

Par convention, le préfixe « ns » est utilisé pour faire référence au namespace NITRO de NetScaler.

Paramètres

Cette section vous permet de définir tous les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Elle décrit l'entrée que votre StyleBook prend. Bien que cette section soit facultative, la plupart des StyleBooks pourraient en avoir besoin. Vous pouvez considérer la section des paramètres pour définir les champs pour les utilisateurs qui utilisent le StyleBook pour créer une configuration sur une instance NetScaler.

Lorsque vous importez votre StyleBook dans NetScaler Console et l'utilisez pour créer une configuration, l'interface graphique utilise cette section du StyleBook pour afficher un formulaire. Ce formulaire prend une entrée pour les valeurs de paramètres définies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La section suivante décrit les attributs que vous devez spécifier pour chaque paramètre de cette section :

'nom'

Le nom du paramètre que vous souhaitez définir. Vous pouvez spécifier un nom alphanumérique.

Le nom doit commencer par une lettre et peut inclure d'autres lettres, des chiffres, un trait d'union (-) ou un trait de soulignement (_).

Lors de la rédaction d'un StyleBook, vous pouvez utiliser cet attribut "name" pour faire référence au paramètre dans d'autres sections en utilisant la notation $parameters.\<name>.

Obligatoire ? Oui

'libellé'

Une chaîne qui est affichée dans l'interface graphique de NetScaler Console comme nom de ce paramètre.

Obligatoire ? Non

'Description'

Une chaîne d'aide qui décrit l'utilisation du paramètre. L'interface graphique de NetScaler Console affiche ce texte lorsque l'utilisateur clique sur l'icône d'aide pour ce paramètre.

Obligatoire ? Non

« type »

Le type de valeur que ces paramètres peuvent prendre. Les paramètres peuvent être de l'un des types intégrés suivants :

- string : Un tableau de caractères. Si une longueur n'est pas spécifiée, la valeur de la chaîne peut prendre n'importe quel nombre de caractères. Cependant, vous pouvez limiter la longueur d'un type de chaîne en utilisant les attributs min-length et max-length.
- `number` : Un nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs min-value et max-value.
- `boolean` : Peut être vrai ou faux. YAML considère tous les littéraux comme des booléens (par exemple, Oui ou Non).
- `ipaddress` : Une chaîne qui représente une adresse IPv4 ou IPv6 valide.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ipnetwork` : Il a deux parties. La première partie est l'adresse IP et la seconde partie est le masque de sous-réseau.

  Le masque de sous-réseau se compose de la longueur du masque de sous-réseau (`netmask-len`) ou de l'adresse IP du masque de sous-réseau (`netmask_ip`). La longueur du masque de sous-réseau est un entier compris entre 0 et 32 et entre 0 et 128 pour une adresse IPv6. Il est utilisé pour déterminer le nombre d'adresses IP dans un réseau.

  Lors de la création ou de la mise à jour d'un pack de configuration à partir de l'interface graphique de NetScaler Console, vous pouvez effectuer l'une des actions suivantes :

  - Activer la longueur du masque de sous-réseau et saisir l'adresse IP et la longueur du masque de sous-réseau
  - Désactiver la longueur du masque de sous-réseau et saisir l'adresse IP et l'adresse IP du masque de sous-réseau

  Dans l'API, la longueur du masque de sous-réseau et l'adresse IP du masque de sous-réseau sont disponibles sous forme de valeur unique, comme le montre l'exemple suivant :

  Exemple :

```
Content-Type: application/json

Accept: application/json

{

“configpack”:

{

      “stylebook”: {

      “namespace”: “com.example.stylebook”,

      “version”:“1.0”,

      “name”: “ipnetwork-example”,

      ..
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        “parameters”: {
           “name: “test-app”,
            “virtual-ip”: “212.100.30.0/255.255.255.0”,
        },
        “targets”:
        [
        ]
  }
  }
```

- `tcp-port` : Un nombre compris entre 0 et 65535 qui représente un port TCP ou UDP.
- `password` : Représente une valeur de chaîne opaque/secrète. Lorsque l'interface graphique de NetScaler Console affiche une valeur pour ce paramètre, elle est représentée par des astérisques (*****).
- `certfile` : Représente un fichier de certificat. Cette valeur vous permet de télécharger les fichiers directement depuis votre système local lorsque vous créez une configuration StyleBook à l'aide de l'interface graphique de NetScaler Console. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` de NetScaler Console.

  Le fichier de certificat est ajouté à la liste des certificats gérés par NetScaler Console.
- `keyfile` : Représente un fichier de clé de certificat. Cette valeur vous permet de télécharger le fichier directement depuis votre système local lorsque vous créez une configuration StyleBook à l'aide de l'interface graphique de NetScaler Console. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` de NetScaler Console.

  Le fichier de clé de certificat est ajouté à la liste des clés de certificat gérées par NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `file` : Représente un fichier.
- `object` : Ce type est utilisé lorsque vous souhaitez regrouper plusieurs paramètres connexes sous un élément parent. Spécifiez le type du paramètre parent comme "object". Un paramètre de type "object" peut avoir une section "parameters" imbriquée pour décrire les paramètres qu'il contient.
- `another StyleBook` : Lorsque vous utilisez ce type de paramètre, ce paramètre s'attend à ce que sa valeur soit sous la forme des paramètres définis dans le StyleBook désignant son type.

Un paramètre peut également avoir un `type` qui est la liste des types. Pour ce faire, ajoutez `[]` à la fin du type. Par exemple, si l'attribut `type` est `string[]`, ce paramètre prend une liste de chaînes en entrée. Vous pouvez fournir une, deux ou plusieurs chaînes pour ce paramètre lors de la création d'une configuration à partir de ce StyleBook.

Obligatoire ? Oui

'réseau'

Pour `type: ipaddress`, vous pouvez spécifier l'attribut `network` pour allouer automatiquement une adresse IP à partir d'un réseau IPAM de NetScaler Console.

NetScaler Console alloue automatiquement une adresse IP à partir de l'attribut `network` lorsque vous créez une configuration StyleBook.

Exemple :

```
name: virtual-ip

label: "Load Balancer IP Address"

type: ipaddress

network: "network-1"

required: true
```

Dans cet exemple, le champ `virtual-ip` alloue automatiquement une adresse IP à partir de `network-1`. L'adresse IP est libérée vers le réseau lorsque la configuration est supprimée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'dynamic-allocation'

L'attribut `dynamic-allocation` est ajouté dans la définition du paramètre de `type:ipaddress`. Utilisez cet attribut pour lister dynamiquement les réseaux IPAM de NetScaler Console. Cet attribut peut prendre `true` ou `false` comme entrée. Pour `type: ipaddress`, spécifiez l'attribut `dynamic-allocation: true` pour lister dynamiquement les réseaux IPAM de NetScaler Console qui se trouvent dans NetScaler Console. Dans le formulaire de création de pack de configuration, vous pouvez effectuer les opérations suivantes :

1. Sélectionnez le réseau IPAM requis dans la liste.
2. Spécifiez une adresse IP que vous souhaitez allouer à partir du réseau IPAM sélectionné.

   Si aucune adresse IP n'est spécifiée, NetScaler Console alloue automatiquement une adresse IP à partir du réseau IPAM sélectionné.

Exemple :

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"

  type: ipaddress

  dynamic-allocation: true

  required: true
```

Dans cet exemple, le champ `virtual-ip` liste les réseaux IPAM de NetScaler Console qui se trouvent dans NetScaler Console. Sélectionnez un réseau dans la liste pour allouer automatiquement une adresse IP à partir de ce réseau. L'adresse IP est libérée et renvoyée au réseau lorsque la configuration est supprimée.

'clé'

Spécifiez true ou false pour indiquer si ce paramètre est un paramètre clé pour le StyleBook.

Un StyleBook ne peut avoir qu'un seul paramètre défini comme paramètre « clé ».

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque vous créez différentes configurations à partir du même StyleBook (sur les mêmes ou différentes instances NetScaler), chaque configuration a une valeur différente/unique pour ce paramètre.

La valeur par défaut est false.

Obligatoire ? Non

'obligatoire'

Spécifiez true ou false pour indiquer si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création des configurations.

L'interface graphique de NetScaler Console force l'utilisateur à fournir une valeur valide pour ce paramètre.

La valeur par défaut est false.

Obligatoire ? Non

'allowed-values'

Utilisez cet attribut pour définir une liste de valeurs valides pour un paramètre, lorsque le type est défini sur "string".

Lors de la création d'une configuration à partir de l'interface graphique de NetScaler Console, l'utilisateur est invité à sélectionner une valeur de paramètre dans cette liste.

REMARQUE

Si vous souhaitez afficher les valeurs de la liste sous forme d'options radio, définissez l'attribut `layout`.

Exemple 1 :

```
-

      name: ipaddress

      type: string

      allowed-values:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            -  SOURCEIP

            -  DEST IP

            -  NONE
```

Exemple 2 :

```
-

      name: TCP Port

      type: tcp-port

      allowed-values:

            -  80

            -  81

            -  8080
```

Exemple 3 :

Liste de `tcp-ports`, où chaque élément de la liste ne peut avoir que les valeurs spécifiées dans `allowed-values`.

```
-

      name: tcpports

      type: tcp-port[]

      allowed-values:

            -  80

            -  81

            -  8080
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            -  8081
```

Obligatoire ? Non

'par défaut'

Utilisez cet attribut pour attribuer une valeur par défaut à un paramètre facultatif. Lorsqu'un utilisateur crée une configuration sans spécifier de valeur, la valeur par défaut est utilisée.

Le paramètre ne prend aucune valeur si les conditions suivantes sont remplies :

- Le paramètre n'a pas de valeur par défaut.
- Un utilisateur ne fournit pas de valeur pour le paramètre.

Exemple 1 :

```
-

      name: timeout

      type: number

      default: 20
```

Exemple 2 :

Pour lister les valeurs par défaut du paramètre :

```
-

      name: protocols

      type: string[]

      default:

            -  TCP

            -  UDP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            -  IP
```

Exemple 3 :

```
-

      name: timeout

      type: number

      default: 20
```

Exemple 4 :

```
-

      name: tcpport

      type: tcp-port

      default: 20
```

Obligatoire ? Non

'motif'

Utilisez cet attribut pour définir un motif (expression régulière) pour les valeurs valides de ce paramètre, lorsque le type du paramètre est "string".

Exemple :

```
-

      name: appname

      type: string

      pattern: "[a-z]+"
```

Obligatoire ? Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'min-value'

Utilisez cet attribut pour définir la valeur minimale pour les paramètres de type `number` ou `tcp-port`.

Exemple :

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

Le `min-value` des nombres peut être négatif. Cependant, le `min-value` pour `tcp-port` doit être positif.

Obligatoire ? Non

'max-value'

Utilisez cet attribut pour définir la valeur maximale des paramètres de type `number` ou `tcp-port`.

Assurez-vous que la valeur maximale est supérieure à la valeur minimale, si elle est définie.

Exemple :

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000

      max-value: 15000
```

Obligatoire ? Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'min-length'

Utilisez cet attribut pour définir la longueur minimale des valeurs acceptées pour un paramètre de type "string".

Assurez-vous que la longueur minimale des caractères définis comme valeurs est supérieure ou égale à zéro.

Exemple :

```
-

      name: appname

      type: string

      min-length: 3
```

Obligatoire ? Non

'max-length'

Utilisez cet attribut pour définir la longueur maximale des valeurs acceptées pour un paramètre de type "string".

Assurez-vous que la longueur maximale des valeurs est supérieure ou égale à la longueur des caractères définis dans `min-length`.

Exemple :

```
-

      name: appname

      type: string

      max-length: 64
```

Obligatoire ? Non

'min-items'

Utilisez cet attribut pour définir le nombre minimum d'éléments dans un paramètre qui est une liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assurez-vous que le nombre minimum d'éléments est supérieur ou égal à zéro.

Exemple :

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2
```

Obligatoire ? Non

'max-items'

Utilisez cet attribut pour définir le nombre maximum d'éléments dans un paramètre qui est une liste.

Assurez-vous que le nombre maximum d'éléments est supérieur au nombre minimum d'éléments, s'il est défini.

Exemple :

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2

      max-items: 250
```

Obligatoire ? Non

'interface graphique'

Utilisez cet attribut pour personnaliser la disposition du paramètre dans l'interface graphique de NetScaler Console.

Obligatoire ? Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'colonnes'

Cet attribut est un sous-attribut de l'attribut `gui`. Utilisez cet attribut pour définir le nombre de colonnes pour afficher les paramètres `type: object[]` dans l'interface graphique de NetScaler Console.

Obligatoire ? Non

'modifiable'

Cet attribut est un sous-attribut de l'attribut `gui`. Utilisez cet attribut pour spécifier si le paramètre peut être mis à jour après la création de la configuration. Définissez cet attribut uniquement sur des types de paramètres simples tels que chaîne, booléen ou nombre.

Si la valeur est définie sur `false`, le champ du paramètre est grisé lorsque vous mettez à jour la configuration.

Obligatoire ? Non

'collapse_pane'

Cet attribut est un sous-attribut de l'attribut `gui`. Utilisez cet attribut pour spécifier si le volet définissant la disposition de ce paramètre d'objet est réductible.

Si la valeur est définie sur true, l'utilisateur peut développer ou réduire les paramètres enfants sous ce paramètre parent.

Exemple :

```
gui:


 collapse_pane: true


 columns: 2
```

Exemple d'une section de paramètres complète :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

   -

      name: ip

      label: IP Address

      description: The virtual IP address used for this application
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: ipaddress

      required: true

  -

      name: svc-servers

      label: Servers

      type: object\[\]

      required: true

      parameters:

        -

              name: svc-ip

              label: Server IP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        description: The IP address of the server

        type: ipaddress

        required: true

    -

        name: svc-port

        label: Server Port

        description: The TCP port of the server

        type: tcp-port

        default: 80

    -

        name: lb-alg
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            label: LoadBalancing Algorithm

            type: string

            allowed-values:

               - ROUNDROBIN

               - LEASTCONNECTION

            default: ROUNDROBIN

      -

            name: enable-healthcheck

            label: Enable HealthCheck?

            type: boolean
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            default: true
```

Voici un exemple qui définit tous les attributs d'une liste et les valeurs expliquées dans les sections précédentes :

```
      -
            name: features-list

            type: string[]

            min-length: 1

            max-length: 3

            min-items: 1

            max-items: 3

            pattern: "\[A-Z\]+"

            allowed-values:

              - SP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                - LB


                - CS


              default:


                - LB
```

'mise en page'

Cet attribut est un sous-attribut de l'attribut `gui`. Utilisez cet attribut pour afficher les valeurs de liste sous forme de boutons radio. Définissez l'attribut `layout` sur `radio` dans la section des paramètres d'une définition de StyleBook. Il s'applique au paramètre qui possède l'attribut `allowed-values`. Lorsque vous créez un pack de configuration, l'interface graphique de NetScaler Console affiche les valeurs de la liste `allowed-values` sous forme de boutons radio.

Exemple :

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two

        - Three
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les valeurs Un, Deux et Trois apparaissent sous forme de boutons radio dans l'interface graphique de NetScaler Console.

'dependent-parameters'

Cet attribut est un sous-attribut de l'attribut `gui`. Il contrôle dynamiquement l'apparence du paramètre ou sa valeur initiale dans le formulaire de configuration StyleBook en fonction de la valeur spécifiée dans un autre paramètre.

Spécifiez cet attribut sur un paramètre source qui contrôle le comportement du paramètre sur le formulaire. Vous pouvez inclure plusieurs conditions qui contrôlent d'autres paramètres. Par exemple, un paramètre source `protocol` peut avoir un paramètre dépendant `certificate`, qui n'apparaît que si la valeur du paramètre `protocol` est `SSL`.

Chaque condition peut avoir les attributs suivants :

- **target-parameter** : Spécifiez le paramètre cible auquel cette condition s'applique.
- **matching-values** : Spécifiez la liste des valeurs du paramètre source qui déclenchent l'action.
- **action** : Spécifiez l'une des actions suivantes sur le paramètre ciblé :
  - `read-only` : Le paramètre est rendu en lecture seule.
  - `show` : Le paramètre apparaît dans le formulaire s'il est masqué.
  - `hide` : Le paramètre est supprimé du formulaire.
  - `set-value` : La valeur du paramètre est définie sur la valeur spécifiée dans l'attribut de valeur.
- **value** : La valeur du paramètre cible si l'action est `set-value`.

Lorsqu'une entrée utilisateur correspond aux valeurs spécifiées sur le paramètre source, l'apparence ou la valeur du paramètre cible change en fonction de l'action spécifiée.

Exemple :

```
-

   name: lb-virtual-port

   label: "Load Balanced App Virtual Port"

   description: "TCP port representing the Load Balanced application"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: tcp-port

    gui:

      updatable: false

      dependent-parameters:

            -

              matching-values:

                - 80

              target-parameter: $parameters.lb-service-type

              action: set-value

              allowed-values:

              - HTTP

              - TCP

              - UDP



    default: 80
```

Dans cet exemple, le paramètre dépendant est spécifié sous le paramètre `lb-virtual-port` (paramètre source).

Lorsque la valeur du paramètre source est définie sur `80`, le paramètre `lb-service-type` déclenche l'action `set-value`. Par conséquent, un utilisateur est autorisé à sélectionner l'une des options suivantes :

- HTTP
- TCP
- UDP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mécanisme parameters-default-sources

Vous pouvez utiliser cette fonctionnalité pour réutiliser les définitions de paramètres d'autres StyleBooks.

Considérez un scénario où un paramètre ou un groupe de paramètres est utilisé de manière répétée dans plusieurs StyleBooks. Pour éviter de redéfinir ces paramètres chaque fois que vous souhaitez créer un nouveau StyleBook, vous pouvez les définir une seule fois, puis importer leurs définitions dans les StyleBooks qui ont besoin de ces paramètres en utilisant le mécanisme **parameters-default-sources**.

Par exemple, si plusieurs de vos StyleBooks doivent configurer une IP virtuelle, vous pourriez avoir à définir les mêmes paramètres liés aux IP virtuelles dans chaque nouveau StyleBook que vous créez. Au lieu de cela, vous pouvez créer un StyleBook distinct appelé, par exemple, "vip-params", où vous définissez tous les paramètres qui y sont liés, comme indiqué dans l'exemple suivant :

```
-

name: vip-params

namespace: com.acme.commontypes

version: "1.0"

description: This StyleBook defines a typical virtual IP config.

private: true

schema-version: "1.0"

parameters:

  -

      name: lb-appname

      label: Load Balanced Application Name

     description: Name of the Load Balanced application

      type: string

      required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
       -

           name: lb-virtual-ip

           label: Load Balanced App Virtual IP address

           description: Virtual IP address representing the Load Balanced
application

           type: ipaddress

           required: true

       -

           name: lb-virtual-port

           label: Load Balanced App Virtual Port

           description: TCP port representing the Load Balanced
application

           type: tcp-port

           default: 80

       -

           name: lb-service-type

           label: Load Balanced App Protocol

           description: Protocol used for the Load Balanced application.

           type: string

           default: HTTP

           required: true

           allowed-values:

                - HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                - SSL

                - TCP
```

Ensuite, vous pouvez créer d'autres StyleBooks qui utilisent ces paramètres. Voici un exemple d'un tel StyleBook.

```
     -

     name: acme-biz-app

     namespace: com.acme.stylebooks

     version: "1.0"

     description: This stylebook defines the NetScaler configuration for
Biz App

     schema-version: "1.0"

     import-stylebooks:

       -

          namespace: com.acme.commontypes

          prefix: cmtypes

          version: "1.0"

     parameters-default-sources:

           - cmtypes::vip-params

     parameters:

         -

           name: monitorname

           label: Monitor Name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      description: Name of the monitor

      type: string

      required: true

    -

      name: type

      label: Monitor Type

      description: Type of the monitor

      type: string

      required: true

      allowed-values:

        - PING

        - TCP

        - HTTP

        - HTTP-ECV

        - TCP-ECV

        - HTTP-INLINE
```

Dans le StyleBook, acme-biz-app, tout d'abord, l'espace de noms et la version du StyleBook vip-params sont importés en utilisant la section "import-stylebooks". Ensuite, le mécanisme **parameters-default-sources** est ajouté, et le nom du StyleBook, c'est-à-dire vip-params, est spécifié. Cela a le même effet que de définir les paramètres du StyleBook vip-params directement dans ce StyleBook.

Vous pouvez inclure des paramètres de plusieurs StyleBooks car le parameters-default-sources est une liste, et chaque élément de la liste est censé être un StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

En plus d'inclure des paramètres d'autres StyleBooks, vous pouvez également définir vos propres paramètres en utilisant la section des paramètres. La liste complète des paramètres du StyleBook est la combinaison des paramètres inclus d'autres StyleBooks et des paramètres définis dans ce StyleBook. Par conséquent, l'expression **$parameters** fait référence à cette combinaison de paramètres.

Notez que si un paramètre est défini à la fois dans un StyleBook importé et dans le StyleBook actuel, la définition dans le StyleBook actuel remplace la définition importée d'un autre StyleBook. Vous pouvez utiliser cela efficacement en personnalisant quelques-uns des paramètres importés si nécessaire, tout en utilisant le reste des paramètres importés tels quels.

Le mécanisme parameters-default-sources peut également être utilisé dans les paramètres imbriqués, comme indiqué :

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true

      parameters-default-sources:

              - cmtypes::vip-params
```

C'est similaire à avoir les paramètres du StyleBook vip-params ajoutés directement en tant que paramètres enfants du paramètre vip-details dans ce StyleBook.

Construction source de paramètres

À l'aide de la construction `parameters-source`, vous pouvez contrôler la façon dont les paramètres importés apparaissent sur l'interface graphique lors de la création d'un pack de configuration. Voici un exemple de StyleBook pour décrire cette construction :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: appname

    label: "LBVserver Name"

    description: "Name of the Load Balancer"

    type: string

    required: true

  -

   parameters-source: stlb::lb

  -

    name: vip-ipaddress

    label: "Load Balancer IP Address"

    description: "IP Address of the Load Balancer VIP"

    type: ipaddress

    required: true
```

Dans cet exemple, la construction `parameters-source` est ajoutée dans la section `parameters`. Le `parameters-source` contient une valeur équivalente à un élément de liste dans la section `parameters-default-sources`. Avec `parameters-source`, vous pouvez importer des paramètres de différents StyleBooks aux positions souhaitées et les afficher sur l'interface graphique. Tandis que la section `parameters-default-sources` importe les attributs et ne s'affiche qu'au début de l'interface graphique.

Conditions de paramètre

Les conditions de paramètre sont utilisées pour modifier le comportement de certains paramètres dans la définition du StyleBook. Les paramètres d'une définition de StyleBook sont les entrées

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fournies pour créer un pack de configuration. Utilisez `parameters-conditions` pour définir une condition de paramètre dans la définition.

Un paramètre peut avoir de nombreuses contraintes dans la définition du StyleBook. Les conditions de paramètre sont utilisées pour résoudre les conflits lorsqu'un utilisateur modifie le comportement du paramètre. Par exemple, lorsqu'un utilisateur sélectionne le protocole SSL, les détails du certificat sont requis pour créer un pack de configuration. Cependant, les détails du certificat peuvent ne pas être définis comme champ obligatoire au début.

La condition de paramètre possède les attributs suivants :

- `target` : Spécifiez le paramètre cible auquel vous souhaitez appliquer une action. Vous pouvez spécifier plusieurs paramètres cibles.
- `action` : Spécifiez l'action à effectuer sur les paramètres cibles. Les conditions de paramètre prennent en charge les actions suivantes :
  - Augmenter les valeurs autorisées
  - Afficher ou masquer les paramètres
  - Définir une valeur par défaut
  - Définir comme champ obligatoire
  - Définir les valeurs autorisées
  - Définir l'étiquette du paramètre
  - Définir la description du paramètre
  - Réduire ou développer le volet du paramètre
  - Définir le modèle du paramètre
- `condition`: Facultatif, spécifiez une condition pour appliquer une action aux paramètres cibles spécifiés. Si vous ne spécifiez pas de condition, l'action est directement appliquée aux paramètres cibles.
- `value`: Définissez les valeurs de l'attribut des paramètres cibles en fonction de l'action.

REMARQUE :

Actuellement, les conditions de paramètre ne peuvent pas être appliquées aux paramètres des objets de liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'augment-allowed-values'

Lorsque l'action est `augment-allowed-values`, le paramètre cible apparaît sous forme de menu déroulant dans l'interface graphique. Le menu déroulant est défini avec les valeurs spécifiées dans l'attribut `value` de la définition du StyleBook.

Exemple :

```
parameters-conditions:

  -

   target: $parameters.rewritepolicy.action

   action: augment-allowed-values

   value:  $parameters.rewriteaction
```

'show' ou 'hide'

Lorsque l'action est `show` et que la condition spécifiée renvoie `True`, le paramètre cible apparaît dans l'interface graphique.

Lorsque l'action est `hide` et que la condition spécifiée renvoie `True`, le paramètre cible disparaît de l'interface graphique.

Exemple :

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: show

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

Au début, les détails du certificat sont masqués pour le paramètre `security-settings`. Lorsqu'un utilisateur sélectionne les protocoles SSL ou SSL-Bridge, les détails du certificat apparaissent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'set-default'

Lorsque l'action est `set-default` et que la condition spécifiée renvoie `True`, la valeur du paramètre cible est définie sur la valeur par défaut.

Exemple 1 :

```
parameters-conditions:

  -

   target: $parameters.port

   action: set-default

   condition: $parameters.protocol == "SSL"

   value: 443

  -

   target: $parameters.port

   action: set-default

   condition: $parameters.protocol != "SSL"

   value: 80
```

Exemple 2:

```
parameters-conditions:

  -

   target: $parameters.port

   action: set-default

   value: if-then-else($parameters.protocol == "SSL", 443, 80)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsqu'un utilisateur sélectionne le protocole **SSL**, la valeur de port par défaut est définie sur `443`. Pour les autres protocoles, la valeur de port par défaut est définie sur `80`. Les exemples 1 et 2 donnent le même résultat.

'set-required'

Lorsque l'action est `set-required` et que la condition spécifiée renvoie `True`, le paramètre cible devient un champ obligatoire pour créer un pack de configuration.

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: set-required

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

Au début, les détails du certificat peuvent ne pas être requis pour le paramètre `security-settings`. Lorsqu'un utilisateur sélectionne les protocoles **SSL** ou **SSL-Bridge**, les détails du certificat deviennent un champ obligatoire pour créer un pack de configuration.

'set-allowed-values'

Lorsque l'action est `set-allowed-values` et que la condition spécifiée renvoie `True`, le paramètre cible vous permet de sélectionner uniquement les valeurs spécifiées.

Exemple:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-allowed-values

   value:

    - "SSL"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   condition: $parameters.lb-virtual-port ==  443
```

Lorsqu'un utilisateur spécifie `443` comme port virtuel de l'équilibreur de charge, le nom de l'application n'autorise que l'option **SSL**.

'set-label'

Lorsque l'action est `set-label` et que la condition spécifiée renvoie `True`, l'étiquette du paramètre cible change pour le texte spécifié.

Exemple:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-label

   value: if-then-else($parameters.lb-service-type == "TCP",
"TCPApp","UDPApp")
```

Lorsqu'un utilisateur sélectionne le protocole de l'équilibreur de charge comme **TCP**, l'étiquette de l'application passe à **TCPApp**. Si l'utilisateur sélectionne une option différente, l'étiquette de l'application passe à **UDPApp**.

'set-description'

Lorsque l'action est `set-description` et que la condition spécifiée renvoie `True`, la description du paramètre cible change pour le texte spécifié. Cette description apparaît dans l'info-bulle d'un paramètre cible.

Exemple :

```
parameters-conditions:

  -

   target: $parameters.app-name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   action: set-description

   value: if-then-else($parameters.lb-service-type == "TCP", "Select a TCP
application name","Select a UDP application name")
```

Lorsqu'un utilisateur sélectionne le protocole de l'équilibreur de charge comme **TCP**, l'info-bulle de l'application affiche un texte : `Select a TCP application name`. Si l'utilisateur sélectionne une option différente, la description de l'application affiche `Select a UDP application name`.

'collapse-pane' ou 'expand-pane'

Lorsque l'action est `collapse-pane` et que la condition spécifiée renvoie `True`, le volet du paramètre cible se réduit dans l'interface graphique.

Lorsque l'action est `expand-pane` et que la condition spécifiée renvoie `True`, le volet du paramètre cible se développe dans l'interface graphique.

Exemple :

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details

    action: expand-pane

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

Au début, le volet des détails du certificat peut ne pas être développé pour le paramètre `security-settings`. Lorsqu'un utilisateur sélectionne les protocoles **SSL** ou **SSL-Bridge**, le volet des détails du certificat se développe dans l'interface graphique.

'set-pattern'

Lorsque l'action est `set-pattern` et que la condition spécifiée renvoie `True`, le champ du paramètre cible est défini sur le modèle spécifié.

Exemple :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-pattern

    value: "[a-z]+"
```

Dans cet exemple, le nom de l'application n'autorise que les caractères alphabétiques minuscules.

Conditions de paramètre imbriquées

Dans une définition StyleBook, vous pouvez spécifier une condition de paramètre au sein d'une autre condition de paramètre. Ces conditions sont appelées conditions de paramètre imbriquées et utilisent une construction de répétition pour les définir. Les conditions de paramètre imbriquées sont utiles lorsque vous souhaitez appliquer une action pour un paramètre à partir d'un autre paramètre.

Exemple :

```
parameters-conditions:

  -

    repeat: $parameters.lbvservers

    repeat-item: lbvserver

    parameters-conditions:

      -

        target: $lbvserver.port

        action: set-allowed-values

        condition: $lbvserver.protocol == "HTTPS"

        value: $parameters.ssl-ports
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, lorsque l'utilisateur sélectionne le protocole HTTPS pour un serveur virtuel d'équilibrage de charge, les valeurs de port sont renseignées dynamiquement. Et cela s'applique à chaque serveur virtuel d'équilibrage de charge de la liste.

Substitutions

Les substitutions sont utilisées pour définir des noms abrégés qui peuvent remplacer des expressions complexes dans le StyleBook, rendant ainsi le StyleBook plus lisible.

Les substitutions sont également utiles lorsque la même expression ou valeur est utilisée de manière répétée dans le StyleBook, par exemple, une valeur constante. L'utilisation d'un nom de substitution pour un paramètre vous permet de mettre à jour uniquement la valeur de substitution au lieu de mettre à jour toutes les occurrences du paramètre dans le StyleBook, ce qui pourrait être sujet aux erreurs.

Les substitutions sont également utilisées pour définir des mappages entre des valeurs.

Chaque substitution de la liste est composée d'une clé et d'une valeur. La valeur peut être une valeur simple, une expression, une fonction ou un mappage.

Dans l'exemple suivant, deux substitutions sont définies. La première est `http-port` qui peut être utilisée comme raccourci pour 8181. En utilisant une substitution, vous pouvez y faire référence dans le reste du StyleBook comme **$substitutions.http-port** au lieu de 8181.

Remplacements:

`http-port: 8181`

Vous pouvez spécifier un nom mnémonique pour un numéro de port et définir ce numéro de port à un seul endroit dans le StyleBook, quel que soit le nombre de fois où il est utilisé. Si vous souhaitez modifier le numéro de port à 8080, vous pouvez le modifier dans la section de substitution, et la modification prendra effet partout où le nom mnémonique `http-port` est utilisé.

L'exemple suivant montre comment une substitution est utilisée dans un composant.

```
components:

 -

     name: my-lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver

    properties:

        name: $parameters.name + "-lb"

        servicetype: HTTP

        ipv46: $parameters.ip

        port: **$substitutions.http-port**

        lbmethod: $parameters.lb-alg
```

Une substitution peut également être une expression complexe. L'exemple suivant montre comment deux substitutions utilisent des expressions.

```
substitutions:

  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS

  app-name: str("acme-") + $parameters.name + str("-app")
```

Une expression de substitution peut également utiliser des expressions de substitution existantes, comme le montre l'exemple suivant.

```
substitutions:

  http-port: 8181

  app-name: str("acme-") + $parameters.name + str($substitutions.http-
port) + str("-app")
```

Une autre fonctionnalité utile des substitutions est les mappages, où vous pouvez mapper des clés à des valeurs. Voici un exemple de substitution de mappage.

```
substitutions:

    secure-port:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        true: int("443")

        false: int("80")

    secure-protocol:

        true: SSL

        false: HTTP
```

L'exemple suivant montre comment utiliser les mappages secure-port et secure-protocol.

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: $substitutions.secure-protocol[$parameters.is-
secure]

          ipv46: $parameters.ip

          port: $substitutions.secure-port[$parameters.is-secure]

          lbmethod: $parameters.lb-alg
```

Cela implique que si l'utilisateur du StyleBook spécifie la valeur booléenne « true » pour le paramètre is-secure, ou sélectionne la case à cocher correspondant à ce paramètre dans l'interface graphique de NetScaler Console, la propriété `servicetype` de ce composant se voit attribuer la valeur **SSL**, et la propriété `port` se voit attribuer la valeur **443**. Cependant, si l'utilisateur spécifie « false » pour ce paramètre ou décoche la case correspondante dans l'interface graphique de NetScaler Console, `servicetype` se voit attribuer la valeur **HTTP** et le port se voit attribuer la valeur **80**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'exemple suivant montre comment utiliser les substitutions comme fonction. Une fonction de substitution peut prendre un ou plusieurs arguments. Les arguments peuvent être de type simple, par exemple, chaîne de caractères, nombre, adresse IP, booléen et d'autres types.

substitutions :

form-lb-name(nom): $nom + "-lb"

Dans cet exemple, une fonction de substitution « form-lb-name » est définie. Elle prend un argument de type chaîne de caractères appelé « name » **** et l'utilise pour créer une chaîne de caractères qui ajoute le suffixe « -lb » à la chaîne de caractères de l'argument name. Une expression utilisant cette fonction de substitution s'écrit comme suit :

`$substitutions.form-lb-name("my")`

Elle renvoie `my-lb`.

Considérez un autre exemple :

substitutions :

```
cspol-priority(priorité): 10100 - 100 &ast; $priorité
```

La substitution `cspol-priority` est une fonction qui prend un argument appelé « priority » et l'utilise pour calculer une valeur. Dans le reste du StyleBook, cette substitution est présentée comme suit :

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:

         name: $parameters.csvserver-name

         policyname: $components.cspolicy-comp.properties.policyname
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        priority: $substitutions.cspol-
priority($parameters.pool.priority)
```

Une substitution peut également être composée d'une clé et d'une valeur. La valeur peut être une valeur simple, une expression, une fonction, une carte, une liste ou un dictionnaire.

Voici un exemple de substitution appelée `slist` dont la valeur est une liste :

```
substitutions:

  slist:

    - a

    - b

    - c
```

La valeur d'une substitution peut également être un dictionnaire de paires clé-valeur, comme le montre l'exemple suivant d'une substitution appelée `sdict` ci-dessous :

```
substitutions:

  sdict:

    a: 1

    b: 2

    c: 3
```

Vous pouvez créer des attributs plus complexes en combinant les listes et les dictionnaires. Par exemple, une substitution appelée `slistofdict` renvoie une liste de paires clé-valeur.

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
```

Mais, dans l'exemple suivant, une substitution `sdictoflist` renvoie une paire clé-valeur, où la valeur elle-même est une autre liste.

```
  sdictoflist:

    a:

      - 1

      - 2

    b:

      - 3

      - 4
```

Dans les composants, ces substitutions peuvent être utilisées dans les constructions de condition, de propriétés, de répétition et de répétition-condition.

L'exemple suivant d'un composant montre comment une substitution peut être utilisée pour spécifier les propriétés :

```
    properties:

      a: $substitutions.slist

      b: $substitutions.sdict

      c: $substitutions.slistofdict
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    d: $substitutions.sdictoflist
```

Un cas d'utilisation pour définir une substitution dont la valeur est une liste ou un dictionnaire est lorsque vous configurez un serveur virtuel de commutation de contenu et plusieurs serveurs virtuels d'équilibrage de charge. Comme tous les serveurs virtuels d'équilibrage de charge liés au même serveur virtuel de commutation de contenu peuvent avoir une configuration identique, utilisez une liste et un dictionnaire de substitution pour construire la configuration afin d'éviter de répéter la même configuration pour chaque serveur virtuel d'équilibrage de charge.

L'exemple suivant montre la substitution et le composant dans les `cs-lb-mon` StyleBooks pour créer une configuration de serveur virtuel de commutation de contenu. Lors de la construction des propriétés des `cs-lb-mon` StyleBooks, la substitution complexe "lb-properties" spécifie les propriétés des serveurs virtuels d'équilibrage de charge associés au serveur virtuel de commutation de contenu. La substitution "lb-properties" est une fonction qui prend le nom, le type de service, l'adresse IP virtuelle, le port et les serveurs comme paramètres et génère une paire clé-valeur comme valeur. Dans le composant `cs-pools`, vous pouvez attribuer la valeur de cette substitution au paramètre `lb-pool` pour chaque pool.

```
substitutions:

  cs-port[]:

    true: int("80")

    false: int("443")

  lb-properties(name, servicetype, vip, port, servers):

    lb-appname: $name

    lb-service-type: $servicetype

    lb-virtual-ip: $vip

    lb-virtual-port: $port

    svc-servers: $servers

    svc-service-type: $servicetype
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    monitors:

      -

        monitorname: $name

        type: PING

        interval: $parameters.monitor-interval

        interval_units: SEC

        retries: 3

components:

  -

    name: cs-pools

    type: stlb::cs-lb-mon

    description: | Updates the cs-lb-mon configuration with the different
pools provided. Each pool with rule result in a dummy LB vserver, cs
action, cs policy, and csvserver_cspolicy_binding configuration.

    condition: $parameters.server-pools

    repeat: $parameters.server-pools

    repeat-item: pool

    repeat-condition: $pool.rule

    repeat-index: ndx

    properties:

      appname: $parameters.appname + "-cs"

      cs-virtual-ip: $parameters.vip

      cs-virtual-port: $substitutions.cs-port($parameters.protocol ==
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"HTTP")

      cs-service-type: $parameters.protocol

      pools:

        -

          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP",
"0.0.0.0", 0, $pool.servers)

          rule: $pool.rule

          priority: $ndx + 1
```

Mappage de substitution

Vous pouvez créer des substitutions qui mappent des clés à des valeurs. Par exemple, considérez un scénario où vous souhaitez définir le port par défaut (valeur) à utiliser pour chaque protocole (clé). Pour cette tâche, écrivez un mappage de substitution comme suit.

```
substitutions:

     port:

          HTTP: 80

          DNS: 53

          SSL: 443
```

Dans cet exemple, HTTP est mappé à 80, DNS est mappé à 53 et SSL est mappé à 443. Pour récupérer le port d'un certain protocole donné en tant que paramètre, utilisez l'expression

$substitutions.port\[$parameters.protocol\]

L'expression renvoie une valeur basée sur le protocole spécifié par l'utilisateur.

- Si la clé est HTTP, l'expression renvoie 80
- Si la clé est DNS, l'expression renvoie 53
- Si la clé est SSL, l'expression renvoie 443

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Si la clé n'est pas présente dans le mappage, l'expression ne renvoie aucune valeur

Itérer à travers les listes de substitution

Dans l'exemple suivant, le StyleBook itère à travers une liste de substitution appelée `apps` pour créer un ensemble de composants `lbvserver` et leurs groupes de services correspondants et serveurs liés.

```
substitutions:

  apps:

    -

      name: lb1

      vip: 1.2.3.4

      vport: 80

      protocol: HTTP

      servers:

        -

          ip: 10.8.11.11

          port: 8080

        -

          ip: 10.8.11.12

          port: 8080

    -

      name: lb2

      vip: 1.2.3.5

      vport: 81
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      protocol: HTTP
      servers:
        -
          ip: 10.9.11.28
          port: 8080
        -
          ip: 10.9.11.29
          port: 8181
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    repeat: $substitutions.apps
    repeat-item: app
    properties:
      name: $app["name"]
      ipv46: $app["vip"]
      port: $app["vport"]
      servicetype: $app["protocol"]
    components:
      -
        name: servicegroup-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        type: ns::servicegroup
        properties:
          servicegroupname: $parent.properties.name + "-svg"
          servicetype: HTTP
        components:
          -
            name: servers-comp
            type: ns::server
            repeat: $app["servers"]
            repeat-item: server
            properties:
              name: $server["ip"]
              ipaddress: $server["ip"]
            components:
              -
                name: servicegroup-servicegroupmember-binding-comp
                type: ns::servicegroup_servicegroupmember_binding
                properties:
                  servicegroupname:
$parent.parent.properties.servicegroupname
                  servername: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                port: $server["port"]
```

Composants

La construction Components dans un StyleBook est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration qui doivent être créés. À l'aide de cette construction, vous pouvez créer un ou plusieurs objets de configuration du même type.

La construction de composants peut utiliser l'entrée fournie dans la section des paramètres pour adapter la configuration générée par le StyleBook. Il s'agit d'une section facultative, bien que la plupart des StyleBooks aient une section de composants.

Le tableau suivant décrit les principaux attributs d'un composant.

ATTRIBUT	DESCRIPTION
nom	Le nom du composant. Vous pouvez spécifier un nom alphanumérique. Le nom doit commencer par une lettre et peut inclure des lettres supplémentaires, des chiffres, un trait d'union (-) ou un trait de soulignement (_).
Description	Une description du rôle de ce composant dans le StyleBook.
Type	Le type détermine les propriétés que ce composant fournit. Les composants ont deux types de types : **Type intégré** : Ce type est fourni par le système et vous n'avez pas à le définir, par exemple, les types d'entités NITRO « lbvserver » ou « servicegroup ». Lorsqu'un composant a un attribut de type intégré, il crée un objet de configuration de ce type sur le NetScaler. Par exemple, si un composant fait référence au type intégré « lbvserver », ce composant crée un serveur virtuel d'équilibrage de charge sur l'instance NetScaler qui est la cible de la configuration. **Type composite** : Ce type fait référence à un StyleBook existant que vous avez créé et

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	DESCRIPTION
	importé dans NetScaler Console. Lorsqu'un composant a un attribut de type composite, il crée tous les objets de configuration, qui sont spécifiés dans le StyleBook référencé, sur l'instance NetScaler qui est la cible de la configuration. Cela vous permet de combiner plusieurs StyleBooks où chaque StyleBook crée une partie de la configuration finale. Pour plus d'informations sur les StyleBooks composites, voir Créer un StyleBook composite.
propriétés	Les sous-attributs qui peuvent être utilisés pour un attribut de type de composant. Les propriétés valides pour un composant sont dictées par son type. Pour un type intégré, ce sont les propriétés ou attributs de l'objet Nitro correspondant. Pour un composant dont le type est un autre StyleBook, c'est-à-dire un type composite, les propriétés correspondent aux paramètres définis dans ce StyleBook.

Exemple :

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        port: 80

        lbmethod: $parameters.lb-alg
```

Dans cet exemple, vous avez défini un composant appelé my-lbvserver-comp. Ce composant est de type ns::lbvserver (un type intégré), où « ns » est le préfixe qui fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5 que vous aviez spécifiée dans la section import-stylebooks, et « lbvserver » est une ressource NITRO dans cet espace de noms.

Les propriétés de cette section incluent quatre attributs obligatoires et un attribut facultatif (lbmethod) de la ressource « lbvserver » et vous permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour servicetype et port, tandis que les propriétés name, ipv46 et lbmethod obtiennent leurs valeurs des paramètres d'entrée. Vous faites référence aux noms de paramètres définis dans la section des paramètres en utilisant la notation $parameters.\<name\>, par exemple, $parameters.ip.

REMARQUE

Vous devez utiliser des minuscules pour les noms d'attributs des types de ressources NITRO (ses propriétés de composant). Sinon, l'importation d'un StyleBook échouera.

Composants d'aide

L'utilisation principale de la section des composants dans un StyleBook est de générer des objets de configuration via les types intégrés Nitro ou un autre StyleBook qui crée les objets de configuration réels. Les composants d'aide ne construisent pas d'objets de configuration par eux-mêmes. Les composants d'aide prennent les entrées d'autres sections, telles que les objets de paramètre, les propriétés d'autres composants ou les sorties d'autres composants, et les transforment sous d'autres formes. Celles-ci peuvent ensuite être utilisées par d'autres composants pour générer les objets de configuration réels. Un composant d'aide peut être de deux types : un type d'objet ou un autre StyleBook qui ne contient pas de section de composant.

L'exemple suivant montre un extrait d'un StyleBook utilisé pour créer un serveur d'équilibrage de charge avec moniteur (lb-mon-comp) sur une instance NetScaler.

```
parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    name: appname

    type: string

  -

    name: ips

    type: ipaddress[]

  -

    name: vip

    type: ipaddress



components:

  -

    name: help-comp

    type: cmtypes::server-ip-port-params

    repeat:

      repeat-list: $parameters.ips

      repeat-item: server-ip

    properties:

      ip: $server-ip

      port: 80

 -

    name: lb-mon-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: stlb::lb-mon

    properties:

      lb-appname: $parameters.appname

      lb-virtual-ip: $parameters.vip

      lb-virtual-port: 80

      lb-service-type: HTTP

      svc-service-type: HTTP

      svc-servers: $components.help-comp.properties
```

La section des paramètres vous permet de saisir le nom de l'application et les adresses IP des serveurs d'équilibrage de charge. Dans la section du composant lb-mon-comp, le paramètre svc-servers du StyleBook lb-mon attend une liste d'objets où chaque élément a deux sous-paramètres : ip et port.

Cependant, la section des paramètres de ce StyleBook n'accepte que les adresses IP des serveurs via $parameters.ips. Le StyleBook suppose que tous les serveurs fonctionnent sur le port 80. Pour créer la configuration d'équilibrage de charge à l'aide du StyleBook lb-mon, vous devez transformer les $parameters.ips en une liste d'objets. Ceci est réalisé à l'aide du composant d'aide, help-comp, dans l'exemple ci-dessus. Le composant help-comp est de type StyleBook server-ip-port-params. Ce StyleBook n'a pas de composants. Par conséquent, il ne crée aucun objet de configuration. Le help-comp crée une liste répétée sur $parameters.ips et construit un objet qui se compose d'une adresse IP et d'un port (qui est défini sur un port statique 80) pour chaque élément de $parameters.ips. Ainsi, help-comp transforme une liste d'adresses IP en une liste d'objets qui peuvent être utilisés ultérieurement dans lb-mon-comp pour attribuer la propriété svc-servers. Le résultat du help-comp est attribué à la propriété svc-servers de lb-mon-comp.

Propriétés facultatives

Dans certains cas, une propriété d’un composant prend sa valeur à partir d’une expression, qui peut être une expression simple telle qu’une référence de paramètre, ou une expression plus complexe. La définition de cette valeur de propriété est facultative dans le composant. Vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pouvez choisir de définir la valeur de la propriété uniquement si l'expression renvoie une valeur réelle, sinon vous pouvez choisir de ne pas définir cette propriété.

Par exemple, considérons que l'une des propriétés que vous souhaitez définir est la méthode lbmethod (algorithme d'équilibrage de charge) d'un composant dont le type est ns::lbvserver. La valeur de la propriété lbmethod est tirée d'une valeur de paramètre fournie par l'utilisateur, comme indiqué ci-dessous :

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod: $parameters.lb-advanced.algorithm
```

Considérons maintenant que le paramètre **lb-advanced.algorithm** est un paramètre facultatif. Et, si l'utilisateur ne fournit pas de valeur pour ce paramètre parce qu'il est facultatif, l'expression **$parameters.lb-advanced.algorithm** évalue à une valeur vide. Par conséquent, une valeur non valide est transmise pour la propriété lbmethod. Afin d'éviter une telle situation, vous pouvez annoter la propriété comme facultative en suffixant son nom avec « ? » comme suit :

```
components
   -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
      lbmethod?: $parameters.lb-advanced.algorithm
```

L'utilisation de « ? » omet la propriété si l'expression de droite n'évalue à rien, ce qui équivaudrait, dans ce cas, à un composant défini comme suit :

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
```

Étant donné que **lbmethod** est facultatif, l'omettre en fait toujours un composant valide. Notez que lbmethod peut prendre sa valeur par défaut si une est définie dans son type « ns::lbvserver ».

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le construct properties-default-sources

Le construct properties-default-sources est analogue au construct parameters-default-sources. Alors que le construct parameters-default-sources permet la réutilisation de paramètres existants (provenant d'autres StyleBooks) dans un StyleBook, le construct properties-default-sources permet à l'utilisateur de spécifier les propriétés d'un composant en fonction de sources existantes.

Les propriétés d'un composant peuvent être réparties dans différentes sections du StyleBook. Par exemple, les propriétés peuvent provenir de paramètres d'objet, de substitutions qui renvoient un objet, de propriétés d'autres composants ou de sorties d'autres composants. Dans de tels cas, vous devez redéfinir les propriétés qui apparaissent dans d'autres sections du StyleBook dans la définition du composant. Clairement, cela est redondant et peut entraîner des erreurs. Pour résoudre ce problème, le construct properties-default-sources peut être utilisé. Le construct properties-default-sources est une liste où chaque élément identifie une source pour certaines propriétés du composant.

Par exemple, considérons un composant qui crée une configuration lbvserver. Ce composant doit définir les propriétés du lbvserver comme suit.

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb.name

      ipv46: $parameters.lb.ipv46

      port: $parameters.lb.port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: $parameters.lb.servicetype

      lbmethod: $parameters.lb.lbmethod
```

Dans l'exemple ci-dessus, observez que les valeurs de toutes les propriétés définies dans la section des composants sont tirées de l'objet $parameters.lb. Bien qu'elles proviennent d'une seule source, les propriétés sont à nouveau définies dans le StyleBook. De plus, si un nouveau sous-paramètre à l'objet $parameters.lb, pertinent pour la configuration du lbvserver, est ajouté, vous devez mettre à jour le composant lb-comp pour ajouter la nouvelle propriété qui correspond au nouveau sous-paramètre.

Pour éviter de redéfinir les propriétés et de récupérer toutes les propriétés pertinentes d'un composant sans les lister explicitement dans la section des propriétés, le construct properties-default-sources peut être utilisé. L'exemple ci-dessus peut être écrit comme suit.

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties-default-sources:

      - $parameters.lb
```

Dans l'exemple ci-dessus, l'utilisation du construct properties-default-sources entraîne une réduction de la taille de la définition du composant, ce qui vous permet de définir un composant de manière concise. De plus, chaque fois que la source des propriétés du composant change, les modifications sont automatiquement répercutées. Par exemple, lorsqu'une nouvelle propriété, telle que « persistencetype », est ajoutée à l'objet $parameters.lb, cette propriété est ajoutée par défaut

© 1997–2026 Citrix Systems, Inc. All rights reserved.

à la configuration de lb-comp, car persistencetype est une propriété de lbvserver. Ainsi, le construct properties-default-sources fournit une interface dynamique pour définir les composants sans se soucier des modifications apportées aux sources des propriétés du composant.

Calcul des propriétés du composant

Cette section explique comment les propriétés sont récupérées si le construct properties-default-sources est utilisé dans un composant. Premièrement, le compilateur StyleBooks identifie la liste des propriétés d'un composant en fonction de son type (dans l'exemple ci-dessus, lbvserver). Ensuite, le compilateur récupère ces propriétés à partir des multiples sources dans l'ordre où elles sont définies (dans la section properties-default-sources du composant). Si une propriété existe dans plusieurs sources, la propriété apparaissant dans la dernière source a priorité sur les autres. Enfin, une propriété récupérée à l'aide du construct properties-default-sources peut être remplacée dans la section des propriétés du composant. Il est important de noter que la définition d'une section de composant doit au moins avoir une section properties-default-sources ou une section de propriétés. Elle peut avoir les deux.

Composants imbriqués

L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer ses objets de configuration en se référant aux objets de configuration ou au contexte créé par le composant parent. Le composant imbriqué peut créer un ou plusieurs objets pour chaque objet créé dans le composant parent. L'imbrication d'un composant dans un autre composant n'indique aucune relation entre les objets de configuration créés. L'imbrication est un moyen de faciliter la tâche des composants pour construire des objets de configuration dans un contexte existant des composants parents.

Exemple :

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: $parameters.name + "-lb"

servicetype: HTTP

ipv46: $parameters.ip

port: 80

lbmethod: $parameters.lb-alg

components:

  -

   name: my-svcg-comp

   type: ns::servicegroup

   properties:

      name: $parameters.name + "-svcgrp"

      servicetype: HTTP

   components:

      -

        name: lbvserver-svg-binding-comp

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parent.parent.properties.name

          servicegroupname: $parent.properties.name

            -

              name: members-svcg-comp

              type: ns::servicegroup_servicegroupmember_binding
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                repeat:
                  repeat-list: $parameters.svc-servers
                  repeat-item: srv
                properties:
                  ip: $srv
                  port: str($parameters.svc-port)
                  servicegroupname: $parent.properties.name
```

Dans cet exemple, une imbrication à plusieurs niveaux est utilisée. Le composant my-lbvserver-comp possède un composant enfant appelé my-svcg-comp. Et le composant my-svcg-comp contient deux composants enfants. Le composant my-svcg-comp est utilisé pour créer un objet de configuration de groupe de services sur l'instance NetScaler en fournissant des valeurs aux attributs du type de ressource NITRO intégré "servicegroup". Le premier composant enfant du composant my-svcg, lbvserver-svg-binding-comp, est utilisé pour lier le groupe de services créé par son composant parent au serveur virtuel d'équilibrage de charge (lbvserver) créé par le composant parent du parent. La notation $parent, également appelée référence parent, est utilisée pour faire référence aux entités dans les composants parents. Le deuxième composant enfant, members-svcg-comp, est utilisé pour lier la liste des services au groupe de services créé par le composant parent. La liaison est réalisée en utilisant la construction de répétition de StyleBook pour itérer sur la liste des services spécifiés pour le paramètre svc-servers. Pour plus d'informations sur les constructions de répétition, consultez Construction de répétition.

Vous pouvez également créer les mêmes objets de configuration sans utiliser l'imbrication de composants. Pour plus d'informations et d'exemples, consultez StyleBook pour créer une configuration d'équilibrage de charge de base.

Construction de condition

Vous pouvez rendre un composant conditionnel en utilisant une construction de condition. La valeur d'une construction conditionnelle est une expression booléenne qui est évaluée à vrai ou faux. Si la condition est vraie, le composant est utilisé pour construire ses objets de configuration. Si la condition est fausse, le composant est ignoré et aucun objet de configuration n'est créé par son intermédiaire. L'expression booléenne est souvent basée sur les valeurs des paramètres.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple :

```
components:

      -

        name: servicegroup-comp

        type: ns::servicegroup

        condition: $parameters.svc-server-ips

        properties:

              name: $parameters.name + "-svcgrp"

              servicetype: HTTP
```

Dans cet exemple, si l'utilisateur spécifie une valeur pour le paramètre facultatif svc-server-ips, alors le composant, servicegroup-comp, est traité par le moteur StyleBook. Si la condition est fausse, c'est-à-dire si l'utilisateur ne fournit pas de valeur à ce paramètre, une valeur nulle est attribuée à ce paramètre et est évaluée à faux, alors le moteur StyleBook ignore la présence de ce composant, et aucun servicegroup n'est créé.

Notez que l'expression booléenne peut être basée sur toute expression valide prise en charge dans les StyleBooks (par exemple, si un autre composant est présent, ou si un paramètre a une certaine valeur).

L'exemple suivant construit l'objet de configuration de type NITRO ns::systemfile si la condition est évaluée à vrai.

Exemple :

```
     components

          -

            name: pem_key_files

            type: ns::systemfile

            condition: "$components.der-certificate-files-comp or
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$components.pem-certificate-files-comp"

            properties:

                  filecontent: $certificate.keyfile.contents

                  fileencoding: "BASE64"

                  filelocation: "/nsconfig/ssl"

                  filename: $certificate.keyfile.filename
```

Dans cet exemple, la condition est une expression "OU" complexe, où vous souhaitez que cet objet de configuration soit créé par le StyleBook uniquement si deux autres composants du StyleBook ont été traités (non ignorés), créant ainsi une dépendance entre les composants.

Structure de répétition

Vous pouvez utiliser la construction **repeat** d'un composant pour créer plusieurs objets de configuration du même type.

Dans l'exemple suivant, le composant **members-svcg-comp** est utilisé pour lier la liste des services au groupe de services créé par le composant parent. Afin de créer un objet de configuration qui lie chaque serveur au groupe de services, utilisez la construction **repeat** pour itérer sur la liste des services spécifiés pour le paramètre **svc-servers**. Pendant l'itération, le composant crée un objet NITRO de type **servicegroup_servicegroupmember_binding** pour chaque service (appelé **srv** dans la construction **repeat-item**) dans le groupe de services, et il définit l'attribut **ip** dans chaque objet NITRO sur l'adresse IP du service correspondant.

Exemple :

```
components:

  -

      name: my-lbvserver-comp

      type: ns::lbvserver

      properties:

           name: $parameters.name + "-lb"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        servicetype: HTTP
        ipv46: $parameters.ip
        port: 80
        lbmethod: $parameters.lb-alg
      components:
            -
              name: my-svcg-comp
              type: ns::servicegroup
              properties:
                  name: $parameters.name + "-svcgrp"
                  servicetype: HTTP
             components:
                   -
                   name: lbvserver-svg-binding-comp
                   type: ns::lbvserver\servicegroup\binding
                   properties:
                         name: $parent.parent.properties.name
                         servicegroupname: $parent.properties.name
                   -
                   name: members-svcg-comp
                   type: ns::servicegroup\servicegroupmember\binding
                   repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        repeat-list: $parameters.svc-servers

                        repeat-item: srv

                    properties:

                          ip: $srv

                          port: $parameters.svc-port

                          servicegroupname: $parent.properties.name
```

Le **repeat** est un objet en soi, et **repeat-list** et **repeat-item** sont des attributs pour l'objet repeat.

- repeat-list est un attribut obligatoire qui identifie la liste sur laquelle le composant itère.
- repeat-item est facultatif et est utilisé pour donner un nom convivial à l'élément actuel dans l'itération.

S'il n'est pas spécifié, l'élément actuel peut être accédé à l'aide de l'expression **$repeat-item**. Le dernier composant de l'exemple ci-dessus peut également être écrit comme suit :

```
        -

        name: members-svcg-comp

        type: ns::servicegroup_servicegroupmember_binding

        repeat:

          repeat-list: $parameters.svc-servers

        properties:

               ip: $repeat-item

               port: $parameters.svc-port

               servicegroupname: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

En plus de pouvoir faire référence à l'élément actuel lors de l'itération sur une liste, il est également possible de faire référence à l'index actuel de l'élément dans la liste en utilisant **repeat-index**. Dans l'exemple suivant, **repeat-index** est utilisé pour calculer un numéro de port basé sur l'index actuel :

```
            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + repeat-index

                servicegroupname: $parent.properties.name
```

Similaire à la construction **repeat-item**, vous pouvez attribuer un nom de variable différent pour faire référence à l'index actuel de l'itération. L'exemple précédent est équivalent à l'exemple suivant :

```
    -

            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

               repeat-index: idx

            properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                ip: $parameters.app-ip

                port: $parameters.base-port + $idx

                servicegroupname: $parent.properties.name
```

Construction de condition de répétition

La construction de condition de répétition est évaluée à chaque itération d'une construction de répétition et le résultat détermine s'il faut créer l'objet de configuration dans cette itération ou passer à l'itération suivante. L'exemple suivant montre l'utilisation de la construction de condition de répétition :

Exemple :

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

         filecontent: base64($certificate.keyfile.contents)

         fileencoding: BASE64

         filelocation: /nsconfig/ssl

         filename: $certificate.keyfile.file
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, le composant der-key-files-comp itère sur tous les certificats fournis par l'utilisateur, mais il ne crée des objets de configuration que pour les certificats avec encodage DER. À chaque itération, l'expression de condition de répétition est évaluée pour vérifier si l'encodage du certificat est de type DER. S'il n'est pas de type DER, aucun objet de configuration n'est créé dans l'itération actuelle, et l'itération passe au certificat suivant dans la liste.

Répétitions imbriquées

Avec la construction de répétition imbriquée, vous pouvez avoir plus d'une construction de répétition dans chaque composant, selon la définition du composant. Considérez une répétition imbriquée de deux niveaux. Pour chaque élément de la liste externe (première liste de répétition), vous pouvez créer une liste de répétition pour tous les éléments de la liste interne (deuxième liste de répétition). Le compilateur StyleBook prend en charge jusqu'à trois répétitions imbriquées. Chaque niveau de répétition possède des attributs repeat-item et repeat-index associés. Les attributs repeat-item et repeat-index sont tous deux facultatifs. De plus, chaque répétition peut également spécifier une condition de répétition (repeat-condition).

Exemple:

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
  -
      name: lbvservers-comp
      type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
repeat:
   repeat-list: $parameters.vips
   repeat-item: ip
   repeat:
        repeat-list: $parameters.vip-ports
        repeat-item: port
properties:
   name: str("lb-") + str($ip) + '-' + str($port)
   servicetype: HTTP
   ipv46: $ip
   port: $port
```

Dans l'exemple ci-dessus, pour chaque élément de $parameters.vips, nous itérons sur tous les éléments de $parameters.vip-ports. Ainsi, pour chaque adresse IP spécifiée dans $parameters.vips, nous créons des objets de configuration lbvserver pour tous les ports spécifiés dans $parameters.vip-ports. La section des propriétés définit le nom de l'objet avec « lb » comme préfixe pour la combinaison de l'adresse IP et du port. Par conséquent, pour chaque itération, $ip + $port définit une combinaison unique de l'adresse IP et du numéro de port.

Si l'attribut repeat-item n'est pas fourni, le compilateur génère une valeur par défaut pour celui-ci. Les valeurs par défaut pour repeat-item sont : $repeat-item, $repeat-item-1, $repeat-item-2 respectivement pour chaque niveau de répétition. De même, si l'attribut repeat-index n'est pas fourni, le compilateur génère une valeur par défaut pour celui-ci. Les valeurs par défaut pour repeat-index sont : $repeat-index, $repeat-index-1 et $repeat-index-2 respectivement pour chaque niveau de répétition.

L'exemple suivant décrit la convention de dénomination en l'absence d'attributs repeat-item et repeat-index dans un objet de répétition imbriquée.

Exemple:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

-

     name: lbvservers-comp

     type: ns::lbvserver

     repeat:

         repeat-list: $parameters.vips

         repeat:

            repeat-list: $parameters.vip-ports

     properties:

        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)

        servicetype: HTTP

        ipv46: $repeat-item

        port: $repeat-item-1
```

Sorties

Dans la section des sorties, vous spécifiez ce qu'un StyleBook expose à ses utilisateurs après avoir terminé la création de tous les objets de configuration avec succès. La section des sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer de sorties. Cependant, en renvoyant certains composants internes comme sorties, il offre plus de flexibilité à tout StyleBook qui l'importe, comme vous pouvez le constater lors de la création d'un StyleBook composite.

Le tableau suivant décrit les attributs utilisés dans la section des sorties.

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
nom	Le nom de la sortie correspondant à l'objet de	Oui

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
	configuration que vous souhaitez exposer.	
Description	Une chaîne de texte décrivant la sortie.	Non
valeur	Cet attribut spécifie comment extraire la valeur renvoyée par un StyleBook.	Oui

Exemple :

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
```

Dans cet exemple, vous exposez le composant **lbvserver** et le **nom** du groupe de services qui seraient créés par le StyleBook. La valeur de la sortie appelée **lbvserver** est le composant **my-lbvserver-comp**. De même, la valeur de la sortie appelée **svc-grp** est le nom du groupe de services créé par le composant **my-svcg**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Référence des paramètres

Dans la construction des composants, vous faites référence aux paramètres définis dans la section des paramètres en utilisant la notation `$parameters.<parametername>`. Si `<parametername>` contient lui-même des paramètres (lorsque le type est un objet), vous devez alors utiliser la notation `$parameters.<parametername>.<sub-parametername>`, et ainsi de suite.

Exemple :

```
parameters:

  -

    name: name

    label: Name

    type: string

    required: true

     -

      name: vip

      label: Virtual IP and Port

      type: object

      required: true

      parameters:

        -

          name: ip

          label: Virtual IP

          description: The Virtual IP Address

          type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
```

Référence parent

Si vous utilisez des composants imbriqués, vous pouvez faire référence au composant parent en utilisant la notation $parent. Si le composant parent construit plusieurs objets de configuration à l'aide du mécanisme de répétition, et que, dans chaque itération, les composants enfants construisent d'autres objets de configuration, alors la notation $parent fait toujours référence à l'itération actuelle du composant parent. Par exemple, $parent.properties.name fait référence à la propriété name de l'objet de configuration construit dans l'itération actuelle par le parent.

Exemple:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
     ipv46: $parameters.ip
     port: 80
     lbmethod: $parameters.lb-alg
     components:
       -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
           name: $parameters.name + "-svcgrp"
           servicetype: HTTP
           components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                name: $parent.parent.properties.name

                servicegroupname: $parent.properties.name

                  -

                    name: members-svcg-comp

                    type: ns::servicegroup_servicegroupmember_binding

                    repeat: $parameters.svc-servers

                    repeat-item: srv

                    properties:

                      ip: $srv

                      port: str($parameters.svc-port)

                      servicegroupname: $parent.properties.name
```

Vous pouvez également naviguer vers le haut dans la hiérarchie des composants en accédant aux propriétés des parents des parents jusqu'aux composants de niveau supérieur. Par exemple, la propriété name du composant **lbvserver-svg-binding-comp** prend sa valeur de la propriété name du parent de son parent, le composant **my-lbvserver-comp**, en utilisant la notation **$parent.parent**.

Référence des composants

Dans la construction des composants, vous faites référence au composant de niveau supérieur dans le StyleBook en utilisant la notation **$components.\<componentname\>**. S'il y a des composants imbriqués dans un composant de niveau supérieur, alors la notation utilisée est **$components.\<componentname\>.components.\<component-name\>** pour y faire référence, et ainsi de suite.

Exemple :

```
components:

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: 80
          lbmethod: $parameters.lb-alg
 -
    name: my-svcg-comp
    type: ns::servicegroup
    properties:
         name: $parameters.name + "-svcgrp"
         servicetype: HTTP
-
    name: members-svcg-comp
    type: ns::servicegroup_servicegroupmember_binding
    repeat: $parameters.svc-servers
    repeat-item: srv
    properties:
       ip: $srv
         port: str($parameters.svc-port)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          servicegroupname: $components.my-svcg-comp.properties.name

-

    name: lbvserver-svg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    properties:

           name: $components.my-lbvserver-comp.properties.name

           servicegroupname: $components.my-svcg-comp.properties.name
```

Dans cet exemple, les composants **my-svcg-comp** et **my-lbvserver-comp** doivent être construits avant de construire le dernier composant **lbvserver-svg-binding-comp**, car il y a des références à ces composants dans ce dernier composant. Ces références sont fournies en utilisant les références de composants désignées par **$components.\<componentname\>**.

Référence des substitutions

Dans la section des composants ou la section des opérations, vous faites référence aux substitutions définies dans la section des substitutions en utilisant la notation `$substitutions.<substitution-name>`. Par exemple, **$substitutions.http-port**.

Si une substitution est une carte, vous pouvez faire référence à un élément de la carte en tant que `$substitutions.<substitutions-name>[<map-key>]`. Par exemple, `$substitutions.protocol-map[$parameters.port]`.

Référence de variable

Lorsque vous utilisez les constructions repeat et repeat-item dans des composants pour créer plusieurs objets de configuration, vous pouvez attribuer un nom de variable à la construction repeat-item. Cette variable peut ensuite être référencée dans les propriétés de ce composant ou dans les composants enfants en utilisant la notation `$\<varname\>`. Notez que lorsque la construction repeat est utilisée sans la construction repeat-item dans un composant, une variable par défaut appelée $repeat-item peut être utilisée pour accéder aux éléments d'itération.

Exemple :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names

    repeat: $parameters.svc-server-domain-names

    repeat-item: server-name

    properties:

      name: $server-name + "-server"

      domain: $server-name

    components:

      -

         name: service-members-comp

         type: ns::service

         properties:

           name: $server-name + "-service"

           servername: $parent.properties.name

           servicetype: $parameters.svc-service-type

           port: $parameters.svc-server-port
```

Dans l'exemple ci-dessus, un nom de variable, server-name, est attribué à la construction repeat-item. Ce nom de variable est référencé dans les propriétés du même composant ainsi que dans les composants enfants **`$\<varname\>`**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Opérations

La section Opérations est facultative dans un StyleBook. Dans cette section, vous pouvez configurer l'analyse de NetScaler Console pour collecter les enregistrements AppFlow sur tout ou partie des transactions de trafic. Le serveur virtuel créé sur une instance NetScaler à l'aide du StyleBook gère ces transactions de trafic. Dans cette section, vous pouvez également configurer NetScaler Console pour déclencher des alarmes lorsque certaines conditions de trafic sont remplies sur un serveur virtuel.

Vous pouvez configurer NetScaler Console via les StyleBooks pour collecter des statistiques de trafic à partir de divers NetScaler Console Insights, qui sont les suivants :

- Web Insight
- Violations de sécurité WAF
- HDX™ Insight
- NetScaler Gateway Insight.

Les serveurs virtuels pris en charge sont l'équilibrage de charge, la commutation de contenu et les serveurs virtuels VPN.

Activez Web Insight et les violations de sécurité WAF, ou l'un d'entre eux, pour l'analyse sur un serveur virtuel d'équilibrage de charge ou de commutation de contenu. Pour les serveurs virtuels VPN, cependant, vous devez activer HDX Insight et NetScaler Gateway Insight, ou l'un d'entre eux.

Tout NetScaler Console Insight activé sur les instances NetScaler via les StyleBooks utilise le protocole IPFIX (AppFlow) pour envoyer les données des instances à NetScaler.

De plus, lorsque vous activez Web Insight, les mesures côté client sont activées sur les serveurs virtuels d'équilibrage de charge et de commutation de contenu. Avec les mesures côté client activées, NetScaler Console capture les métriques de temps de chargement et de temps de rendu pour les pages HTML, via l'injection HTML. À l'aide de ces métriques, les administrateurs peuvent identifier les problèmes de latence L7.

Exemple 1 :

L'exemple suivant montre comment rédiger la section des opérations dans un StyleBook pour activer HDX Insight et NetScaler Gateway Insight sur un serveur virtuel VPN :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: simple-vpn-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable hdxinsight and gatewayinsight on a
VPN vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

components:

    -

        name: vpnvserver-comp

        type: ns::vpnvserver

        properties:

            name: str("vpn-") + str($current-target.ip)

            servicetype: SSL

            ipv46: 1.1.21.37

            port: 443

operations:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    analytics:

        -

            name: comp-ops

            properties:

                target: $components.vpnvserver-comp

                filter: "true"

                insights:

                  -

                 type: hdxinsight**

                  -

                    type: gatewayinsight

outputs:

  -

    name: myvpns

    value: $components.vpnvserver-comp
```

Exemple 2 :

L'exemple suivant montre comment rédiger la section des opérations dans un StyleBook pour activer Web Insight et les violations de sécurité WAF sur un serveur virtuel d'équilibrage de charge :

```


name: simple-lb-ops

namespace: com.example.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable webinsight and securityinsight on LB
vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:

            name: str("lb-") + str($current-target.ip)

            servicetype: HTTP

            ipv46: 1.1.21.37

            port: 80

operations:

    analytics:

        -

            name: comp-ops
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            properties:

                target: $components.lbvserver-comp

                filter: "true"

                 insights:

                 -

                  type: webinsight

                    -

                  type: securityinsight

outputs:

  -

    name: mylbs

    value: $components.lbvserver-comp
```

Analyse

Chaque élément de la section d'analyse est utilisé pour configurer la fonctionnalité d'analyse de NetScaler Console pour un ou plusieurs serveurs virtuels créés dans StyleBooks.

Un élément de la section d'analyse possède les attributs suivants :

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
nom	Nom de l'élément d'analyse.	Oui
Détails	Une chaîne de texte décrivant cet élément.	Non
Critère	Une expression booléenne. Lorsque cette condition est évaluée à faux, l'intégralité de	Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
	l'élément d'analyse est ignorée.	
répéter	Itère sur une liste.	Non
condition-de-répétition	Une expression booléenne. Si l'expression est évaluée à faux, l'itération actuelle est ignorée.	Non
élément-de-répétition	Nom de l'élément dans l'itération actuelle.	Non
index-de-répétition	Nom de la valeur d'index de l'itération actuelle.	Non
propriétés	Une liste de propriétés d'opération d'analyse.	Oui
cible	L'une des propriétés de la liste. L'expression cible est le nom d'un serveur virtuel, configuré sur le NetScaler, pour lequel les analyses sont collectées.	Oui
filtre	L'une des propriétés de la liste. La valeur de cet attribut est une expression de stratégie avancée NetScaler utilisée pour filtrer les requêtes sur le serveur virtuel pour lequel les analyses sont collectées. Par défaut, les données d'analyse sont collectées sur tout le trafic passant par le serveur virtuel.	Non
aperçus	L'une des propriétés de la liste. La valeur de cet attribut est le type de données d'insights à collecter à partir	Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
	du serveur virtuel cible. Par défaut, tous les insights autorisés sont configurés sur les serveurs virtuels cibles en fonction du type de serveur virtuel, comme spécifié dans Serveurs virtuels cibles et types d'insights.	
mode-de-transport	L'une des propriétés de la liste. La valeur de cet attribut est soit `logstream`, soit `ipfix`. `logstream` est la valeur par défaut.	Non
mesures-côté-client	L'une des propriétés de la liste. La valeur de cet attribut est soit ENABLED, soit DISABLED. DISABLED est la valeur par défaut.	Non
http-x-forwarded-for	L'une des propriétés de la liste. La valeur de cet attribut est soit ENABLED, soit DISBALED. L'attribut active ou désactive l'insertion de l'en-tête X-Forwarded-For pour transmettre les informations d'adresse IP du client au serveur principal. DISABLED est la valeur par défaut.	Non
enable-hdxinsight-for	L'une des propriétés de la liste. La valeur de cet attribut est soit ICA, soit TCP. Cet attribut active `hdxinsight` pour des données de trafic spécifiques. ICA est la valeur par défaut.	Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple 1 : Configuration de l'analyse pour un seul serveur virtuel

```
operations:



  analytics:

    -

    name: lbvserver-ops-comp

    properties:

        target: $components-basic-lb-comp.outputs.lbvserver-name

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        transport-mode: logstream

        client-side-measurements: ENABLED

        insights:

          -

            type: webinsight

          -

            type: securityinsight
```

Exemple 2 : Configuration de l'analyse pour une liste de serveurs virtuels VPN

```
operations:



    analytics:

    -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

         http-x-forwarded-for: ENABLED

        insights:

          -

            type: hdxinsight

            enable-hdxinsight-for: TCP
```

Chaque attribut de la section d'analyse configure les instances NetScaler pour collecter les enregistrements AppFlow sur le serveur virtuel identifié par la propriété cible.

Serveurs virtuels cibles et types d'informations

Les serveurs virtuels cibles et les types d'informations autorisés correspondants sont les suivants :

SERVEUR VIRTUEL CIBLE	TYPE D'INFORMATIONS
LB vserver	analyse web, analyse de sécurité, analyse des bots
serveur virtuel CS	Analyse Web, Analyse de sécurité, Analyse des bots
serveur vpn	aperçu hdx, aperçu de la passerelle

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

IPFIX est le mode de transport par défaut utilisé pour configurer les analyses pour les serveurs virtuels dans les StyleBooks.

Alarmes

La sous-section des alarmes de la section des opérations a une structure similaire et les mêmes attributs que la sous-section d'analyse. La seule différence réside dans l'attribut des propriétés. Pour une liste de tous les attributs (autres que l'attribut des propriétés), voir Analyse.

Les propriétés suivantes sont disponibles dans une sous-section d'alarmes :

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
cible	Une expression qui évalue le nom d'un serveur virtuel, configuré sur le NetScaler, pour lequel des alarmes sont configurées.	Oui
email-profile	Nom d'un profil de messagerie défini dans la fonctionnalité NetScaler Console Analytics et contenant une liste d'adresses e-mail que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un profil de messagerie ou un profil SMS doit être défini)
sms-profile	Nom d'un profil SMS défini dans la fonctionnalité NetScaler Console Analytics et contenant une liste de numéros de téléphone que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un profil de messagerie ou un profil SMS doit être défini)
règles	Une liste de règles qui définissent les conditions qui déclencheraient une alarme	Oui

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	DESCRIPTION	OBLIGATOIRE
	pour le serveur virtuel défini par la propriété cible.	
métrique	Un attribut de règle. Le nom d'une métrique que vous souhaitez suivre concernant le serveur virtuel NetScaler.	Oui
opérateur	Un attribut de règle. L'opérateur à utiliser pour comparer la métrique à la valeur. Les opérateurs valides sont « greaterthan » et « lessthan ».	Oui
valeur	Un attribut de règle. La valeur seuil à laquelle la métrique est comparée à l'aide de l'opérateur. Si la valeur de la métrique dépasse ce seuil, les alarmes associées sont déclenchées.	Oui
unité de période	Un attribut d'une règle. La fréquence à laquelle alerter les utilisateurs si la règle d'alarme est respectée. Cela peut contenir la valeur jour, heure ou hebdomadaire. Cela signifie que si la règle est respectée, une alarme sera envoyée une fois par unité de période (par exemple, une fois par jour).	Oui

Le tableau suivant fournit une liste de métriques suivies concernant le serveur virtuel NetScaler.

Compteurs|Description|Description détaillée|Calcul de la console NetScaler

Pour un serveur virtuel VPN			

© 1997–2026 Citrix Systems, Inc. All rights reserved.

app_count	Nombre de lancements d'applications VPN	Nombre total d'applications VPN uniques sur ce serveur virtuel VPN lancées pendant un intervalle de temps spécifié par l'utilisateur.	Compteur croissant de manière monotone à chaque nouveau lancement d'application
app_launch_duration	Durée de lancement de l'application VPN	Temps moyen nécessaire au lancement d'une application (en millisecondes)	Valeur moyenne calculée sur les durées de lancement de toutes les applications VPN lancées sur ce serveur virtuel VPN
Autres serveurs virtuels (CS, LB, Auth, GSLB)			
total_requests	Nombre de requêtes	Nombre de requêtes client sur ce serveur virtuel depuis le dernier redémarrage de l'appliance, ou depuis la création du serveur virtuel, selon la date la plus récente.	Compteur à augmentation monotone, incrémenté à chaque nouvelle requête vers ce serveur virtuel.
total_bytes	Octets	Total des octets transférés du serveur virtuel vers NetScaler Console sur l'intervalle de temps spécifié.	Compteur à augmentation monotone pour le nombre total d'octets servis par ce serveur virtuel.
application_response_time	Temps de réponse	Temps de réponse moyen du serveur virtuel.	La valeur moyenne des temps de réponse de toutes les requêtes reçues par ce serveur virtuel

© 1997–2026 Citrix Systems, Inc. All rights reserved.

			depuis le dernier redémarrage de l'appliance (ou depuis la création du serveur virtuel), la plus récente des deux dates étant retenue.

Exemple de section d'alarmes dans un StyleBook :

```
operations:

alarms:

 -

  name:lbvserver_alarm

  properties:

  target: $outputs.lbvserver

  email-profile: $parameters.emailprofile

  sms-profile: "NetScalerSMS"

     rules:

      -

        metric: "total_requests"

        operator: "greaterthan"

        value: 25

        period-unit: weekly

        -

          metric: "total_bytes"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        operator: "lessthan"

        value: 1024

        period-unit: day
```

Expressions

L'une des fonctionnalités les plus puissantes d'un StyleBook est l'utilisation d'expressions. Vous pouvez utiliser les expressions StyleBooks dans divers scénarios pour calculer des valeurs dynamiques. L'exemple suivant est une expression permettant de concaténer une valeur de paramètre avec une chaîne littérale.

Exemple :

```
$parameters.appname + "-mon"
```

Cette expression récupère le paramètre nommé `appname` et le concatène avec la chaîne `-mon`.

Les types d'expressions suivants sont pris en charge :

Expressions arithmétiques

- Addition (+)
- Soustraction (-)
- Multiplication (*)
- Division (/)
- Modulo (%)

Exemples :

- Ajout de deux nombres : $parameters.a + $parameters.b
- Multiplication de deux nombres : $parameters.a * 10
- Recherche du reste après la division d'un nombre par un autre :

Résulte en `15%10` `5`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expressions de chaîne

- Concaténer deux chaînes (+)

Exemple :

Concaténer deux chaînes : str("app-") + $parameters.appname

Expressions de liste

Fusionne deux listes (+)

Exemple :

- Concaténer deux listes : $parameters.external-servers + $parameters.internal-servers
- Si `$parameters.ports-1` est et `$parameters.port-2` est , le `$parameters.ports-1 + $parameters.ports-2` s'affiche sous forme de liste .

Expressions relationnelles

- **==** : Teste si deux opérandes sont égaux et renvoie vrai s'ils le sont, sinon renvoie faux.
- **!=** : Teste si deux opérandes sont différents et renvoie vrai s'ils le sont, sinon renvoie faux.
- **\>** : Renvoie vrai si le premier opérande est supérieur au second opérande, sinon renvoie faux.
- **\>=** : Renvoie vrai si le premier opérande est supérieur ou égal au second opérande, sinon renvoie faux.
- **\<** : Renvoie vrai si le premier opérande est inférieur au second opérande, sinon renvoie faux.
- **\<=** : Renvoie vrai si le premier opérande est inférieur ou égal au second opérande, sinon renvoie faux.

Exemple :

- Utilisation de l'opérateur d'égalité : `$parameters.name = = "abcd"`
- Utilisation de l'opérateur d'inégalité : `$parameters.name != "default"`
- Exemples d'autres opérateurs relationnels
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 10 != 1

Expressions logiques - booléennes

- **and** : L'opérateur logique 'et'. Si les deux opérandes sont vrais, le résultat est vrai, sinon il est faux.
- **or** : L'opérateur logique 'ou'. Si l'un des opérandes est vrai, le résultat est vrai, sinon il est faux.
- **not** : L'opérateur unaire. Si l'opérande est vraie, le résultat est faux, et inversement.
- **in** : Teste si le premier argument est une sous-chaîne du second argument.
- **in** : Teste si un élément fait partie d'une liste.

REMARQUE

Vous pouvez transtyper des expressions où les chaînes sont converties en nombres et les nombres en chaînes. De même, vous pouvez transtyper `tcp-port` en nombre, et une adresse IP peut être transtypée en chaîne.

Utilisez un délimiteur avant et après tout opérateur. Vous pouvez utiliser les délimiteurs suivants :

- Avant un opérateur : `space`, `tab`, `comma`, `(`, `)`, `[`, `]`
- Après un opérateur : `space`, `tab`, `(`, `[`

Par exemple :

- `abc + def`
- `100 % 10`
- `10 > 9`

Expressions de chaîne littérales

Vous pouvez utiliser des chaînes littérales lorsque des caractères spéciaux dans une chaîne doivent prendre leur forme littérale. Ces chaînes peuvent contenir des caractères d'échappement, des barres obliques inverses, des guillemets, des parenthèses, des espaces, des crochets, etc. Dans les chaînes littérales, l'interprétation habituelle des caractères spéciaux est ignorée. Tous les caractères de la chaîne sont conservés dans leur forme littérale.

Dans les StyleBooks, vous pouvez inclure des expressions de stratégie NetScaler sous leur forme littérale en utilisant des chaînes littérales. Les expressions de stratégie contiennent généralement

© 1997–2026 Citrix Systems, Inc. All rights reserved.

des caractères spéciaux. Sans chaînes littérales, vous devez échapper les caractères spéciaux en divisant les chaînes en sous-chaînes.

Pour créer une chaîne de caractères littérale, encapsulez une chaîne entre des caractères spéciaux comme suit :

```
~{string}~
```

Vous pouvez utiliser des chaînes de caractères littérales n'importe où dans le StyleBook.

REMARQUE

N'utilisez pas la séquence de caractères `}~` dans une chaîne d'entrée, car cette séquence indique la fin d'une chaîne de caractères littérale.

Exemple :

```
~{HTTP.REQ.COOKIE.VALUE("jsessionid") ALT
HTTP.REQ.URL.BEFORE_STR("=").AFTER_STR(";jsessionid=") ALT
HTTP.REQ.URL.AFTER_STR(";jsessionid=")}~
```

Expressions cibles

Dans une définition de StyleBook, vous pouvez utiliser l'expression `$current-target` pour faire référence à l'instance NetScaler cible actuelle. Pour faire spécifiquement référence à l'adresse IP de l'instance NetScaler cible, utilisez cette expression comme suit :

```
$current-target.ip
```

Exemple :

```
components:

 -

  name: lb-comp

  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  properties:

    name: $current-target.ip + "-lbvserver"
```

Dans cet exemple, le nom du `lbvserver` est construit avec l'adresse IP de l'instance NetScaler cible.

Validation du type d'expression

Le moteur StyleBook permet une vérification de type plus stricte au moment de la compilation, c'est-à-dire que les expressions utilisées lors de l'écriture du StyleBook sont validées lors de l'importation du StyleBook lui-même plutôt que lors de la création du pack de configuration.

Toutes les références aux paramètres, substitutions, composants, propriétés des composants, sorties des composants, variables définies par l'utilisateur (repeat-item, repeat-index, arguments des fonctions de substitution) et ainsi de suite sont toutes validées pour leur existence et leurs types.

Exemple de vérifications de type :

Dans l'exemple suivant, le type attendu de la propriété de port du StyleBook `lbvserver` est `tcp-port`. Dans NetScaler Console, les validations de type se produisent au moment de la compilation (importation). Le compilateur constate que la chaîne et `tcp-port` ne sont pas des types compatibles et, par conséquent, le compilateur StyleBook affiche une erreur et ne parvient pas à importer ou à migrer un StyleBook.

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: str("80")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: HTTP
```

Pour compiler ce StyleBook avec succès, déclarez ce qui suit comme un nombre dans le compilateur :

`port: 80`

Exemple de signalement d'expressions non valides :

Dans les versions précédentes, lorsqu'une expression non valide était attribuée à un nom de propriété, le compilateur ne détectait pas les expressions non valides et permettait l'importation des StyleBooks dans NetScaler Console. Désormais, si ce StyleBook est importé dans NetScaler Console, le compilateur identifie ces expressions non valides et les signale. Par conséquent, l'importation du StyleBook dans NetScaler Console échoue.

Dans cet exemple, l'expression attribuée à la propriété de nom dans le composant `lb-sg-binding-comp` est : `$components.lbvserver-comp.properties.lbvservername`. Cependant, il n'y a pas de propriété appelée `lbvservername` dans le composant `lbvserver-comp`. Dans les versions précédentes de NetScaler Console, le compilateur aurait autorisé cette expression et l'aurait importée avec succès. L'échec réel se produirait lorsqu'un utilisateur voudrait créer un pack de configuration à l'aide de ce StyleBook. Cependant, maintenant, ce type d'erreur est identifié lors de l'importation et le StyleBook n'est pas importé dans NetScaler Console. Corrigez manuellement ces erreurs et importez les StyleBooks.

```
Components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    servicetype: HTTP

-

  name: sg-comp

  type: ns::servicegroup

  properties:

    servicegroupname: mysg

    servicetype: HTTP

-

  name: lb-sg-binding-comp

  type: ns::lbvserver_servicegroup_binding

  condition: $parameters.create-binding

  properties:

    name: $components.lbvserver-comp.properties.lbvservername

    servicegroupname: $components.sg-comp.properties.servicegroupname
```

Indexation des listes

Les éléments d'une liste peuvent désormais être accédés en les indexant directement :

Expression	Description
`$components.test-lbs[0]`	Fait référence au premier élément du composant test-lbs
`$components.test-lbs[0].properties.p1`	Fait référence à la propriété p1 du premier élément du composant test-lbs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Fait référence à la propriété `servicegroupname` du deuxième élément du composant `servicegroups`, qui est une sortie du premier élément du composant `lbcomps`

Interpolations sur place

Il est maintenant possible de remplacer une ou plusieurs parties d'une chaîne de caractères à l'aide d'une ou plusieurs expressions StyleBook. Lorsque ces expressions de chaîne sont évaluées par le compilateur StyleBook, la partie de la chaîne qui utilise une expression StyleBook sera remplacée par la valeur de l'expression. Pour inclure des expressions StyleBook dans une chaîne, nous utilisons la notation suivante :

```
"...%{...}%..."
```

où les caractères encadrés entre « %{ » et « }% » forment une expression StyleBook. Ces expressions sont appelées « interpolations sur place ».

Par exemple, la chaîne « lb-%{$parameters.appname}%-svc » est une expression de chaîne avec interpolation sur place d'une expression StyleBook. La valeur de l'expression de chaîne dépend de la valeur de l'expression d'interpolation. Supposons que **$parameters.appname** soit affecté de la valeur « app1 ». Alors, l'expression de chaîne s'évalue en **lb-app1-svc**. Cela permet que les valeurs ne soient pas codées en dur dans les expressions de chaîne, mais plutôt évaluées en fonction des valeurs définies par l'utilisateur.

Un cas d'utilisation pratique des interpolations sur place est la paramétrisation des expressions de stratégie dans les StyleBooks. Considérez un scénario où vous souhaitez écrire une expression de stratégie qui vérifie si l'URL HTTP contient un mot spécifique, par exemple, « jpeg ».

Pour cela, vous écrivez une expression de stratégie comme suit : "HTTP.REQ.URL.CONTAINS(\ \"jpeg\\\")".

Maintenant, si vous souhaitez paramétrer l'objet dans l'URL HTTP, vous pouvez ajouter un paramètre de chaîne dans le StyleBook, par exemple, $parameters.url-object. L'expression de stratégie doit être écrite en fonction de ce paramètre. Pour ce faire, vous utilisez la concaténation de chaînes pour obtenir le résultat. L'expression ressemblerait à ceci :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
```

Si $parameter.url-object est affecté de la valeur « csv », l'expression ci-dessus s'évaluera en « HTTP.REQ.URL.CONTAINS(\\"csv\\") ». Cependant, cette expression n'est pas facile à lire. Pour rendre cette paramétrisation facile à lire et à comprendre, vous pouvez utiliser des interpolations sur place.

L'expression avec interpolation sur place est maintenant :

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

Dans l'expression ci-dessus, vous avez utilisé une expression d'interpolation qui ajoute les guillemets intérieurs autour de la valeur de $parameters.url-object. Le résultat de cette expression est le même que ci-dessus, mais il semble plus intuitif et plus proche du résultat réel.

Types autorisés dans les interpolations

Vous pouvez utiliser des expressions qui génèrent des valeurs des types suivants à l'intérieur des interpolations : booléen, nombre, port TCP, adresse IP et chaîne de caractères. La valeur générée est automatiquement transformée en chaîne de caractères lorsque les interpolations sont remplacées par le résultat.

Les expressions de chaîne peuvent avoir 0, 1 ou plusieurs interpolations. Dans une interpolation séquentielle, différentes parties de l'expression de chaîne peuvent être remplacées par différentes expressions StyleBook. Par exemple, la chaîne lb-%{$parameters.appname}%-%{$parameters.vip}% renvoie "lb-app1-1.1.1.1", si $parameters.appname est "app1" et $parameters.vip est "1.1.1.1"

Les expressions de chaîne prennent également en charge les interpolations imbriquées. Autrement dit, une expression d'interpolation peut être imbriquée dans une autre expression d'interpolation afin que la valeur d'une expression puisse devenir une entrée pour la seconde expression.

Par exemple, considérons la chaîne "%{lb-%{$parameters.port + 1}%}%"

La chaîne interne, "**%{$parameters.port + 1}%**" renvoie "lb-81" si $parameters.port est 80. Ici, cette expression est imbriquée dans une autre expression d'interpolation.

Le tableau suivant décrit les différents types d'interpolations avec des exemples et les résultats correspondants. La valeur des paramètres utilisés dans les exemples est la suivante :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- $parameters.appname: "lb1"
- $parameters.vip: "1.1.1.1"
- $parameters.n1: 1
- $parameters.n2: 3

Interpolations simples

EXPRESSION	RÉSULTAT
lb-%{$parameters.appname}%-def	lb-lb1-def

Conversions de type automatiques

EXPRESSION	RÉSULTAT
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Interpolations séquentielles

EXPRESSION	RÉSULTAT
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Interpolations imbriquées

EXPRESSION	RÉSULTAT
%{abc-%{$parameters.n1 + 1}%}%	abc-2
str("%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%")	bc-1-3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Interpolations avec quotewrap

EXPRESSION	RÉSULTAT
str("%{quotewrap(abcd)}%")str("%{quotewrap(`https://`)}%`+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	"exemple"<`https://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL`

Caractères d'échappement dans les interpolations

Si les caractères "%{" ou "}%" font partie de la chaîne, vous devez fournir "`\`" comme caractère d'échappement afin que le compilateur StyleBook ne les évalue pas comme des balises d'interpolation.

Exemple :

str("%{\%\{ + str($parameters.vip) + \}\%}%") renvoie "%{1.1.1.1}%" si $parameters.vip est 1.1.1.1

Le tableau suivant décrit quelques expressions supplémentaires et leurs résultats :

CATÉGORIE	EXPRESSION	RÉSULTAT
Échappement des interpolations	str("%{str($parameters.n1) + } \%}%")	1}%
	lb-%{str($parameters.n1) + }\%}%	lb-1}%
	"%{str($parameters.n1) + \"\}\%\"}%"	1}%

Fonctions intégrées

Les fonctions intégrées sont utilisées par les expressions dans les StyleBooks.

Par exemple, vous pouvez utiliser la fonction intégrée, `str()` pour transformer un nombre en chaîne de caractères.

`str($parameters.order)`

Ou, vous pouvez utiliser la fonction intégrée, `int()` pour transformer une chaîne de caractères en entier.

`int($parameters.priority)`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voici la liste des fonctions intégrées prises en charge dans les expressions StyleBook, avec des exemples de leur utilisation :

Fonction str()

La fonction `str()` transforme l'argument d'entrée en une valeur de chaîne de caractères.

Types d'arguments autorisés :

- `string`
- `number`
- `TCP-port`
- `boolean`
- `IP address`

Exemples :

- La fonction `"set-" + str(10)` renvoie `"set-10"`.
- La fonction `str(10)` renvoie `10`.
- La fonction `str(1.1.1.1)` renvoie `1.1.1.1`.
- La fonction `str(T rue)` renvoie `"T rue"`.
- La fonction `str(ADM)` renvoie `"mas"`.

entier()

La fonction `int()` prend une chaîne de caractères, un nombre, une adresse IP ou `tcpport` comme argument et renvoie un entier.

Exemples :

- La fonction `int("10")` renvoie `10`.
- La fonction `int(10)` renvoie `10`.
- La fonction `int(ip('0.0.4.1'))` renvoie `1025`.

booléen()

La fonction `bool()` prend n'importe quel type comme argument. Si la valeur de l'argument est `false`, vide ou absente, cette fonction renvoie `false`.

Sinon, elle renvoie `true`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemples :

- La fonction `bool(true)` renvoie `true`.
- La fonction `bool(false)` renvoie `false`.
- La fonction `bool($parameters.a)` renvoie `false` si le `$parameters.a` est `false`, vide ou absent.

Fonction len()

La fonction `len()` prend une chaîne ou une liste comme argument et renvoie le nombre de caractères dans une chaîne ou le nombre d'éléments dans une liste.

Exemple 1 :

Si vous définissez une substitution comme suit :

```
items: ["123", "abc", "xyz"]
```

La fonction `len($substitutions.items)` renvoie `3`

Exemple 2 :

La fonction `len("NetScaler Console")` renvoie `10`.

Exemple 3 :

Si `$parameters.vips` a les valeurs `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, la fonction `len($parameters.vips)` renvoie `3`.

Fonction min()

La fonction `min()` prend en argument soit une liste, soit une série de nombres ou `tcp-ports`, et renvoie l'élément le plus petit.

Exemples avec une série de nombres/ports TCP :

- La fonction `min(80, 100, 1000)` renvoie `80`.
- La fonction `min(-20, 100, 400)` renvoie `-20`.
- La fonction `min(-80, -20, -10)` renvoie `-80`.
- La fonction `min(0, 100, -400)` renvoie `-400`.

Exemples avec une liste de nombres/ports TCP :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le support `$parameters.ports` est une liste de `tcp-ports` et a les valeurs : `[80, 81, 8080]`.

  La fonction `min($parameters.ports)` renvoie `80`.

maximum()

La fonction `max()` prend en argument soit une liste, soit une série de nombres ou `tcp-ports`, et renvoie l'élément le plus grand.

Exemples avec une série de nombres/ports TCP :

- La fonction `max(80, 100, 1000)` renvoie `1000`.
- La fonction `max(-20, 100, 400)` renvoie `400`.
- La fonction `max(-80, -20, -10)` renvoie `-10`.
- La fonction `max(0, 100, -400)` renvoie `100`.

Exemples avec une liste de nombres/ports TCP :

- Le support `$parameters.ports` est une liste de `tcp-ports` et a les valeurs : `[80, 81, 8080]`.

  La fonction `max($parameters.ports)` renvoie `8080`.

binaire()

La fonction `bin()` prend un nombre comme argument et renvoie une chaîne de caractères qui représente le nombre au format binaire.

Exemples d'expressions :

La fonction `bin(100)` renvoie `0b1100100`.

octal()

La fonction `oct()` prend un nombre comme argument et renvoie une chaîne de caractères qui représente le nombre au format octal.

Exemples d'expressions :

La fonction `oct(100)` renvoie `0144`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

hexadécimal()

La fonction `hex()` prend un nombre comme argument et renvoie une chaîne de caractères en minuscules qui représente le nombre au format hexadécimal.

Exemples d'expressions :

La fonction `hex(100)` renvoie `0x64`.

minuscule()

La fonction `lower()` prend une chaîne de caractères comme argument et renvoie la même chaîne en minuscules.

Exemple :

La fonction `lower("ADM")` renvoie `adm`.

majuscule()

La fonction `upper()` prend une chaîne de caractères comme argument et renvoie la même chaîne en majuscules.

Exemple :

La fonction `upper("NetScaler Console")` renvoie `NetScaler Console`.

somme()

La fonction `sum()` prend une liste de nombres ou `tcpports` comme arguments et renvoie la somme des nombres de la liste.

Exemple 1 :

Si vous définissez une substitution comme suit : substitutions :

```
list-of-numbers = [11, 22, 55]
```

La fonction `sum($substitutions.list-of-numbers)` renvoie `88`.

Exemple 2 :

Si `$parameters.ports` est `[80, 81, 82]`, la fonction `sum($parameters.ports)` renvoie `243`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fonction pow()

La fonction `pow()` prend deux nombres comme arguments et renvoie un nombre qui représente le premier argument élevé à la puissance du second.

Exemple :

La fonction `pow(3,2)` renvoie `9`.

ip()

La fonction `ip()` prend un entier, une chaîne de caractères ou une adresse IP comme argument et renvoie l'adresse IP basée sur la valeur d'entrée.

Exemples :

- Spécifiez une adresse IP dans la fonction `ip` :

  La fonction `ip(3.1.1.1)` renvoie `3.1.1.1`.
- Spécifiez une chaîne de caractères dans la fonction `ip` :

  La fonction `ip('2.1.1.1')` renvoie `2.1.1.1`
- Spécifiez un entier dans la fonction `ip` :
  - La fonction `ip(12)` renvoie `0.0.0.12`.
  - Lorsque vous spécifiez un entier sous forme de chaîne dans la fonction `ip`, elle renvoie une adresse IP équivalente à l'entrée.

    La fonction `ip('1025')` renvoie `0.0.4.1`.

  Cette fonction prend également en charge les opérations d'addition et de soustraction d'entiers et renvoie une adresse IP résultante.

  - Addition : La fonction `ip(1025) + ip(12)` renvoie `0.0.4.13`.
  - Soustraction : La fonction `ip('1025') - ip(12)` renvoie `0.0.3.245`.
  - Combiner l'addition et la soustraction : La `ip('1.1.1.1') + ip('1.1.1.1') – ip(2)` renvoie `2.2.2.0`.

base64.encode()

La fonction `base64.encode()` prend un argument de type chaîne et renvoie la chaîne encodée en base64.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple :

La fonction `base64.encode("abcd")` renvoie `YWJjZA==`.

base64.decode()

La fonction `base64.decode` prend une chaîne encodée en base64 comme argument et renvoie la chaîne décodée.

Exemple :

La fonction `base64.decode("YWJjZA==")` renvoie `abcd`.

existe()

La fonction `exists()` prend un argument de n'importe quel type et renvoie un booléen. La valeur de retour est `True` si l'entrée a une valeur. La valeur de retour est `False` si l'argument d'entrée n'a pas de valeur (c'est-à-dire, aucune valeur).

Considérons que `$parameters.monitor` est un paramètre facultatif. Si vous fournissez une valeur à ce paramètre lors de la création d'un pack de configuration, la fonction `($parameters.monitor)` renvoie `True`.

Sinon, elle renvoie `False`.

Filtrer()

La fonction `filter()` prend deux arguments.

Argument 1 : une fonction de substitution qui prend un argument et renvoie une valeur booléenne.

Argument 2 : une liste.

La fonction renvoie un sous-ensemble de la liste originale où chaque élément est évalué à `True` lorsqu'il est passé à la fonction de substitution dans le premier argument.

Exemple :

Considérons une fonction de substitution comme suit :

Substitutions :

```
x(a): $a != 81
```

Cette fonction renvoie True si la valeur d'entrée n'est pas égale à `81`. Sinon, elle renvoie `False`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supposons que `$parameters.ports` soit `[81, 80, 81, 89]`.

La fonction `filter($substitutions.x, $parameters.ports)` renvoie `[80, 89]` en supprimant toutes les occurrences de `81` de la liste.

if-then-else()

La fonction `if-then-else()` prend trois arguments.

Argument 1 : Expression booléenne

Argument 2 : Toute expression

Argument 3 : Toute expression (facultatif)

Si l'expression de l'argument 1 est évaluée à `True`, la fonction renvoie la valeur de l'expression fournie comme argument 2.

Sinon, si l'argument 3 est fourni, la fonction renvoie la valeur de l'expression de l'argument 3.

Si l'argument 3 n'est pas fourni, la fonction renvoie `no`.

Exemple 1 :

La fonction `if-then-else($parameters.servicetype == HTTP, 80, 443)` renvoie `80` si `$parameters.servicetype` a la valeur `HTTP`. Sinon, la fonction renvoie `443`.

Exemple 2 :

La fonction `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` renvoie la valeur de `$parameters.hport` si `$parameters.servicetype` a la valeur `HTTP`.

Sinon, la fonction renvoie la valeur de `$parameters.sport`.

Exemple 3 :

La fonction `if-then-else($parameters.servicetype == HTTP, 80)` renvoie `80` si `$parameters.servicetype` a la valeur `HTTP`.

Sinon, la fonction ne renvoie aucune valeur.

joindre()

La fonction `join()` prend deux arguments :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Argument 1 : liste de nombres, `tcp-ports`, chaînes de caractères ou adresses IP

Argument 2 : chaîne de délimitation (facultatif)

Cette fonction joint les éléments de la liste fournie en tant qu'argument 1 en une chaîne de caractères, où chaque élément est séparé par la chaîne de délimitation fournie en tant qu'argument 2. Si l'argument 2 n'est pas fourni, les éléments de la liste sont joints en une seule chaîne.

Exemple :

- `$parameters.ports` est `[81, 82, 83]`.
  - Avec l'argument de délimitation :

    La fonction `join($parameters.ports, '-')` renvoie `81-82-83`.
  - Sans l'argument de délimitation :

    La fonction `join($parameters.ports)` renvoie `818283`.

diviser()

La fonction `split()` divise une chaîne d'entrée en plusieurs listes en fonction des séparateurs spécifiés. Si aucun séparateur ou un séparateur vide (`''`) n'est spécifié, cette fonction considère l'espace comme un séparateur et divise la chaîne en listes.

Exemples :

- La fonction `split('Example_string_split', 's')` renvoie `['Example_','tring_','plit']`.
- La fonction `split('Example string split')` renvoie `['Example','string','split']`.
- La fonction `split('Example string split', '')` renvoie `['Example','string','split']`.
- La fonction `split('Example string')` renvoie `['Example','string']`.

  Cette fonction considère les espaces continus comme un seul espace.

Mapper()

La fonction `map()` prend deux arguments ;

Argument 1 : Toute fonction

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Argument 2 : Une liste d'éléments.

La fonction renvoie une liste où chaque élément de la liste est le résultat de l'application de la fonction `map()` (argument 1) à l'élément correspondant de l'argument 2.

Fonctions autorisées dans l'argument 1 :

- Fonctions intégrées qui prennent un argument :

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`

- Fonctions de substitution qui prennent au moins un argument.

Exemple :

Supposons que $parameters.nums soit `[81, 82, 83]`.

- Mappage à l'aide d'une fonction intégrée, str

  La fonction `map(str, $parameters.nums)` renvoie `["81", "82", "83"]`

  Le résultat de la fonction de mappage est la liste de chaînes où chaque élément est une chaîne calculée en appliquant la fonction str sur l'élément correspondant de la liste d'entrée ($parameters.nums).

- Mappage à l'aide d'une fonction de substitution

  - Substitutions :

    `add-10(port): $port + 10`

  - Expression :

    La fonction `map($substitutions.add-10, $parameters.nums)` renvoie une liste de nombres : `[ 91, 92, 93 ]`

Le résultat de cette fonction de mappage est une liste de nombres. Chaque élément est calculé en appliquant la fonction de substitution `$substitutions.add-10` sur l'élément correspondant de la liste d'entrée `($parameters.nums)`.

mettre_entre_guillemets()

La fonction `quotewrap()` prend une chaîne de caractères comme argument et renvoie une chaîne après avoir ajouté un caractère de guillemet double avant et après la valeur d'entrée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple :

La fonction `quotewrap("ADM")` renvoie `"mas"`

remplacer()

La fonction `replace()` prend trois arguments :

Argument 1 : un `string` ou une liste des types intégrés suivants :

- `string`
- `number`
- `ipaddress`
- `tcp-port`
- `boolean`

Argument 2 : une valeur unique ou une liste de valeurs dont le type correspond au type spécifié dans l'argument 1

Argument 3 : une valeur unique du même type que celui spécifié dans l'argument 1 (facultatif)

La fonction `replace()` remplace toutes les occurrences de l'argument 2 par l'argument 3 dans l'argument 1.

Si l'argument 3 n'est pas fourni, toutes les occurrences de l'argument 2 sont supprimées de l'argument 1.

Exemple :

- La fonction `replace('abcdef', 'def', 'xyz')` renvoie `abcxyz`.

  Toutes les occurrences de `def` sont remplacées par `xyz`.
- `replace('abcdefabc', 'def')` renvoie `abcabc`.

  Comme il n'y a pas d'argument 3, `def` est supprimé de la chaîne résultante.
- La fonction `replace('An#example@to%replace!characters', ['@', '#', '!', '%'], '_')` renvoie `An_example_to_replace_characters`.

  La chaîne de sortie contient un trait de soulignement (_) au lieu des caractères spécifiés dans `['@', '#', '!', '%']`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La fonction `replace([10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4], [10.10.10.2, 10.10.10.4])` renvoie `[10.10.10.1, 10.10.10.3]`.

  Comme il n'y a pas d'argument 3, `10.10.10.2` et `10.10.10.4` sont supprimés de la liste d'adresses IP résultante.

- La fonction `replace([8080, 8081, 8082, 8083, 8084], 8083, 80)` renvoie `[8080, 8081, 8082, 80, 8084]`.

  Toutes les occurrences de `8083` sont remplacées par `80`.

rogner()

La fonction `trim()` renvoie une chaîne où les espaces blancs de début et de fin sont supprimés de la chaîne d'entrée.

Exemple :

La fonction `trim(' abc ')` renvoie `abc`.

tronquer()

La fonction `truncate()` prend deux arguments :

Argument 1 : chaîne

Argument 2 : nombre

La fonction renvoie une chaîne où la chaîne d'entrée de l'argument 1 est tronquée à la longueur spécifiée par l'argument 2.

Exemple :

Le `truncate('NetScaler Console', 6)` renvoie `Citrix`.

unique()

La fonction `distinct()` extrait les éléments uniques d'une entrée de liste.

Exemples : Si `$parameters.input_list` est `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`, la fonction `distinct($parameters.input_list)` renvoie `['ADM', 'ADC', 'VPX', 'CPX']`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

url.encode()

La fonction `url.encode()` renvoie une chaîne où les caractères sont transformés à l'aide du jeu de caractères ASCII conformément à la RFC 3986.

Exemple :

La fonction `url.encode("a/b/c")` renvoie `a%2Fb%2Fc`.

url.decode()

La fonction `url.decode()` renvoie une chaîne où l'argument encodé en URL est décodé en une chaîne de caractères normale conformément à la RFC 3986.

Exemple :

La fonction `url.decode("a%2Fb%2Fc")` renvoie `a/b/c`.

is-ipv4()

La fonction `is-ipv4()` prend une adresse IP comme argument et renvoie le booléen `True` si l'adresse IP est au format IPv4.

La fonction `is-ipv4(10.10.10.10)` renvoie `True`

is-ipv6()

La fonction `is-ipv6()` prend une adresse IP comme argument et renvoie le booléen `True` si l'adresse IP est au format IPv6.

La fonction `is-ipv6(2001:DB8::)` renvoie `True`

Commence par()

La fonction `startswith()` détermine si une chaîne commence par un préfixe donné. Cette fonction nécessite deux arguments de chaîne obligatoires.

`startswith(str, sub_str)`

Cette fonction renvoie `True` lorsque la chaîne (`str`) commence par la sous-chaîne (`sub_str`).

Exemples :

- La fonction `startswith('Citrix', 'Ci')` renvoie `True`.
- La fonction `startswith('Citrix', 'iC')` renvoie `False`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La fonction `startswith('Citrix', 'Ab')` renvoie `False`

Se termine par()

La fonction `endswith()` détermine si une chaîne se termine par un suffixe donné. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
endswith(str, sub_str)
```

Cette fonction renvoie `True` lorsque la chaîne (`str`) se termine par la sous-chaîne (`sub_str`).

Exemples :

- La fonction `endswith('Citrix', 'ix')` renvoie `True`.
- La fonction `endswith('Citrix', 'Ix')` renvoie `False`.
- La fonction `endswith('Citrix', 'ab')` renvoie `False`.

contient()

La fonction `contains()` détermine si une chaîne contient une sous-chaîne donnée. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
contains(str, sub_str)
```

Cette fonction renvoie `True` lorsque la sous-chaîne (`sub_str`) est contenue n'importe où dans la chaîne (`str`).

Exemple :

- La fonction `contains('Citrix', 'tri')` renvoie `True`.
- La fonction `contains('Citrix', 'Ci')` renvoie `True`.
- La fonction `contains('Citrix', 'ti')` renvoie `False`

sous-chaîne()

Utilisez la fonction `substring()` pour extraire une sous-chaîne d'une chaîne.

```
substring(str, start_index, end_index)
```

Cette fonction requiert deux arguments obligatoires et un argument entier facultatif.

- `str` (Obligatoire)
- `start_index` (Obligatoire)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `end_index` (Facultatif)

Cette fonction renvoie la sous-chaîne de la chaîne (`str`) qui se trouve entre les positions d'index spécifiées. Si vous ne spécifiez pas la position de l'index de fin, la fonction extrait la sous-chaîne de l'index de début jusqu'à la fin de la chaîne.

REMARQUE

Lorsque vous spécifiez `end_index`, la sous-chaîne exclut le caractère à la position `end_index`.

Exemple :

- La fonction `substring('Citrix', 2)` renvoie `trix`
- La fonction `substring('Citrix', 10)` renvoie (`''`)

  Dans cet exemple, la fonction renvoie une chaîne vide car elle a une position `start_index` non valide.
- La fonction `substring('Citrix', 2, 4)` renvoie `tr`

  Dans cet exemple, la fonction extrait les caractères entre les positions d'index 2 et 4.
- La fonction `substring('Citrix', -3)` renvoie `rix`

  Si vous souhaitez extraire des caractères qui se trouvent à la fin de la chaîne, spécifiez une valeur négative pour l'argument `start_index`.

  Dans cet exemple, la fonction extrait la sous-chaîne qui inclut les trois derniers caractères de la chaîne.

multiples()

La fonction `multiple()` prend deux arguments :

Argument 1 : un `number`, `string`, `boolean`, `ipaddress`, `tcp-port`, ou `password`

Argument 2 : un `number`

La fonction `multiple(argument1, argument2)` renvoie une liste avec de nombreuses copies de l'argument 1. Le nombre de copies est égal au nombre passé à l'argument 2.

Exemples :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La fonction `multiple(10.10.10.10, 3)` renvoie `[10.10.10.10, 10.10.10.10, 10.10.10.10]`.
- La fonction `multiple(8080, 4)` renvoie `[8080, 8080, 8080, 8080]`.

inverser()

La fonction reverse() prend une liste d'éléments comme argument et renvoie une liste avec les mêmes éléments, mais répertoriés dans l'ordre inverse.

L'argument peut être une liste des types intégrés suivants :

- `string`
- `number`
- `ipaddress`
- `ipnetwork`
- `tcp-port`
- `boolean`
- `password`
- `object`
- `file`
- `certfile`
- `keyfile`
- `certkey`

Exemples :

- reverse() renvoie .
- reverse() renvoie .
- reverse() renvoie .

Détection des dépendances

Les composants d'un StyleBook peuvent faire référence aux propriétés ou aux sections d'autres composants du même StyleBook. Les composants sont des blocs complets en eux-mêmes et peuvent ne pas être écrits dans le même ordre que celui dans lequel ils doivent être exécutés. Le

© 1997–2026 Citrix Systems, Inc. All rights reserved.

compilateur StyleBook vérifie l'ordre dans lequel les composants sont écrits, puis les exécute dans un ordre logique.

Exemple :

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

 -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: $components.lbvserver-comp.properties.name

      servicegroupname: $components.sg-comp.properties.servicegroupname

-

    name: sg-comp

    type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

      servicegroupname: mysg

      servicetype: HTTP
```

Dans l'exemple ci-dessus, trois composants sont définis : **lbvserver-comp**, **lb-sg-binding-comp** et **sg-comp**. Lorsque ce StyleBook est exécuté, le lbvserver-comp est d'abord créé. Le lb-sg-binding-comp fait référence aux propriétés du lbvserver-comp, mais il ne peut pas être créé ensuite, même s'il s'agit du deuxième composant défini dans le StyleBook. Cela est dû au fait que le lb-sg-binding-comp a également une dépendance vis-à-vis du sg-comp qui n'a pas encore été créé. Par conséquent, le compilateur réorganise les composants de manière à ce que les dépendances d'un composant soient résolues au moment où un composant est créé, et exécute cette liste de composants réorganisée. L'ordre d'exécution du StyleBook ci-dessus est : lbvserver-comp, sg-comp et lb-sg-binding-comp.

Ainsi, l'auteur d'un StyleBook n'a pas à se soucier de l'ordre correct des composants. Les composants peuvent apparaître dans n'importe quel ordre. Le compilateur calcule l'ordre d'exécution correct des composants en fonction de la manière dont les composants se réfèrent les uns aux autres. Notez que cette détection de dépendance et ce réordonnancement fonctionnent également pour les sections de substitutions et de sorties.

Dépendances cycliques

Puisqu'un composant peut faire référence à un autre composant, il est possible qu'un cycle de dépendances soit introduit dans la définition du StyleBook. Par exemple, si le composant A fait référence à une propriété définie dans le composant B, qui à son tour fait référence à une propriété définie dans le composant A. Ce type de dépendance est appelé dépendances cycliques. Les dépendances cycliques ne peuvent pas être résolues automatiquement. L'auteur du StyleBook doit corriger manuellement la définition du StyleBook pour éliminer ces dépendances cycliques. Le compilateur sera en mesure d'identifier les dépendances cycliques, si elles existent, et de les signaler.

L'exemple suivant montre une dépendance cyclique de composants :

```
components:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $components.lb-sg-binding-comp.properties.name
    ipv46: 10.102.190.15
    port: 80
    servicetype: HTTP
-
  name: lb-sg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  condition: $parameters.create-binding
  properties:
   name: mylb
    servicegroupname: $components.sg-comp.properties.servicegroupname
-
  name: sg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: mysg
    servicetype: $components.lbvserver-comp.properties.servicetype
```

Dans l'exemple ci-dessus, il y a trois composants : **lbvserver-comp**, **lb-sg-binding-comp** et **sg-comp**. lbvserver-comp dépend de lb-sg-binding-comp, lb-sg-binding-comp dépend de sg-comp et

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sg-comp dépend de lbvserver-comp. Ici, un cycle de dépendances entre ces composants est formé et cela ne peut pas être résolu automatiquement. Par conséquent, ce StyleBook ne peut pas être exécuté. Le compilateur StyleBook le détecte et empêche l'importation du StyleBook dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sécurité

Les analyses de sécurité de NetScaler Console vous aident à surveiller, détecter et atténuer les menaces pesant sur vos applications. Les rubriques suivantes vous aident à visualiser et à agir sur les informations de sécurité :

- Tableau de bord de sécurité des applications
- Violations de sécurité
- Sécurité des API

Tableau de bord de sécurité des applications

Le tableau de bord **Sécurité des applications** vous donne un aperçu des métriques de sécurité pour les applications découvertes/sous licence. Ce tableau de bord affiche les informations sur les attaques de sécurité pour les applications découvertes/sous licence, telles que les attaques de synchronisation, les attaques par petite fenêtre, les attaques par inondation DNS, etc.

Pour afficher les métriques de sécurité sur le tableau de bord de sécurité des applications :

1. Accédez à **Sécurité** > **Tableau de bord de sécurité**.
2. Sélectionnez l'adresse IP de l'instance dans la liste des instances.

   Les rapports incluent les informations suivantes pour chaque application :

   - **Indice de menace**. Un système de notation à un chiffre qui indique la criticité des attaques sur l'application. Plus les attaques sur une application sont critiques, plus l'indice de menace pour cette application est élevé. Les valeurs vont de 1 à 7.

     L'indice de menace est basé sur les informations d'attaque. Les informations relatives aux attaques, telles que le type de violation, la catégorie d'attaque, l'emplacement et les détails du client, donnent un aperçu des attaques sur l'application. Les informations de violation sont envoyées à NetScaler Console uniquement lorsqu'une violation ou une attaque se produit. Un grand nombre de brèches et de vulnérabilités entraîne une valeur d'indice de menace élevée.
   - **Indice de sécurité**. Un système de notation à un chiffre qui indique le niveau de sécurité avec lequel vous avez configuré les instances NetScaler pour protéger les applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

contre les menaces et vulnérabilités externes. Moins les risques de sécurité pour une application sont élevés, plus l'indice de sécurité est élevé. Les valeurs vont de 1 à 7.

L'indice de sécurité prend en compte à la fois la configuration du pare-feu d'application et la configuration de sécurité du système NetScaler. Pour une valeur d'indice de sécurité élevée, les deux configurations doivent être robustes. Par exemple, si des contrôles rigoureux du pare-feu d'application sont en place, mais que les mesures de sécurité du système NetScaler, telles qu'un mot de passe fort pour l'utilisateur `nsroot`, ne sont pas fournies, alors les applications se voient attribuer une faible valeur d'indice de sécurité.

Vous pouvez consulter les écarts signalés sur l'**App Security Investigator**.

Détails de l'indice de menace



1 - Affiche l'adresse IP de l'instance NetScaler pour laquelle vous pouvez afficher les détails.

2 - Affiche des détails tels que le score de l'indice de menace, le nombre total de violations survenues et le nombre total de violations bloquées.

3 - Affiche le serveur virtuel de l'instance sélectionnée.

4 - Affiche les violations de sécurité basées sur les clients. Le graphique App Security Investigator est affiché pour chaque client. Vous pouvez cliquer sur chaque adresse IP de client pour afficher les résultats.

5 - Affiche les violations en vue cartographique et en vue tabulaire.

6 - Affiche les détails de la violation. Lorsque vous survolez le graphique avec le pointeur de la souris, les détails tels que le type de violation, l'heure de l'attaque et le nombre total d'événements sont affichés.

Lorsque vous cliquez sur un graphique à bulles, les détails s'affichent dans la page **Détails de la violation de sécurité de l'application**. Par exemple, si vous souhaitez afficher plus de détails sur une violation de script intersite (cross-site scripting), cliquez sur le graphique renseigné pour **XSS** dans **App Security Investigator**.

Les **Détails de la violation de sécurité de l'application** s'affichent avec les détails de la violation tels que l'heure de l'attaque, la catégorie de l'attaque, la gravité, l'URL, etc.



Vous pouvez également cliquer sur l'option **Paramètres** pour sélectionner les options que vous souhaitez afficher.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Détails de l'indice de sécurité

Après avoir examiné l'exposition aux menaces d'une application, vous souhaitez déterminer quelles configurations de sécurité d'application sont en place et quelles configurations sont manquantes pour cette application. Vous pouvez obtenir ces informations en explorant le résumé de l'indice de sécurité de l'application.

Le résumé de l'indice de sécurité vous donne des informations sur l'efficacité des configurations de sécurité suivantes :

- **Configuration du pare-feu d'application**. Indique le nombre d'entités de signature et de sécurité non configurées.
- **Sécurité du système NetScaler Console**. Indique le nombre de paramètres de sécurité du système non configurés.

Pour afficher les détails de l'**Indice de sécurité**, sélectionnez un serveur virtuel/une application et cliquez sur l'onglet **Indice de sécurité**.

Les détails sont affichés.

1 - Affiche les informations détaillées pour les configurations du pare-feu d'application.

2 - Affiche les informations détaillées pour la sécurité du système. Cliquez sur chaque groupe de sécurité pour obtenir des détails sur l'état actuel et les recommandations Citrix.

3 - Affiche le résumé pour la vérification de sécurité et la violation de signature.

Vous pouvez également afficher le résumé de l'environnement de menaces en activant les **Violations de sécurité WAF** pour les serveurs virtuels, puis en accédant à **Sécurité** > **Violations de sécurité**.

Tableau de bord de sécurité unifié

Le tableau de bord **Sécurité unifiée** est un tableau de bord unique où vous pouvez configurer des protections, activer l'analyse et déployer les protections sur votre application. Dans ce tableau de bord, vous pouvez choisir parmi différentes options de modèle et effectuer l'ensemble du processus de configuration en un seul flux de travail. Pour commencer, accédez à **Sécurité > Tableau de bord de sécurité**, puis cliquez sur **Gérer l'application**. Sur la page **Gérer l'application**, vous pouvez afficher les détails de vos applications sécurisées et non sécurisées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Si vous êtes un nouvel utilisateur ou si vous n'avez configuré aucune protection, que ce soit via des StyleBooks ou directement sur des instances NetScaler®, la page suivante apparaît après avoir cliqué sur **Sécurité > Tableau de bord de sécurité**.



- Vous pouvez afficher le nombre total de serveurs virtuels qui nécessitent une protection. Cliquez sur **Démarrer** pour afficher les détails dans **Applications non sécurisées**.
- Les types de serveurs virtuels éligibles pour la configuration des protections sont l'équilibrage de charge et la commutation de contenu.

Applications sécurisées

Vous pouvez afficher les détails après avoir configuré les protections à l'aide du tableau de bord de sécurité unifié. Pour plus d'informations, consultez Configurer les protections pour les applications non sécurisées.

Si vous avez déjà configuré des protections directement sur les instances NetScaler ou via des StyleBooks, vous pouvez afficher les applications dans l'onglet **Applications sécurisées** marquées comme **Autres** sous **Profil**.



Configurer les protections pour les applications non sécurisées

REMARQUE :

Le nombre maximal d'entités de configuration (règles) prises en charge dans la liste de blocage est de 32.

Dans l'onglet **Applications non sécurisées**, sélectionnez une application, puis cliquez sur **Sécuriser l'application**.



Vous pouvez sélectionner l'une des options suivantes pour protéger votre application :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Scanner de recommandations WAF** - Cette option vous permet d'exécuter une analyse sur votre application. En fonction de certains paramètres de l'analyse, le résultat vous suggère les protections pour votre application. Vous pourriez envisager d'appliquer ces recommandations.
- **Sélectionner et personnaliser les protections** - Cette option vous permet de choisir parmi différentes options de modèle ou de personnaliser vos protections et de les déployer.

  - **OWASP Top 10** - Un modèle prédéfini qui contient les protections standard de l'industrie contre les 10 principaux risques de sécurité OWASP. Pour plus d'informations, consultez `https://owasp.org/www-project-top-ten/`.
  - **Protections CVE** - Vous pouvez créer l'ensemble de signatures à partir de la liste des règles de signature préconfigurées classées sous des catégories de vulnérabilités connues. Vous pouvez sélectionner des signatures pour configurer une action de journalisation ou de blocage lorsqu'un modèle de signature correspond au trafic entrant. Le message de journal contient les détails de la vulnérabilité.
  - **Protections personnalisées** - Sélectionnez les protections et déployez-les en fonction de vos exigences.

- **Choisir les protections existantes** - Cette option clone les protections déployées dans une application existante. Si vous souhaitez déployer ces mêmes protections sur une autre application, vous pouvez sélectionner cette option et la déployer telle quelle sur une autre application. Vous pouvez également sélectionner cette option comme modèle, modifier les protections, puis les déployer.

Scanner de recommandations WAF

REMARQUE :

- Vous ne pouvez exécuter qu'une seule analyse à la fois pour une application. Pour démarrer une nouvelle analyse pour la même application ou une application différente, vous devez attendre que l'analyse précédente soit terminée.
- Vous pouvez cliquer sur **Afficher l'historique** pour consulter l'historique et l'état des analyses précédentes. Vous pouvez également cliquer sur **Afficher le rapport**, puis appliquer les recommandations ultérieurement.

Prérequis :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'instance NetScaler doit être de version 13.0 41.28 ou ultérieure (pour les contrôles de sécurité) et 13.0 ou ultérieure (pour les signatures).
- Doit avoir la licence premium.
- Doit être le serveur virtuel d'équilibrage de charge.

Pour commencer l'analyse de recommandation WAF, vous devez fournir les informations suivantes :

1. Sous **Paramètres d'analyse** :
    - **Nom de domaine** – Spécifiez une adresse IP valide et accessible ou le nom de domaine publiquement accessible associé à l'application. Par exemple : `www.example.com`.
    - **Protocole HTTP/HTTPS** – Sélectionnez le protocole de l'application.
    - **Délai d'expiration du trafic** – Le temps d'attente (en secondes) pour une seule requête pendant l'analyse. La valeur doit être supérieure à 0.
    - **URL de début d'analyse** – La page d'accueil de l'application pour lancer l'analyse. Par exemple, `https://www.example.com/home`. L'URL doit être une adresse IPv4 valide. Si les adresses IP sont privées, vous devez vous assurer que l'adresse IP privée est accessible depuis l'IP de gestion sur site de NetScaler Console.
    - **URL de connexion** – L'URL à laquelle les données de connexion sont envoyées pour l'authentification. En HTML, cette URL est communément appelée URL d'action.
    - **Méthode d'authentification** – Sélectionnez la méthode d'authentification prise en charge (basée sur un formulaire ou basée sur un en-tête) pour votre application.
        - L'authentification basée sur un formulaire nécessite la soumission d'un formulaire à l'URL de connexion avec les informations d'identification. Ces informations d'identification doivent être sous la forme de champs de formulaire et de leurs valeurs. L'application partage ensuite le cookie de session qui est utilisé pour maintenir les sessions pendant l'analyse.
        - L'authentification basée sur un en-tête nécessite l'en-tête d'authentification et sa valeur dans la section des en-têtes. L'en-tête d'authentification doit avoir une valeur valide et est utilisé pour maintenir les sessions pendant l'analyse. Les champs de formulaire doivent être laissés vides pour l'authentification basée sur un en-tête.
    - **Méthode de requête** – Sélectionnez la méthode HTTP utilisée lors de la soumission des données de formulaire à l'URL de connexion. Les méthodes de requête autorisées sont **POST**, **GET** et **PUT**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Champs de formulaire** – Spécifiez les données de formulaire à soumettre à l'URL de connexion. Les champs de formulaire ne sont requis que si vous sélectionnez l'authentification basée sur un formulaire. Vous devez spécifier les paires clé-valeur, où **Nom du champ** est la clé et **Valeur du champ** est la valeur. Assurez-vous que tous les champs de formulaire nécessaires au bon fonctionnement de la connexion sont ajoutés correctement, y compris les mots de passe. Les valeurs sont chiffrées avant d'être stockées dans la base de données. Vous pouvez cliquer sur **Ajouter** pour ajouter plusieurs champs de formulaire. Par exemple, **Nom du champ** – nom d'utilisateur et **Valeur du champ** – admin.
- **URL de déconnexion** – Spécifiez l'URL qui met fin à la session après l'accès. Par exemple : `https://www.example.com/customer/logout`.

2. Sous **Configurations d'analyse** :

   - **Vulnérabilités à vérifier** – Sélectionnez les vulnérabilités que le scanner doit détecter. Actuellement, cela est fait pour les violations d'injection SQL et de script intersite. Par défaut, toutes les violations sont sélectionnées. Après avoir sélectionné les vulnérabilités, il simule ces attaques sur l'application pour signaler la vulnérabilité potentielle. Il est recommandé d'activer cette détection en dehors de l'environnement de production. Toutes les autres vulnérabilités sont également signalées, sans simuler ces attaques sur l'application.
   - **Limite de taille de réponse** – La limite maximale de la taille de la réponse. Toute réponse dépassant la valeur mentionnée n'est pas analysée. La limite recommandée est de 10 Mo (1000000 octets).
   - **Concurrence des requêtes** – Le nombre total de requêtes envoyées à l'application web en parallèle.

3. La configuration des paramètres d'analyse WAF est terminée. Vous pouvez cliquer sur **Démarrer l'analyse** pour lancer le processus d'analyse et attendre que la progression soit terminée. Une fois l'analyse terminée, cliquez sur **Afficher le rapport**.

   

4. Dans la page des résultats d'analyse, cliquez sur **Examiner la recommandation**.

   

5. Examinez les protections ou modifiez/ajoutez d'autres protections, puis cliquez sur **Déployer**.

   

   Lorsque vous appliquez les contrôles de sécurité avec succès :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La configuration est appliquée sur l'instance NetScaler via les StyleBooks, en fonction de la version.
  - Pour NetScaler 13.0, le StyleBook `unified-appsec-protection-130` est utilisé.
  - Pour NetScaler 13.1, le StyleBook `unified-appsec-protection-131` est utilisé.
  - Pour NetScaler 14.1, le StyleBook `unified-appsec-protection-141` est utilisé.
- Le profil `Appfw` est créé sur votre NetScaler et lié à l'application à l'aide de `policylabel`.
- Les signatures sont liées au profil appfw, si les signatures recommandées sont déjà appliquées.

REMARQUE

Les contrôles de sécurité sont pris en charge dans NetScaler 13.0 41.28 ou une version ultérieure.

Vous pouvez vérifier que les profils et signatures WAF sont appliqués via les StyleBooks par défaut en accédant à **Applications > Configuration > Packs de configuration**.



Exporter le rapport du scanner WAF

Pour exporter le rapport du scanner WAF, suivez ces étapes :

1. Accédez à **Sécurité > Tableau de bord > Gérer les applications.**
2. Dans l'onglet **Applications non sécurisées**, cliquez sur **Afficher l'historique**.
3. Sur la page **Historique des analyses**, sélectionnez l'analyse souhaitée et cliquez sur **Afficher le rapport**.
4. Sur la page **Résultats de l'analyse**, cliquez sur l'icône **Exporter**.
5. Sur la page **Exporter maintenant**, choisissez le type d'exportation.

Pour le type d'exportation **Instantané** :

1. Sélectionnez un format de fichier d'exportation : PDF, JPG ou PNG
2. Saisissez un titre pour le rapport.
3. Cliquez sur **Exporter**.



Pour le type d'exportation **Tabulaire** :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

À partir de la version 14.1 build 25.x, vous pouvez exporter le rapport du scanner WAF dans un format tabulaire.

1. Sélectionnez le format de fichier CSV.
2. Sélectionnez le nombre d'enregistrements de données à exporter à partir de la liste.
3. Saisissez un titre pour le rapport.
4. Cliquez sur **Exporter**.



Sélectionner et personnaliser les protections

OWASP TOP 10



1 - Fournit des informations sur l'application telles que l'adresse IP, le type de serveur virtuel, le type de licence, l'instance à partir de laquelle l'application est configurée, etc.

2 - Affiche le modèle sélectionné. Vous pouvez le renommer selon votre choix.

3 - Affiche les protections. Certaines protections nécessitent des informations supplémentaires.

4 - Affiche le type de journal détaillé. Vous pouvez sélectionner les options suivantes :

- **Modèle**. Enregistre uniquement le modèle de violation.
- **Charge utile du modèle**. Enregistre le modèle de violation et 150 octets de charge utile JSON supplémentaire.
- **Modèle, charge utile, en-tête**. Enregistre le modèle de violation, 150 octets de charge utile JSON supplémentaire et les informations d'en-tête HTTP.

5 - Permet d'activer le mode Moniteur. Si vous activez le mode Moniteur, le trafic est uniquement journalisé et les mesures d'atténuation ne sont pas activées.

6 - Permet d'ajouter d'autres protections. Cliquez sur **Ajouter des protections** et examinez-les pour les ajouter.

7 - Vous permet de choisir un nouveau modèle à l'aide de l'option Modifier le modèle.

8 - Vous permet de modifier ou de supprimer la protection.

9 - Active l'analyse pour les protections que vous sélectionnez. Cette option est sélectionnée par défaut. Vous pouvez afficher les analyses des protections configurées sous **Sécurité > Violations de sécurité**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir configuré les protections, cliquez sur **Déployer**.

PROTECTIONS CVE

Pour déployer les protections CVE, cliquez sur **Créer une protection CVE**. Dans la page **Créer un ensemble de signatures**, sélectionnez les signatures dans la liste pour configurer l'action de journalisation ou de blocage, puis cliquez sur **Enregistrer**.

Après avoir cliqué sur **Enregistrer**, vous pouvez afficher les signatures ajoutées à la page de configuration.

Vous pouvez également cliquer sur **Ajouter une protection** pour ajouter d'autres protections à l'application. Après avoir configuré toutes les protections, cliquez sur **Déployer**.

PROTECTION PERSONNALISÉE

Pour déployer des protections en fonction de vos besoins, cliquez sur **Créer une nouvelle protection**. Dans la page **Ajouter des protections**, sélectionnez les protections que vous souhaitez déployer et cliquez sur **Enregistrer**.

Après avoir cliqué sur **Enregistrer**, examinez les protections sélectionnées dans la page de configuration, puis cliquez sur **Déployer**.

Choisir les protections existantes

Pour déployer des protections existantes d'une application à une autre, sélectionnez une protection existante dans la liste.

Après avoir sélectionné une protection, les protections existantes sont clonées et affichées dans la page de configuration. Vous pouvez les modifier en fonction de vos besoins, puis cliquer sur **Déployer**.

Afficher les détails des violations de sécurité des applications

Les applications web exposées à Internet sont devenues drastiquement vulnérables aux attaques. NetScaler Console vous permet de visualiser les détails exploitables des violations pour protéger les applications contre les attaques. Accédez à **Sécurité** > **Violations de sécurité** pour une solution à volet unique afin de :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Visualiser les applications avec une visibilité complète sur les détails des menaces associées aux violations de sécurité WAF et aux violations de sécurité des bots
- Accéder aux violations de sécurité des applications en fonction de leurs catégories telles que **Réseau**, **Bot** et **WAF**
- Prendre des mesures correctives pour sécuriser les applications

La page **Violations de sécurité** propose les options suivantes :

- **Vue d'ensemble de l'application** – Affiche une vue d'ensemble avec les applications qui ont un nombre total de violations, un nombre total de violations WAF et Bot, des violations par pays, etc. Pour plus d'informations, consultez Vue d'ensemble de l'application.
- **Toutes les violations** – Affiche les détails des violations de sécurité des applications. Pour plus d'informations, consultez Toutes les violations.

Prérequis

Assurez-vous que le **Collecteur de métriques** est activé. Pour plus d'informations, consultez Configurer Intelligent App Analytics.

Sécurité des API

La sécurité des API de NetScaler Console offre une visibilité sur le trafic API géré par vos applications, vous aidant à analyser l'utilisation et à découvrir les points de terminaison API exposés. Les rubriques suivantes vous aident à démarrer :

- Afficher les analyses API
- Découvrir les points de terminaison API

Afficher les analyses d'API

L'analyse d'API permet une visibilité sur le trafic d'API. Cette analyse permet aux administrateurs informatiques de surveiller les instances et les points de terminaison d'API servis par une passerelle d'API. Elle fournit une surveillance périodique intégrée des requêtes d'API.

Avant de surveiller les analyses d'API, assurez-vous d'activer Web Insight sur les instances d'API. Pour plus d'informations, consultez Configurer l'analyse sur les serveurs virtuels.

Dans **API Analytics**, vous pouvez surveiller le temps de réponse des instances et des points de terminaison d'API qui sont ajoutés dans le cadre des définitions d'API. Il affiche également la bande passante consommée par les instances et les points de terminaison d'API.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Par défaut, le tableau de bord affiche les analyses d'API pour la dernière heure. Vous pouvez sélectionner une durée pour afficher les analyses d'API pour cet intervalle. Cliquez sur **Voir plus** sur chaque vignette pour afficher la liste complète. Dans cette vue, vous pouvez rechercher des instances et des points de terminaison d'API par leurs noms partiels, à l'exception de la vignette **Emplacements géographiques**.

Distribution des points de terminaison d'API

Ce graphique affiche la distribution du temps de réponse de l'application et du serveur pour les points de terminaison d'API. Vous pouvez identifier un point de terminaison d'API qui a un temps de réponse élevé et prendre les mesures nécessaires.



Les points de terminaison d'API apparaissent dans l'une des couleurs suivantes en fonction de leurs limites de temps de réponse :

- **Vert** – Si le temps de réponse est inférieur à 30 millisecondes.
- **Orange** – Si le temps de réponse est compris entre 30 et 100 millisecondes.
- **Rouge** – Si le temps de réponse est supérieur à 100 millisecondes.

Instances d'API

La vignette **Instances d'API** affiche les principales instances d'API avec un temps de réponse élevé de l'application et du serveur.



Sélectionnez une instance d'API pour afficher ses détails de performance, d'utilisation et de sécurité. L'instance d'API sélectionnée affiche les informations suivantes :

- Nombre de points de terminaison d'API
- Nombre de requêtes
- Temps de réponse de l'application et du serveur
- Bande passante consommée
- Échecs d'authentification



Points de terminaison d'API

La vignette **Points de terminaison d'API** affiche les principaux points de terminaison avec un temps de réponse élevé de l'application et du serveur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Sélectionnez un point de terminaison d'API pour afficher les détails de performance, d'utilisation et de sécurité.

Échecs d'authentification

La vignette **Échecs d'authentification** affiche les principaux points de terminaison d'API qui présentent plus d'échecs d'authentification. L'échec ou le succès de l'authentification dépend de la politique ajoutée à une définition d'API.



Si vous souhaitez afficher le taux d'échec et de succès d'authentification dans un point de terminaison d'API, procédez comme suit :

1. Sélectionnez un point de terminaison dans **Points de terminaison d'API**.
2. Sélectionnez l'onglet **Sécurité**. Cet onglet affiche les échecs et les succès d'authentification dans le point de terminaison sélectionné.



Si vous souhaitez afficher le taux d'échec et de succès d'authentification dans les points de terminaison d'API d'une instance, procédez comme suit :

1. Sélectionnez une instance dans **Instance d'API**.
2. Sélectionnez l'onglet **Sécurité**. Cet onglet affiche les échecs et les succès d'authentification dans les points de terminaison de l'instance sélectionnée.

Afficher différentes informations d'API

Naviguez dans l'analyse d'API pour afficher des informations spécifiques sur les éléments suivants :

- Principaux points de terminaison d'API dans une instance
- API les plus consultées
- Géolocalisation d'un point de terminaison
- État de la réponse HTTPS
- Tendance des requêtes API
- Consommation de bande passante d'un point de terminaison
- Erreurs et utilisation SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les principaux points de terminaison d'API dans une instance

La page **API Analytics** affiche les principaux points de terminaison qui ont un temps de réponse élevé. Si vous souhaitez afficher des points de terminaison similaires d'une instance, sélectionnez une instance dans **Instances d'API**.

La vignette **Principaux points de terminaison d'API** affiche les points de terminaison qui ont un temps de réponse d'application et de serveur élevé.



Afficher les API les plus consultées

Dans **API Analytics**, sélectionnez une instance d'API parmi les instances d'API. La vignette **API les plus consultées** affiche les principaux points de terminaison qui ont le plus de requêtes et de bande passante.



Afficher la géolocalisation d'un point de terminaison

1. Dans **API Analytics**, sélectionnez l'une des options suivantes :
   - Sélectionnez une instance dans **Instances d'API** pour afficher les emplacements d'où les points de terminaison de l'instance sélectionnée ont reçu des requêtes.
   - Sélectionnez un point de terminaison dans **Points de terminaison d'API** pour afficher les emplacements d'où le point de terminaison a reçu des requêtes.
2. Dans **Performances et utilisation**, la vignette **Géolocalisations** apparaît.

   Vous pouvez trier les emplacements en fonction du temps de réponse, de la bande passante et des requêtes.



Afficher l'état de la réponse HTTPS

La vignette **HTTPS Response Status** affiche l'état de la réponse avec ses raisons et ses occurrences. Vous pouvez afficher l'état de la réponse HTTPS de l'une des manières suivantes :

- Sélectionnez une instance dans **API Instances**.
- Sélectionnez un point de terminaison dans **API Endpoints**.

Cette vignette apparaît dans l'onglet **Performance and Usage**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher la tendance des requêtes API

Sélectionnez un point de terminaison dans **API Endpoints**. Dans **Performance and Usage**, la vignette **Total Requests** affiche la tendance du nombre total de requêtes reçues par un point de terminaison.



Si vous souhaitez afficher la tendance des requêtes abandonnées en raison d'une limite de débit, sélectionnez une instance dans **API Instances**. Dans **Security**, la vignette **Rate Limit** affiche la tendance des requêtes abandonnées. Elle affiche également la tendance du nombre total de requêtes reçues par un point de terminaison.



Grâce à cette comparaison, vous pouvez déterminer le nombre de requêtes abandonnées en raison d'une limite de débit parmi le total des requêtes.

Afficher la consommation de bande passante d'un point de terminaison

Pour afficher la tendance de consommation de bande passante par un point de terminaison, sélectionnez un point de terminaison dans les points de terminaison API. La vignette **Bandwidth** affiche un graphique de consommation de bande passante.



Afficher les erreurs et l'utilisation SSL

Sélectionnez une instance dans **Instances d'API**. Dans **Sécurité**, les vignettes suivantes apparaissent :

- **Erreurs SSL** – Affiche les échecs SSL survenus sur les clients et les serveurs d'applications.
- **Utilisation SSL** – Affiche les certificats SSL, les protocoles, les chiffrements et les forces de clé avec leurs occurrences.



Pour afficher l'utilisation SSL dans un point de terminaison, sélectionnez un point de terminaison parmi les points de terminaison d'API. La vignette **Utilisation SSL** apparaît dans l'onglet **Sécurité**.



Découvrir les points de terminaison d'API

Utilisez la sécurité des API pour afficher les points de terminaison d'API découverts dans votre organisation. NetScaler Console découvre les points de terminaison d'API en fonction du trafic API reçu sur les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans NetScaler Console, la page **Sécurité > Sécurité des API > Découverte des API** affiche les points de terminaison d'API découverts.

L'onglet **VServers** affiche les serveurs virtuels de vos instances NetScaler. Les serveurs virtuels apparaissent dans cet onglet lorsqu'ils reçoivent les requêtes API pour la période spécifiée.

REMARQUE :

Assurez-vous de configurer l'analyse et d'activer Web Insights sur les serveurs virtuels. Voir, Activer Web Insight sur les instances API.

Afficher les points de terminaison d'API

Dans **Découverte des API**, lorsque vous sélectionnez un serveur virtuel, l'interface graphique de NetScaler Console affiche les points de terminaison d'API et leurs détails, tels que :

- **Méthode** - Elle affiche la méthode utilisée dans un point de terminaison d'API. Par exemple, les méthodes `GET` et `POST`.
- **Total des requêtes** - Il affiche le nombre de requêtes API sur le point de terminaison d'API.
- **Statuts de réponse** - Il affiche le nombre pour chaque statut de réponse. Par exemple, `2xx`, `3xx`, `4xx` et `5xx`.

Les points de terminaison d'API dans un serveur virtuel sont disponibles comme suit :

☐
Vous pouvez également sélectionner le point de terminaison d'API requis pour afficher son rapport d'analyse détaillé.

☐
Pour plus d'informations sur chaque section, consultez Afficher les analyses d'API.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Passerelle

NetScaler Console fournit des analyses de passerelle qui vous donnent une visibilité sur les performances et l'expérience utilisateur du trafic servi via NetScaler Gateway. Les rubriques suivantes vous aident à surveiller et à dépanner le trafic de passerelle :

- Gateway Insight
- HDX Insight

Gateway Insight

Dans un déploiement NetScaler Gateway, la visibilité sur les détails d'accès d'un utilisateur est essentielle pour résoudre les problèmes d'échec d'accès. En tant qu'administrateur réseau, vous voulez savoir quand un utilisateur ne peut pas se connecter à NetScaler Gateway, et vous voulez connaître l'activité de l'utilisateur et les raisons de l'échec de la connexion. Ces informations ne sont généralement pas disponibles à moins que l'utilisateur n'envoie une demande de résolution.

Gateway Insight offre une visibilité sur les échecs rencontrés par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à NetScaler Gateway. Vous pouvez afficher une liste de tous les utilisateurs disponibles, le nombre d'utilisateurs actifs, le nombre de sessions actives, ainsi que les octets et les licences utilisés par tous les utilisateurs à tout moment. Vous pouvez afficher les échecs d'analyse des points d'extrémité (EPA), d'authentification, d'authentification unique (SSO) et de lancement d'applications pour un utilisateur. Vous pouvez également afficher les détails des sessions actives et terminées pour un utilisateur.

Gateway Insight offre également une visibilité sur les raisons de l'échec du lancement d'applications pour les applications virtuelles. Cela améliore votre capacité à résoudre tout type de problèmes de connexion ou d'échec de lancement d'applications. Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommée par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement pour une application.

Vous pouvez afficher le nombre de passerelles, le nombre de sessions actives, le total des octets et la bande passante utilisés par toutes les passerelles associées à une appliance NetScaler Gateway à tout moment. Vous pouvez afficher les échecs EPA, d'authentification, d'authentification

© 1997–2026 Citrix Systems, Inc. All rights reserved.

unique et de lancement d'applications pour une passerelle. Vous pouvez également afficher les détails de tous les utilisateurs associés à une passerelle et leur activité de connexion.

Tous les messages de journal sont stockés dans la base de données NetScaler Console, afin que vous puissiez afficher les détails des erreurs pour n'importe quelle période. Vous pouvez également afficher un résumé des échecs de connexion et déterminer à quelle étape du processus de connexion un échec s'est produit.

Points à noter

- Gateway Insight est pris en charge sur les déploiements suivants :
  - Access Gateway
  - Unified Gateway
- La version et la build de NetScaler Console doivent être identiques ou plus récentes que celles de l'appliance NetScaler Gateway.
- Une heure de rapports Gateway Insight peut être consultée pour les instances NetScaler avec une licence Advanced. Une licence Premium est indispensable pour consulter les rapports Gateway Insight au-delà d'une heure.

Limitations

- NetScaler Gateway ne prend pas en charge Gateway Insight lorsque la méthode d'authentification est configurée comme authentification basée sur des certificats.
- Pour les rapports Gateway Insight, les informations de géolocalisation ne sont pas fournies par l'appliance NetScaler.
- Les ouvertures de session utilisateur réussies, la latence et les détails au niveau de l'application pour les applications et bureaux ICA virtuels ne sont visibles que sur le tableau de bord des utilisateurs HDX™ Insight.
- En mode double-saut, la visibilité sur les défaillances de l'appliance NetScaler Gateway dans la deuxième DMZ n'est pas disponible.
- Les problèmes d'accès au bureau du protocole RDP (Remote Desktop Protocol) ne sont pas signalés.
- Gateway Insight prend en charge les types d'authentification suivants. Si un autre type d'authentification est utilisé, vous pourriez constater des incohérences dans Gateway Insight.
  - Local
  - LDAP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RADIUS
- TACACS
- SAML
- OTP natif
- OAuth-OpenID Connect

  Pour l'authentification OAuth-OpenID Connect, NetScaler peut agir en tant que partie de confiance (RP) OAuth-OpenID Connect ou fournisseur d'identité (IdP) OAuth-OpenID Connect. Lorsque l'authentification réussit, le nom d'utilisateur est signalé sous l'onglet Utilisateurs du rapport Gateway Insight. Cependant, vous ne pouvez pas identifier si la session a été créée au niveau de l'IdP ou du RP.

  Remarque : L'authentification OAuth-OpenID Connect est prise en charge à partir de la version 13.1 build 4.xx et ultérieure de NetScaler Console.

Activer Gateway Insight

Pour activer Gateway Insight pour votre appliance NetScaler Gateway, vous devez d'abord ajouter l'appliance NetScaler Gateway à NetScaler Console. Vous devez ensuite activer AppFlow pour le serveur virtuel représentant l'application VPN. Pour plus d'informations sur l'ajout d'un appareil à NetScaler Console, consultez la section Ajout d'appareils.

REMARQUE

Pour afficher les échecs d'analyse des points de terminaison (EPA) dans NetScaler Console, vous devez activer la journalisation du nom d'utilisateur d'authentification, d'autorisation et d'audit AppFlow sur l'appliance NetScaler Gateway.

La procédure suivante pour activer Gateway Insight est applicable si votre NetScaler Console est la version **13.0 Build 36.27** :

1. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance pour laquelle vous souhaitez activer AppFlow.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.
3. Dans la page **Configurer Insight**, sous **Configurer l'analyse**, sélectionnez **NetScaler Gateway**.
4. Sélectionnez le serveur virtuel, puis cliquez sur **Activer AppFlow**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Sur l'écran **Activer AppFlow**, dans la liste **Sélectionner une expression**, cliquez sur true.
6. À côté de **Mode de transport**, cochez la case **Logstream**.

   REMARQUE

   Vous pouvez choisir **IPFIX** ou **Logstream** comme mode de transport.

   Pour plus d'informations sur **IPFIX** et **Logstream**, consultez **Présentation de Logstream**.
7. Cliquez sur **OK**.

Pour NetScaler Console version 13.0 Build 41.x ou ultérieure

1. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance.
2. Dans la liste **Sélectionner l'action**, sélectionnez **Configurer l'analyse**.
3. Sélectionnez le serveur virtuel et cliquez sur **Activer l'analyse**.
4. Sous **Options avancées** :
   a. Sélectionnez **Logstream**
   b. Sélectionnez **NetScaler Gateway**
5. Cliquez sur **OK**.

Activer la journalisation du nom d'utilisateur pour l'authentification, l'autorisation et l'audit AppFlow sur une appliance NetScaler Gateway à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > AppFlow > Paramètres**, puis cliquez sur **Modifier les paramètres AppFlow**.
2. Dans l'écran **Configurer les paramètres AppFlow**, sélectionnez **Nom d'utilisateur AAA**, puis cliquez sur **OK**.

Affichage des rapports Gateway Insight

Dans NetScaler Console, vous pouvez afficher les rapports pour tous les utilisateurs, applications et passerelles associés aux appliances NetScaler Gateway, et vous pouvez afficher les détails pour un utilisateur, une application ou une passerelle spécifique. Dans la section **Vue d'ensemble**, vous pouvez afficher les échecs EPA, SSO, d'authentification et de lancement d'application. Vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pouvez également afficher un résumé des différents modes de session utilisés par les utilisateurs pour se connecter, les types de clients et le nombre d'utilisateurs connectés chaque heure.

REMARQUE

Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au niveau de l'application au groupe et attribuer des utilisateurs au groupe. L'analyse de NetScaler Console prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais consulter les rapports pour toutes les informations (Insights) uniquement pour les applications (serveurs virtuels) auxquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'attribution d'utilisateurs au groupe, consultez Configurer les groupes.

Pour afficher les échecs EPA, SSO, d'authentification, d'autorisation et de lancement d'application

1. Dans NetScaler Console, accédez à **Passerelle > Gateway Insight**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'utilisateur. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.
3. Cliquez sur les onglets EPA (End Point Analysis), Authentification, Autorisation, SSO (Single Sign On) ou Lancement d'application pour afficher les détails des échecs.



Pour afficher un résumé des modes de session, des clients et du nombre d'utilisateurs

Dans NetScaler Console, accédez à **Gateway > Gateway Insight**, faites défiler vers le bas pour afficher les rapports.



Affichage des rapports Gateway Insight pour les utilisateurs

Vous pouvez afficher les rapports pour :

- Tous les utilisateurs associés aux appliances NetScaler Gateway.
- Les échecs EPA, d'authentification, de SSO et de lancement d'application pour un utilisateur.
- Les détails des sessions actives et terminées pour un utilisateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Les types de modes de session tels que Full Tunnel, VPN sans client et ICA® Proxy.

Pour afficher les détails de l'utilisateur

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight > Users**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'utilisateur. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.
3. Vous pouvez afficher le nombre d'utilisateurs actifs, le nombre de sessions actives, les octets et les licences utilisés par tous les utilisateurs pendant la période.



Faites défiler vers le bas pour afficher une liste des utilisateurs disponibles et des utilisateurs actifs.



Dans l'onglet **Utilisateurs** ou **Utilisateurs actifs**, cliquez sur un utilisateur pour afficher les détails suivants :

- **Détails de l'utilisateur** - Vous pouvez afficher des informations pour chaque utilisateur associé aux appliances NetScaler Gateway. Accédez à **Gateway** > **Gateway Insight** > **Utilisateurs** et cliquez sur un utilisateur pour afficher des informations sur l'utilisateur sélectionné, telles que le mode de session, le système d'exploitation et les navigateurs.



- **Utilisateurs et applications pour la passerelle sélectionnée** - Accédez à **Gateway** > **Gateway Insight** > **Gateway** et cliquez sur un nom de domaine de passerelle pour afficher les 10 principales applications et les 10 principaux utilisateurs associés à la passerelle sélectionnée.



- **Option Afficher plus pour les applications et les utilisateurs** – Pour plus de 10 applications et utilisateurs, vous pouvez cliquer sur l'icône Plus dans Applications et Utilisateurs pour afficher tous les détails des utilisateurs et des applications associés à la passerelle sélectionnée.
- **Afficher les détails en cliquant sur le graphique à barres** – Lorsque vous cliquez sur un graphique à barres, vous pouvez afficher les détails pertinents. Par exemple, accédez à **Gateway > Gateway Insight > Gateway** et cliquez sur le graphique à barres de la passerelle pour afficher les détails de la passerelle.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Les **sessions actives** et les **sessions terminées** de l'utilisateur.

  

- Le nom de domaine de la passerelle et l'adresse IP de la passerelle dans **Sessions actives**.
- La durée de connexion de l'utilisateur.

  

- La raison de la déconnexion de l'utilisateur. Les raisons de déconnexion peuvent être :
  - Délai d'expiration de la session
  - Déconnecté en raison d'une erreur interne
  - Déconnecté en raison de l'expiration d'une session inactive
  - L'utilisateur s'est déconnecté
  - L'administrateur a arrêté la session

Affichage des rapports Gateway Insight pour les applications

Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommée par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement pour une application.

Pour afficher les détails de l'application

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight > Applications**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'application. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

Vous pouvez maintenant afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommée par les applications.



Faites défiler vers le bas pour afficher le nombre de sessions, la bande passante et le total des octets consommés par ICA et d'autres applications.



Dans l'onglet **Autres applications**, vous pouvez cliquer sur une application dans la colonne **Nom** pour afficher les détails de cette application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Affichage des rapports Gateway Insight pour les passerelles

Vous pouvez afficher le nombre de passerelles, le nombre de sessions actives, le total des octets et la bande passante utilisés par toutes les passerelles associées à une appliance NetScaler Gateway à tout moment. Vous pouvez afficher les échecs EPA, d'authentification, d'authentification unique et de lancement d'application pour une passerelle. Vous pouvez également afficher les détails de tous les utilisateurs associés à une passerelle et leur activité de connexion.

Pour afficher les détails de la passerelle

1. Dans **NetScaler Console**, accédez à **Gateway > Gateway Insight > Gateways**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de la passerelle. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

Vous pouvez maintenant afficher le nombre de passerelles, le nombre de sessions actives, le total des octets et la bande passante utilisés par toutes les passerelles associées à une appliance NetScaler Gateway à tout moment.

Faites défiler vers le bas pour afficher les détails de la passerelle tels que le nom de domaine de la passerelle, le nom du serveur virtuel, l'adresse IP NetScaler®, les modes de session et le total des octets.

Vous pouvez cliquer sur une passerelle dans la colonne **Nom de domaine de la passerelle** pour afficher les échecs EPA, d'authentification, d'authentification unique et de lancement d'application, ainsi que d'autres détails pour une passerelle.

Exportation des rapports

Vous pouvez enregistrer les rapports Gateway Insight avec tous les détails affichés dans l'interface graphique au format PDF, JPEG, PNG ou CSV sur votre ordinateur local. Vous pouvez également planifier l'exportation des rapports vers des adresses e-mail spécifiées à divers intervalles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Les utilisateurs disposant d'un accès en lecture seule ne peuvent pas exporter les rapports.
- Les rapports de carte géographique ne sont exportés que si la console NetScaler dispose d'une connectivité Internet.

Pour exporter un rapport

1. Dans l'onglet **Tableau de bord**, dans le volet de droite, cliquez sur le bouton **Exporter**.
2. Sous **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.

Pour planifier l'exportation :

1. Dans l'onglet **Tableau de bord**, dans le volet de droite, cliquez sur le bouton **Exporter**.
2. Sous **Planifier l'exportation**, spécifiez les détails et cliquez sur **Planifier**.

Pour ajouter un serveur de messagerie ou une liste de distribution de messagerie :

1. Dans l'onglet **Configuration**, accédez à **Paramètres > Notifications > E-mail**.
2. Dans le volet de droite, sélectionnez **Serveur de messagerie** pour ajouter un serveur de messagerie, ou sélectionnez **Liste de distribution de messagerie** pour créer une liste de distribution de messagerie.
3. Spécifiez les détails et cliquez sur **Créer**.

Pour exporter l'intégralité du tableau de bord Gateway Insight :

1. Sur l'onglet **Tableau de bord**, dans le volet de droite, cliquez sur le bouton **Exporter**.
2. Sous **Exporter maintenant**, sélectionnez le format **PDF**, puis cliquez sur **Exporter**.

Cas d'utilisation de Gateway Insight

Les cas d'utilisation suivants montrent comment vous pouvez utiliser Gateway Insight pour obtenir une visibilité sur les détails d'accès des utilisateurs, les applications et les passerelles sur les appliances NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un utilisateur ne peut pas se connecter à l'appliance NetScaler Gateway ou aux serveurs web internes

Vous êtes un administrateur NetScaler Gateway qui surveille les appliances NetScaler Gateway via NetScaler Console, et vous souhaitez savoir pourquoi un utilisateur ne peut pas se connecter, ou à quelle étape du processus de connexion l'échec s'est produit.

NetScaler Console vous permet d'afficher les détails des erreurs de connexion utilisateur aux étapes suivantes du processus de connexion :

- Authentification
- Analyse des points d'extrémité (EPA)
- Authentification unique

Dans NetScaler Console, vous pouvez rechercher un utilisateur particulier, puis afficher tous les détails de cet utilisateur.

Pour rechercher un utilisateur :

Dans NetScaler Console, accédez à **Gateway > Gateway Insight** et, dans la zone de texte **Rechercher des utilisateurs**, spécifiez l'utilisateur que vous souhaitez rechercher.

Échecs d'authentification

Vous pouvez afficher les erreurs d'authentification telles que des informations d'identification incorrectes ou l'absence de réponse du serveur d'authentification. Vous pouvez également voir le facteur auquel l'authentification a échoué.

Pour afficher les détails d'échec d'authentification :

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'authentification. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

   
3. Cliquez sur l'onglet **Authentification**. Vous pouvez afficher le nombre d'erreurs d'authentification à tout moment dans le graphique **Échecs**.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Faites défiler vers le bas pour afficher les détails de chaque erreur d'authentification tels que **Nom d'utilisateur, Adresse IP du client, Heure de l'erreur, Type d'authentification, Adresse IP du serveur d'authentification**, et plus encore à partir du tableau du même onglet. La colonne **Description de l'erreur** du tableau affiche la raison de l'échec de la connexion, et la colonne **État** affiche le nième facteur auquel l'échec s'est produit.

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs d'authentification et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de l'icône des paramètres.

IMPORTANT :

Si l'authentification OAuth-OpenID Connect échoue, le nom d'utilisateur est affiché comme **NA** dans le rapport Gateway Insight pour certains échecs, par exemple « Échec de la vérification du jeton ». Dans cet échec, les noms d'utilisateur ne sont pas disponibles pour l'échec d'authentification dû à « Échec de la vérification du jeton » au niveau de la partie de confiance OAuth-OpenID Connect.

Échecs EPA

Vous pouvez afficher les échecs EPA aux étapes de pré-authentification ou de post-authentification.

IMPORTANT :

NetScaler Gateway signale les échecs EPA à NetScaler Console pour les expressions classiques et avancées. Pour les expressions avancées, les noms de stratégie ne sont pas affichés dans le tableau de bord Gateway Insight. Les échecs sont signalés si l'EPA est configurée comme l'un des facteurs dans le flux d'authentification nFactor.

Pour afficher les détails des échecs EPA :

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight**.
2. Dans la section Vue d'ensemble, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs EPA. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Cliquez sur l'onglet **EPA (End Point Analysis)**. Vous pouvez afficher le nombre d'erreurs EPA à tout moment dans le graphique **Échecs**.



Faites défiler vers le bas pour afficher les détails de chaque erreur EPA tels que **Nom d'utilisateur, Adresse IP NetScaler, Adresse IP de la passerelle, VPN, Heure de l'erreur, Nom de la stratégie, Nom de domaine de la passerelle** et plus encore à partir du tableau du même onglet.

La colonne **Description de l'erreur** du tableau affiche la raison de l'échec de l'EPA. Par exemple, le message d'erreur « Échecs de la vérification de pré-authentification EPA » apparaît lorsqu'une vérification EPA échoue en raison d'échecs EPA nFactor.

La colonne **Nom de la stratégie** affiche la stratégie qui a entraîné l'échec.



Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs EPA et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas. L'ID de cas est affiché sur les entrées qui n'ont pas de nom d'utilisateur attribué si l'EPA est utilisée comme facteur dans le flux d'authentification nFactor.

REMARQUE

NetScaler Gateway ne signale pas les échecs EPA lorsque l'expression « clientSecurity » est configurée comme règle de stratégie de session VPN.

Échecs SSO

Vous pouvez afficher toutes les défaillances SSO à n'importe quelle étape pour un utilisateur accédant à des applications via l'appliance NetScaler Gateway.

Pour afficher les détails de la défaillance SSO :

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight**.
2. Dans la section Vue d'ensemble, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs SSO. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur l'onglet **SSO (Single Sign On)**. Vous pouvez afficher le nombre d'erreurs SSO à tout moment dans le graphique des défaillances.



Faites défiler vers le bas pour afficher les détails de chaque erreur SSO tels que **Nom d'utilisateur, Adresse IP NetScaler, Heure de l'erreur, Description de l'erreur, Nom de la ressource** et plus encore à partir du tableau sur le même onglet.



Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs SSO et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

Après s'être connecté avec succès à NetScaler Gateway, un utilisateur ne peut pas lancer d'application virtuelle

En cas d'échec de lancement d'application, vous pouvez obtenir une visibilité sur les raisons, telles qu'une autorité de ticket sécurisé (STA) inaccessible ou un serveur Citrix Virtual App, ou un ticket STA invalide. Vous pouvez afficher l'heure à laquelle l'erreur s'est produite, les détails de l'erreur et la ressource pour laquelle la validation STA a échoué.

Pour afficher les détails de l'échec de lancement de l'application :

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs SSO. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.



3. Cliquez sur l'onglet **Lancement d'application**. Vous pouvez afficher le nombre d'échecs de lancement d'application à tout moment dans le graphique **Échecs**.



Faites défiler vers le bas pour afficher les détails de chaque erreur de lancement d'application, tels que **Adresse IP NetScaler, Heure de l'erreur, Description de l'erreur, Nom de la ressource, Nom de domaine de la passerelle**, et plus encore, à partir du tableau du même onglet. La colonne **Description de l'erreur** du tableau affiche l'adresse IP du serveur STA et la colonne **Nom de la ressource** affiche les détails de la ressource pour laquelle la validation STA a échoué.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs de lancement d'application et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

Après avoir lancé une nouvelle application avec succès, un utilisateur souhaite afficher le nombre total d'octets et la bande passante consommés par cette application

Après avoir lancé une nouvelle application avec succès, dans NetScaler Console, vous pouvez afficher le nombre total d'octets et la bande passante consommés par cette application.

Pour afficher le nombre total d'octets et la bande passante consommés par une application :

Dans NetScaler Console, accédez à **Gateway > Gateway Insight > Applications**, faites défiler vers le bas et, sous l'onglet **Autres applications**, cliquez sur l'application pour laquelle vous souhaitez afficher les détails.

Vous pouvez afficher le nombre de sessions et le nombre total d'octets consommés par cette application.

Vous pouvez également afficher la bande passante consommée par cette application.

Un utilisateur s'est connecté à NetScaler Gateway avec succès, mais ne peut pas accéder à certaines ressources réseau dans le réseau interne

Avec Gateway Insight, vous pouvez déterminer si l'utilisateur a accès ou non aux ressources réseau. Vous pouvez également afficher le nom de la stratégie qui a entraîné l'échec.

Pour afficher l'accès utilisateur aux ressources :

1. Dans NetScaler Console, **accédez à Gateway > Gateway Insight > Applications**.
2. Sur l'écran qui apparaît, faites défiler vers le bas et, sous l'onglet **Autres applications**, sélectionnez l'application à laquelle l'utilisateur n'a pas pu se connecter.
3. Faites défiler vers le bas et, dans le tableau **Utilisateurs**, tous les utilisateurs ayant accès à cette application sont affichés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Différents utilisateurs peuvent utiliser différents déploiements de NetScaler Gateway ou se connecter à NetScaler Gateway via différents modes d'accès. L'administrateur doit pouvoir afficher les détails sur les types de déploiement et les modes d'accès

Avec Gateway Insight, vous pouvez afficher un résumé des différents modes de session utilisés par les utilisateurs pour se connecter, les types de clients et le nombre d'utilisateurs connectés chaque heure. Vous pouvez également déterminer si le déploiement d'un utilisateur est un déploiement de passerelle unifiée ou de NetScaler Gateway classique. Pour les déploiements de passerelle unifiée, vous pouvez afficher le nom et l'adresse IP du serveur virtuel de commutation de contenu, ainsi que le nom du serveur virtuel VPN.

Pour afficher le résumé des modes de session, du type de clients et du nombre d'utilisateurs connectés :

1. Dans NetScaler Console, accédez à **Gateway > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, faites défiler vers le bas pour afficher les graphiques **Mode de session, Systèmes d'exploitation, Navigateurs** et **Activité de connexion utilisateur** qui affichent les différents modes de session utilisés par les utilisateurs pour se connecter, les types de clients et le nombre d'utilisateurs connectés chaque heure.



Dépanner les problèmes de Gateway Insight

Si la solution Gateway Insight ne fonctionne pas comme prévu, le problème peut provenir de l'un des éléments suivants. Reportez-vous aux listes de contrôle des sections respectives pour le dépannage.

- Configuration de Gateway Insight.
- Problème de connectivité entre NetScaler et NetScaler Console.
- Génération d'enregistrements dans NetScaler.
- Validations dans NetScaler Console.

Liste de contrôle de la configuration de Gateway Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans l'appliance NetScaler. Pour plus de détails, consultez Activation d'AppFlow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Vérifiez la configuration de Gateway Insight dans la configuration en cours d'exécution de NetScaler.

  Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration de Gateway Insight. Assurez-vous que le type de liaison est REQUEST. Par exemple ;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Le type de liaison OTHERTCP_REQUEST est également requis pour Gateway Insight.

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type
  OTHERTCP_REQUEST
  ```

- Pour un déploiement à saut unique, Access Gateway ou Unified Gateway, assurez-vous que la politique AppFlow de Gateway Insight est liée au serveur virtuel VPN, où le trafic VPN circule. Pour plus de détails, consultez Activation de la collecte de données HDX Insight.
- Pour un double saut, Gateway Insight doit être configuré sur les deux sauts.
- Vérifiez le paramètre `appflowlog` dans le serveur virtuel NetScaler Gateway/VPN. Pour plus de détails, consultez Activation d'AppFlow pour les serveurs virtuels.

Liste de contrôle de la connectivité entre NetScaler et NetScaler Console

- Vérifiez l'état du collecteur AppFlow dans NetScaler. Pour plus de détails, consultez Comment vérifier l'état de la connectivité entre NetScaler et le collecteur AppFlow.
- Vérifiez les accès de la politique AppFlow® de Gateway Insight.

  Exécutez la commande `show appflow policy <policy_name>` pour vérifier les accès de la politique AppFlow.

  Vous pouvez également accéder à **Paramètres > AppFlow > Politiques** dans l'interface graphique pour vérifier les accès de la politique AppFlow.
- Vérifiez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Liste de contrôle de la génération d'enregistrements dans NetScaler

- Exécutez la commande `nsconmsg -d stats -g ai_tot` et vérifiez les incréments de statistiques dans NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Capturez `nstrace logs` et vérifiez les paquets CFLOW pour confirmer que NetScaler exporte les enregistrements AppFlow.

  REMARQUE :

  Les `nstrace logs` sont requis uniquement pour IPFIX. Pour Logstream, les journaux nstrace ne confirment pas si l'appliance NetScaler a exporté les enregistrements AppFlow.

Validation des enregistrements dans NetScaler Console

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` pour vérifier les journaux afin de confirmer que NetScaler Console reçoit les enregistrements AppFlow.
- Assurez-vous que l'instance NetScaler est ajoutée à NetScaler Console.
- Assurez-vous que le serveur virtuel NetScaler Gateway/VPN est sous licence dans NetScaler Console.

Validation des journaux Logstream dans NetScaler Console

La validation des données Logstream reçues par NetScaler Console peut être effectuée à l'aide des méthodes suivantes :

- **Activation de la journalisation des enregistrements de données dans NetScaler Console**

  Une fois activés, les journaux peuvent être consultés dans le fichier /var/mps/log/mps_afdecoder.log
- **Activation de la journalisation de la bibliothèque ULFD**

  Exécutez la commande `/mps/decoder_enable_debug`

  Les journaux sont capturés dans `/var/ulflog/libulfd.log`

  Vous pouvez désactiver la journalisation à l'aide de la commande `/mps/decoder_disable_debug`

Compteurs Gateway Insight

Les compteurs Gateway Insight suivants sont disponibles.

- ai_tot_preauth_epa_export

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

Enregistrements AppFlow dans le journal NetScaler

À partir de la version 13.0 build 71.x, vous pouvez vérifier les journaux NetScaler pour confirmer si les enregistrements AppFlow sont exportés. Le niveau de journalisation par défaut de `syslogparams` capture tous les journaux d'erreurs et d'informations. Si vous ne trouvez pas d'indice sur les erreurs, activez tous les niveaux de journalisation, y compris DEBUG, dans `syslogparams` pour capturer même les journaux DEBUG.

Exemples de journaux

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "GwInsight:
Sent auth record Func=ns_sslvpn_export_auth_data Username=<name>
Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid> Gwip=<ip>:443
StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<vpnfqdn> Authtype=3
EPAid=(null) AuthStage=1 AuthDuration=309 AuthAgent=<auth_server_ip>
Groupname= Policyname=<name> CurfactorPolname=<name> NextfactorPolname=
CSecExpr= Devicetype=16777219 Deviceid=0 email="

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight:
Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is zero"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight:
Func=update_session_appflow_collector pcb or session is NULL"

<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record Username=<>
Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=1 Sessid=<sessid>
Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn>
SSOAuthMethod=0 SessState=2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/
Citrix/Store

Web BackendServername= SSOurl= email="

SSO logs:
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=1 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=3 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=2 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:443 SessSeq=c
Sessid=<sessid> Gwip=<ip>:443 StatusCode=155 CSappid=0 CSAppname=(null)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
VPNfqdn=<fqdn> SSOAuthMethod=6 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

Contacter le support technique de Citrix

Pour une résolution rapide, assurez-vous de disposer des informations suivantes avant de contacter le support technique de Citrix :

- Détails du déploiement et de la topologie réseau.
- Versions de NetScaler et NetScaler Console.
- Bundle de support technique pour NetScaler et NetScaler Console.
- Capture `nstrace` pendant le problème.

Problèmes connus

Consultez les notes de publication de NetScaler pour les problèmes connus concernant Gateway Insight.

HDX™ Insight

HDX Insight offre une visibilité de bout en bout pour le trafic HDX vers Citrix Virtual Apps and Desktop passant par NetScaler. Il permet également aux administrateurs d'afficher les métriques de latence client et réseau en temps réel, les rapports historiques, les données de performance de bout en bout et de résoudre les problèmes de performance. La disponibilité des données de visibilité en temps réel et historiques permet à NetScaler Console de prendre en charge une grande variété de cas d'utilisation.

Pour que les données apparaissent, vous devez activer AppFlow sur vos serveurs virtuels NetScaler Gateway. AppFlow peut être fourni par le protocole IPFIX ou la méthode LogStream.

REMARQUE

Pour permettre l'enregistrement des calculs de temps d'aller-retour ICA®, activez les paramètres de stratégie suivants :

- Calcul du temps d'aller-retour ICA
- Intervalle de calcul du temps d'aller-retour ICA
- Calcul du temps d'aller-retour ICA pour les connexions inactives

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si vous cliquez sur un utilisateur individuel, vous pouvez voir chaque session HDX, active ou terminée, que l'utilisateur a effectuée dans la période sélectionnée. D'autres informations incluent plusieurs statistiques de latence et la bande passante consommée pendant la session. Vous pouvez également obtenir des informations sur la bande passante à partir de canaux virtuels individuels tels que l'audio, le mappage d'imprimante et le mappage de lecteur client.

REMARQUE

Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au niveau de l'application au groupe et attribuer des utilisateurs au groupe. L'analyse de NetScaler Console prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais consulter les rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) auxquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'attribution d'utilisateurs au groupe, consultez Configurer les groupes.

Vous pouvez également accéder à **Gateway > HDX Insight > Applications** et cliquer sur **Durée de lancement** pour afficher le temps nécessaire au lancement de l'application. Vous pouvez également afficher l'agent utilisateur de tous les utilisateurs connectés en accédant à **Gateway > HDX Insight > Users.**

REMARQUE

HDX Insight prend en charge les partitions d'administration configurées dans les instances NetScaler exécutant la version logicielle 12.0.

Les clients légers suivants prennent en charge HDX Insight :

- Clients légers WYSE basés sur Windows
- Clients légers WYSE basés sur Linux
- Clients légers WYSE basés sur ThinOS
- Clients légers 10ZiG basés sur Ubuntu

Identification de la cause première des problèmes de performances lentes

Scénario 1

L'utilisateur rencontre des retards lors de l'accès à Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les retards peuvent être dus à la latence sur le réseau du serveur, aux retards du trafic ICA causés par le réseau du serveur, ou à la latence sur le réseau client.

Pour identifier la cause première du problème, analysez les métriques suivantes :

- Latence WAN
- Latence DC
- Délai de l'hôte

Pour afficher les métriques client :

1. Accédez à **Gateway > HDX Insight > Users**.
2. Faites défiler vers le bas et sélectionnez le nom d'utilisateur, puis sélectionnez la période dans la liste. La période peut être d'un jour, d'une semaine, d'un mois, ou vous pouvez même personnaliser la période pour laquelle vous souhaitez afficher les données.
3. Le graphique affiche les valeurs de latence ICA RTT et DC de l'utilisateur pour la période spécifiée sous forme de graphique.

   
4. Dans le tableau **Sessions actuelles**, survolez la valeur **RTT** et notez les valeurs de délai de l'hôte, de latence du centre de données et de latence WAN.
5. Dans le tableau **Sessions actuelles**, cliquez sur le symbole du diagramme de sauts pour afficher les informations sur la connexion entre le client et le serveur, y compris les valeurs de latence.

   

Résumé

Dans cet exemple, la **latence du centre de données** est de 751 millisecondes, la **latence WAN** est de 52 millisecondes et les **délais de l'hôte** sont de 6 secondes. Cela indique que l'utilisateur subit un délai dû à une latence moyenne causée par le réseau du serveur.

Scénario 2

L'utilisateur subit un délai lors du lancement d'une application sur Citrix Virtual App ou Desktop

Le délai peut être dû à la latence sur le réseau du serveur, aux délais du trafic ICA causés par le réseau du serveur, à la latence sur le réseau client ou au temps nécessaire pour lancer une application.

Pour identifier la cause première du problème, analysez les métriques suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Latence WAN
- Latence DC
- Délai de l'hôte

Pour afficher les métriques utilisateur :

1. Accédez à **Passerelle > HDX Insight > Utilisateurs.**
2. Faites défiler vers le bas et cliquez sur le nom d'utilisateur.
3. Dans la représentation graphique, notez les valeurs de latence WAN, de latence DC et de RTT pour la session particulière.
4. Dans le tableau **Sessions actuelles**, notez que le délai de l'hôte est élevé.

   Sessions actuelles(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-7.png)

Résumé

Dans cet exemple, la **latence DC** est de 1 milliseconde, la **latence WAN** est de 12 millisecondes, mais le **délai de l'hôte** est de 517 millisecondes. Un RTT élevé avec de faibles latences DC et WAN indique une erreur d'application sur le serveur hôte.

Remarque HDX Insight affiche également davantage de métriques utilisateur, telles que la gigue WAN et les retransmissions côté serveur si vous utilisez NetScaler Console exécutant le logiciel 11.1 build 51.21 ou version ultérieure. Pour afficher ces métriques, accédez à **Gateway > HDX Insight > Users**, et sélectionnez un nom d'utilisateur. Les métriques utilisateur apparaissent dans le tableau à côté du graphique.

Utilisateurs(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-8.png)

Cartes géographiques pour HDX Insight

La fonctionnalité de cartes géographiques de NetScaler Console affiche l'utilisation des applications dans différentes zones géographiques sur une carte. Les administrateurs peuvent utiliser ces informations pour comprendre les tendances d'utilisation des applications dans diverses zones géographiques.

Vous pouvez configurer NetScaler Console pour afficher les cartes géographiques d'un emplacement géographique ou d'un réseau local particulier en spécifiant la plage d'adresses IP privées (adresse IP de début et de fin) pour cet emplacement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également afficher les détails des utilisateurs historiques et actifs à partir des cartes de géolocalisation dans HDX Insight. Accédez à **Gateway > HDX Insight**, et dans la section **Monde** de la carte, cliquez sur le pays ou la région pour lequel vous souhaitez voir les détails. Vous pouvez ensuite affiner l'affichage pour voir les informations par ville et par état.

Pour configurer une carte géographique pour les centres de données :

Accédez à **Settings > Analytics Settings > IP Blocks** pour configurer les cartes géographiques pour un emplacement particulier.

Cas d'utilisation

Considérons un scénario dans lequel l'organisation ABC possède 2 succursales, l'une à Santa Clara et l'autre en Inde.

Les utilisateurs de Santa Clara utilisent l'appliance NetScaler Gateway à SClara.x.com pour accéder au trafic VPN. Les utilisateurs indiens utilisent l'appliance NetScaler Gateway à India.x.com pour accéder au trafic VPN.

Pendant un intervalle de temps particulier, disons de 10h à 17h, les utilisateurs de Santa Clara se connectent à SClara.x.com pour accéder au trafic VPN. La plupart des utilisateurs accèdent à la même NetScaler Gateway, ce qui entraîne un délai de connexion au VPN, de sorte que certains utilisateurs se connectent à India.x.com au lieu de SClara.x.com.

Un administrateur NetScaler analysant le trafic peut utiliser la fonctionnalité de carte géographique pour afficher le trafic dans le bureau de Santa Clara. La carte montre que le temps de réponse dans le bureau de Santa Clara est élevé, car le bureau de Santa Clara ne dispose que d'une seule appliance NetScaler Gateway par laquelle les utilisateurs peuvent accéder au trafic VPN. L'administrateur pourrait donc décider d'installer une autre NetScaler Gateway, afin que les utilisateurs disposent de deux appliances NetScaler Gateway locales pour accéder au VPN.



Limitations

Si les instances NetScaler ont une licence Advanced, les seuils définis sur NetScaler Console pour HDX Insight ne seront pas déclenchés car les données analytiques ne sont collectées que pendant 1 heure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activation de la collecte de données HDX™ Insight

HDX Insight permet aux services informatiques d'offrir une expérience utilisateur exceptionnelle en offrant une visibilité de bout en bout sans précédent sur le trafic ICA qui transite par les instances NetScaler et fait partie de NetScaler Console Analytics. HDX Insight offre des capacités d'analyse des défaillances et de veille stratégique convaincantes et puissantes pour le réseau, les bureaux virtuels, les applications et l'infrastructure d'applications. HDX Insight peut à la fois trier instantanément les problèmes des utilisateurs, collecter des données sur les connexions de bureaux virtuels, générer des enregistrements AppFlow et les présenter sous forme de rapports visuels.

La configuration pour activer la collecte de données dans le NetScaler diffère selon la position de l'appliance dans la topologie de déploiement.

Activation de la collecte de données pour la surveillance des NetScaler déployés en mode utilisateur LAN

Les utilisateurs externes qui accèdent aux applications Citrix Virtual Apps and Desktops doivent s'authentifier sur le NetScaler Gateway. Les utilisateurs internes, cependant, pourraient ne pas avoir besoin d'être redirigés vers le NetScaler Gateway. De plus, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les politiques de routage afin que les requêtes soient redirigées vers l'appliance NetScaler.

Pour surmonter ces défis, et pour que les utilisateurs LAN se connectent directement aux applications Citrix Virtual Apps and Desktops, vous pouvez déployer l'appliance NetScaler en mode utilisateur LAN en configurant un serveur virtuel de redirection de cache, qui agit comme un proxy SOCKS sur l'appliance NetScaler Gateway.

REMARQUE :

NetScaler Console et l'appliance NetScaler Gateway résident dans le même sous-réseau.

Pour surveiller les appliances NetScaler déployées dans ce mode, ajoutez d'abord l'appliance NetScaler à l'inventaire NetScaler Insight, activez AppFlow, puis consultez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance NetScaler à l'inventaire NetScaler Console, vous devez activer AppFlow pour la collecte de données.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Sur une instance NetScaler, vous pouvez accéder à **Paramètres > AppFlow > Collecteurs** pour vérifier si le collecteur (c'est-à-dire NetScaler Console) est actif ou non. L'instance NetScaler envoie les enregistrements AppFlow à NetScaler Console en utilisant le NSIP. Mais l'instance utilise son SNIP pour vérifier la connectivité avec NetScaler Console. Assurez-vous donc que le SNIP est configuré sur l'instance.
- Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode utilisateur LAN en utilisant l'utilitaire de configuration de NetScaler Console.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez Référence des commandes.
- Pour des informations sur les expressions de stratégie, consultez Stratégies et expressions.

Pour configurer la collecte de données sur une appliance NetScaler à l'aide de l'interface de ligne de commande :

À l'invite de commandes, effectuez les opérations suivantes :

1. Connectez-vous à une appliance.
2. Ajoutez un serveur virtuel de redirection de cache proxy avant avec l'adresse IP et le port du proxy, et spécifiez le type de service comme HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

Exemple

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

REMARQUE :

Si vous accédez au réseau LAN à l'aide d'une appliance NetScaler Gateway, ajoutez une action à appliquer par une stratégie qui correspond au trafic VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]



add vpn trafficPolicy <name> <rule> <action>
```

Exemple

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Ajoutez NetScaler Console en tant que collecteur AppFlow sur l'appliance NetScaler.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Créez une action AppFlow® et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string>
```

Exemple :

```
add appflow action act -collectors MyInsight
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy <policyname> <rule> <action>
```

Exemple :

```
add appflow policy pol true act
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Lie la stratégie AppFlow à un point de liaison global.

```
bind appflow global <policyname> <priority> -type <type>
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

REMARQUE

La valeur de type doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA®.

7. Définissez la valeur du paramètre flowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
```

Exemple :

```
set appflow param -flowRecordInterval 60
```

8. Enregistrez la configuration. Tapez : `save ns config`

Activation de la collecte de données pour les appliances NetScaler Gateway déployées en mode saut unique

Lorsque vous déployez NetScaler Gateway en mode saut unique, il se trouve en périphérie du réseau. L'instance Gateway fournit des connexions ICA proxy à l'infrastructure de livraison de bureaux. Le mode saut unique est le déploiement le plus simple et le plus courant. Le mode saut unique assure la sécurité si un utilisateur externe tente d'accéder au réseau interne d'une organisation. En mode saut unique, les utilisateurs accèdent aux appliances NetScaler via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance NetScaler Gateway à l'inventaire de NetScaler Console et activer AppFlow sur NetScaler Console.

Pour activer la fonctionnalité AppFlow depuis NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans un navigateur web, tapez l'adresse IP de NetScaler Console (par exemple, `<http://192.168.100.1>`).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer l'analyse.
4. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.
5. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer l'analyse**.
6. Sélectionnez **HDX Insight**, puis sélectionnez **ICA**.
7. Cliquez sur **OK**.

REMARQUE

lorsque vous activez AppFlow en mode saut unique, les commandes suivantes s'exécutent en arrière-plan. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.

```
- add appflow collector <name> -IPAddress <ip_addr>

- add appflow action <name> -collectors <string>

- set appflow param -flowRecordInterval <secs>

- disable ns feature AppFlow

- enable ns feature AppFlow

- add appflow policy <name> <rule> <expression>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  set appflow policy <name> -rule <expression>


-  bind vpn vserver <vsname> -policy <string> -type <type> -priority
<positive_integer>


-  set vpn vserver <name> -appflowLog ENABLED


-  save ns config
```

Les données du canal virtuel EUEM font partie des données HDX Insight que la NetScaler Console reçoit des instances Gateway. Le canal virtuel EUEM fournit les données concernant l'ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur la NetScaler Console.

Activation de la collecte de données pour les appliances NetScaler Gateway déployées en mode double saut

Le mode double saut de NetScaler Gateway offre une protection supplémentaire au réseau interne d'une organisation, car un attaquant devrait pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé. Si vous souhaitez analyser le nombre de sauts (appliances NetScaler Gateway) par lesquels passent les connexions ICA, ainsi que les détails sur la latence de chaque connexion TCP et comment elle se compare à la latence ICA totale perçue par le client, vous devez installer NetScaler Console afin que les appliances NetScaler Gateway signalent ces statistiques vitales.



Le NetScaler Gateway de la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Ce NetScaler Gateway chiffre les connexions utilisateur, détermine comment les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Le NetScaler Gateway de la deuxième DMZ sert de périphérique proxy NetScaler Gateway. Ce NetScaler Gateway permet au trafic ICA de traverser la deuxième DMZ pour établir les connexions utilisateur avec la batterie de serveurs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La NetScaler Console peut être déployée soit dans le sous-réseau appartenant à l'appliance NetScaler Gateway de la première DMZ, soit dans le sous-réseau appartenant à l'appliance NetScaler Gateway de la deuxième DMZ. Dans l'image ci-dessus, la NetScaler Console et le NetScaler Gateway de la première DMZ sont déployés dans le même sous-réseau.

En mode double saut, NetScaler Console collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Après avoir ajouté les appliances NetScaler Gateway à l'inventaire de NetScaler Console et activé la collecte de données, chacune des appliances exporte les rapports en suivant le nombre de sauts et l'ID de chaîne de connexion.

Pour que NetScaler Console identifie quelle appliance exporte les enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances NetScaler Gateway par lesquelles le trafic circule d'un client vers les serveurs. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

NetScaler Console utilise le nombre de sauts et l'ID de chaîne de connexion pour corréler les données des deux appliances NetScaler Gateway et générer les rapports.

Pour surveiller les appliances NetScaler Gateway déployées dans ce mode, vous devez d'abord ajouter le NetScaler Gateway à l'inventaire de NetScaler Console, activer AppFlow sur NetScaler Console, puis afficher les rapports sur le tableau de bord de NetScaler Console.

Configurer HDX Insight sur les serveurs virtuels utilisés pour Optimal Gateway

Étapes pour configurer HDX Insight sur les serveurs virtuels utilisés pour Optimal Gateway :

1. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.
3. Sélectionnez le serveur virtuel VPN configuré pour l'authentification, puis cliquez sur **Activer l'analyse**.
4. Sélectionnez **HDX Insight**, puis sélectionnez **ICA**.
5. Sélectionnez d'autres options avancées si nécessaire.
6. Cliquez sur **OK**.
7. Répétez les étapes 3 à 6 sur l'autre serveur virtuel VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activer la collecte de données sur NetScaler Console

Si vous activez NetScaler Console pour commencer à collecter les détails ICA des deux appliances, les détails collectés sont redondants. C'est-à-dire que les deux appliances signalent les mêmes métriques. Pour remédier à cette situation, vous devez activer AppFlow pour ICA sur l'une des premières appliances NetScaler Gateway, puis activer AppFlow pour TCP sur la deuxième appliance. Ce faisant, l'une des appliances exporte les enregistrements AppFlow ICA et l'autre appliance exporte les enregistrements AppFlow TCP. Cela permet également de gagner du temps de traitement lors de l'analyse du trafic ICA.

Pour activer la fonctionnalité AppFlow depuis NetScaler Console :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler Console (par exemple, `<http://192.168.100.1>`).
2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer l'analyse.
4. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.
5. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer l'analyse**.
6. Sélectionnez **HDX Insight**, puis sélectionnez **ICA** ou **TCP** pour le trafic ICA ou le trafic TCP respectivement.

   REMARQUE

   Si la journalisation AppFlow n'est pas activée pour les services ou groupes de services respectifs sur l'appliance NetScaler, le tableau de bord NetScaler Console n'affiche pas les enregistrements, même si la colonne Insight indique Activé.

7. Cliquez sur **OK**.

Configuration des appliances NetScaler Gateway pour l'exportation de données

Après avoir installé les appliances NetScaler Gateway, vous devez configurer les paramètres suivants sur les appliances NetScaler Gateway pour exporter les rapports vers NetScaler Console :

- Configurez les serveurs virtuels des appliances NetScaler Gateway dans la première et la deuxième DMZ pour qu'ils communiquent entre eux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Lie le serveur virtuel NetScaler Gateway de la deuxième DMZ au serveur virtuel NetScaler Gateway de la première DMZ.
- Activez le double saut sur le NetScaler Gateway dans la deuxième DMZ.
- Désactivez l'authentification sur le serveur virtuel NetScaler Gateway dans la deuxième DMZ.
- Activez l'une des appliances NetScaler Gateway pour exporter les enregistrements ICA
- Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements TCP :
- Activez le chaînage de connexion sur les deux appliances NetScaler Gateway.

Configurer NetScaler Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel NetScaler Gateway de la première DMZ pour qu'il communique avec le serveur virtuel NetScaler Gateway de la deuxième DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON or
OFF)] [-imgGifToPng]



add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Lie le serveur virtuel NetScaler Gateway de la deuxième DMZ au serveur virtuel NetScaler Gateway de la première DMZ. Exécutez la commande suivante sur le NetScaler Gateway de la première DMZ :

```
bind vpn vserver <name> -nextHopServer <name>



bind vpn vserver vs1 -nextHopServer nh1
```

3. Activez le double saut et AppFlow sur le NetScaler Gateway de la deuxième DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
 appflowLog ( ENABLED or DISABLED )]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Désactivez l'authentification sur le serveur virtuel NetScaler Gateway de la deuxième DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]



set vpn vserver vs -authentication OFF
```

5. Activez l'une des appliances NetScaler Gateway pour exporter les enregistrements TCP.

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
OTHERTCP_REQUEST
```

6. Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements ICA :

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA_REQUEST
```

7. Activez le chaînage de connexion sur les deux appliances NetScaler Gateway :

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]



set appflow param -connectionChaining ENABLED
```

Configurer NetScaler Gateway à l'aide de l'utilitaire de configuration :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Configurez le NetScaler Gateway de la première DMZ pour qu'il communique avec le NetScaler Gateway de la deuxième DMZ et liez le NetScaler Gateway de la deuxième DMZ au NetScaler Gateway de la première DMZ.

    a. Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.

    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe Avancé, développez **Applications publiées**.

    c. Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance NetScaler Gateway.

2. Activez le double saut sur le NetScaler Gateway de la deuxième DMZ.

    a. Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.

    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.

    c. Développez plus, sélectionnez **Double saut** et cliquez sur **OK**.

3. Désactivez l'authentification sur le serveur virtuel du NetScaler Gateway dans la deuxième DMZ.

    a. Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.

    b. Dans le volet de droite, double-cliquez sur le serveur virtuel, et dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.

    c. Développez **Plus**, et décochez **Activer l'authentification**.

4. Activez l'un des dispositifs NetScaler Gateway pour exporter les enregistrements TCP.

    a. Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.

    b. Dans le volet de droite, double-cliquez sur le serveur virtuel, et dans le groupe Avancé, développez Stratégies.

    c. Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez **AppFlow**, puis dans la liste **Choisir un type**, sélectionnez **Autre requête TCP**.

    d. Cliquez sur **Continuer**.

    e. Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Activez l'autre dispositif NetScaler Gateway pour exporter les enregistrements ICA :
    a. Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
    b. Dans le volet de droite, double-cliquez sur le serveur virtuel, et dans le groupe **Avancé**, développez **Stratégies**.
    c. Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez AppFlow, puis dans la liste Choisir un type, sélectionnez **Autre requête TCP**.
    d. Cliquez sur **Continuer**.
    e. Ajoutez une liaison de stratégie, et cliquez sur **Fermer**.
6. Activez le chaînage de connexion sur les deux appliances NetScaler Gateway.
    a. Dans l'onglet **Configuration**, accédez à **Système** > **Appflow**.
    b. Dans le volet droit, dans le groupe **Paramètres**, double-cliquez sur **Modifier les paramètres Appflow**.
    c. Sélectionnez **Chaînage de connexion** et cliquez sur **OK**.
7. Configurez le NetScaler Gateway de la première DMZ pour qu'il communique avec le NetScaler Gateway de la deuxième DMZ et liez le NetScaler Gateway de la deuxième DMZ au NetScaler Gateway de la première DMZ.
    a. Dans l'onglet Configuration, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe **Avancé**, développez **Applications publiées**.
    c. Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance NetScaler Gateway.
8. Activez le double saut sur le NetScaler Gateway de la deuxième DMZ.
    a. Dans l'onglet Configuration, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
    c. Développez Plus, sélectionnez **Double saut**, et cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Désactivez l'authentification sur le serveur virtuel sur le NetScaler Gateway de la deuxième DMZ.
    a. Sous l'onglet Configuration, développez NetScaler Gateway et cliquez sur **Serveurs virtuels**.
    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
    c. Développez **Plus**, et décochez **Activer l'authentification**.
10. Activez l'un des appliances NetScaler Gateway pour exporter des enregistrements TCP.
    a. Sous l'onglet Configuration, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe Avancé, développez **Stratégies**.
    c. Cliquez sur l'icône **+** et dans la liste Choisir une stratégie, sélectionnez AppFlow, et dans la liste **Choisir le type**, sélectionnez **Autre requête TCP**.
    d. Cliquez sur **Continuer**.
    e. Ajoutez une liaison de stratégie, et cliquez sur **Fermer**.
11. Activez l'autre appliance NetScaler Gateway pour exporter des enregistrements ICA.
    a. Sous l'onglet Configuration, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
    b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe Avancé, développez **Stratégies**.
    c. Cliquez sur l'icône **+** et dans la liste **Choisir une stratégie**, sélectionnez AppFlow, et dans la liste **Choisir le type**, sélectionnez **Autre requête TCP**.
    d. Cliquez sur **Continuer**.
    e. Ajoutez une liaison de stratégie, et cliquez sur **Fermer**.
12. Activez le chaînage de connexion sur les deux appliances NetScaler Gateway.

Activer la collecte de données pour la surveillance des NetScaler déployés en mode transparent

Lorsqu'un NetScaler est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans serveur virtuel intermédiaire. Si une appliance NetScaler est déployée en mode

© 1997–2026 Citrix Systems, Inc. All rights reserved.

transparent dans un environnement Citrix Virtual Apps and Desktop, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté le NetScaler à l'inventaire de NetScaler Console, vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend de l'appareil et du mode. Dans ce cas, vous devez ajouter NetScaler Console en tant que collecteur AppFlow sur chaque appliance NetScaler, et vous devez configurer une stratégie AppFlow pour collecter tout ou partie du trafic ICA qui transite par l'appliance.

REMARQUE

- Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode transparent à l'aide de l'utilitaire de configuration de NetScaler Console.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez Référence des commandes.
- Pour plus d'informations sur les expressions de stratégie, consultez Stratégies et expressions.

La figure suivante montre le déploiement réseau d'une NetScaler Console lorsqu'un NetScaler est déployé en mode transparent :



Pour configurer la collecte de données sur une appliance NetScaler à l'aide de l'interface de ligne de commande :

À l'invite de commandes, effectuez les opérations suivantes :

1. Connectez-vous à une appliance.
2. Spécifiez les ports ICA sur lesquels l'appliance NetScaler écoute le trafic.

```
set ns param --icaPorts <port>...
```

Exemple :

```
set ns param -icaPorts 2598 1494
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Vous pouvez spécifier jusqu'à 10 ports avec cette commande.
- Le numéro de port par défaut est 2598. Vous pouvez modifier le numéro de port si nécessaire.

3. Ajoutez NetScaler Insight Center en tant que collecteur AppFlow sur l'appliance NetScaler.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

Remarque Pour afficher les collecteurs AppFlow configurés sur l'appliance NetScaler, utilisez la commande **show appflow collector**.

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string> ...
```

Exemple :

ajouter une action AppFlow act-collectors MyInsight

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy <policyname> <rule> <action>
```

Exemple :

```
add appflow policy pol true act
```

6. Lie la stratégie AppFlow à un point de liaison global.

```
bind appflow global <policyname> <priority> -type <type>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

REMARQUE

La valeur de **type** doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre flowRecordInterval pour AppFlow à 60 secondes.

```
set appflow param -flowRecordInterval 60
```

Exemple :

```
set appflow param -flowRecordInterval 60
```

8. Enregistrez la configuration. Tapez : `save ns config`

Activer la collecte de données pour les appliances NetScaler Gateway déployées en mode saut unique

Lorsque vous déployez NetScaler Gateway en mode saut unique, il se trouve en périphérie du réseau. L'instance Gateway fournit des connexions ICA proxy à l'infrastructure de livraison de bureaux. Le mode saut unique est le déploiement le plus simple et le plus courant. Le mode saut unique assure la sécurité si un utilisateur externe tente d'accéder au réseau interne d'une organisation. En mode saut unique, les utilisateurs accèdent aux appliances NetScaler via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance NetScaler Gateway à l'inventaire de NetScaler Console et activer AppFlow sur NetScaler Console.

Saut unique(/en-us/netscaler-application-delivery-management-software/media/single-hop-2.png)

Pour activer la fonctionnalité AppFlow depuis NetScaler Console :

1. Accédez à **Infrastructure** \> **Instances**, et sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Action**, sélectionnez **Activer/Désactiver Insight**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Sélectionnez les **serveurs virtuels VPN**, puis cliquez sur **Activer AppFlow®**.
4. Dans le champ **Activer AppFlow**, tapez **true**, et sélectionnez **ICA®**.
5. Cliquez sur **OK**.

REMARQUE

Lorsque vous activez AppFlow en mode saut unique, les commandes suivantes s'exécutent en arrière-plan. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

Les données du canal virtuel EUEM font partie des données HDX Insight que la console NetScaler reçoit des instances Gateway. Le canal virtuel EUEM fournit les données concernant le RTT ICA. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur la console NetScaler.

Activer la collecte de données pour surveiller les NetScaler déployés en mode transparent

Lorsqu'un NetScaler est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans serveur virtuel intermédiaire. Si un NetScaler est déployé en mode transparent dans un environnement Citrix Virtual Apps and Desktops, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté le NetScaler à l'inventaire de NetScaler Console, vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend de l'appareil et du

© 1997–2026 Citrix Systems, Inc. All rights reserved.

mode. Dans ce cas, vous devez ajouter NetScaler Console en tant que collecteur AppFlow sur chaque instance NetScaler, et vous devez configurer une stratégie AppFlow pour collecter tout ou partie du trafic ICA qui transite par l'appliance.

REMARQUE

- Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode transparent à l'aide de l'utilitaire de configuration de NetScaler Console.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez Référence des commandes.
- Pour plus d'informations sur les expressions de stratégie, consultez Stratégies et expressions.

La figure suivante montre le déploiement réseau d'une NetScaler Console lorsqu'un NetScaler est déployé en mode transparent :



Pour configurer la collecte de données sur une appliance NetScaler à l'aide de l'interface de ligne de commande :

À l'invite de commandes, effectuez les opérations suivantes :

1. Connectez-vous à une appliance.
2. Spécifiez les ports ICA sur lesquels l'appliance NetScaler écoute le trafic.

```
set ns param --icaPorts \<port\>...
```

Exemple :

```
set ns param -icaPorts 2598 1494
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Vous pouvez spécifier jusqu'à 10 ports avec cette commande.
- Le numéro de port par défaut est 2598. Vous pouvez modifier le numéro de port selon vos besoins.

3. Ajoutez NetScaler Insight Center en tant que collecteur AppFlow sur l'instance NetScaler.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

Remarque Pour afficher les collecteurs AppFlow configurés sur l'instance NetScaler, utilisez la commande **show appflow collector**.

4. Créez une action AppFlow® et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string> ...
```

Exemple :

```
add appflow action act -collectors MyInsight
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy <policyname> <rule> <action>
```

Exemple :

```
add appflow policy pol true act
```

6. Lie la stratégie AppFlow à un point de liaison global.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global <policyname> <priority> -type <type>
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

REMARQUE

La valeur de **type** doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA®.

7. Définissez la valeur du paramètre flowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
```

8. Enregistrez la configuration.

```
save ns config
```

Activer la collecte de données pour les appliances NetScaler Gateway déployées en mode double-saut

Le mode double-saut de NetScaler Gateway offre une protection supplémentaire au réseau interne d'une organisation, car un attaquant devrait pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé. Si vous souhaitez analyser le nombre de sauts (appliances NetScaler Gateway) par lesquels passent les connexions ICA, ainsi que les détails sur la latence de chaque connexion TCP et comment elle se compare à la latence ICA totale perçue par le client, vous devez installer NetScaler Console, afin que les appliances NetScaler Gateway signalent ces statistiques vitales.

Figure 3. NetScaler Console déployée en mode double-saut



Le NetScaler Gateway de la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Ce NetScaler Gateway chiffre les connexions utilisateur, détermine comment les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le NetScaler Gateway de la deuxième DMZ sert de dispositif proxy NetScaler Gateway. Ce NetScaler Gateway permet au trafic ICA de traverser la deuxième DMZ pour établir les connexions utilisateur vers la ferme de serveurs.

La NetScaler Console peut être déployée soit dans le sous-réseau appartenant à l'appliance NetScaler Gateway de la première DMZ, soit dans le sous-réseau appartenant à l'appliance NetScaler Gateway de la deuxième DMZ. Dans l'image ci-dessus, la NetScaler Console et le NetScaler Gateway de la première DMZ sont déployés dans le même sous-réseau.

En mode double-saut, NetScaler Console collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Après avoir ajouté les appliances NetScaler Gateway à l'inventaire de NetScaler Console et activé la collecte de données, chaque appliance exporte les rapports en suivant le nombre de sauts et l'ID de chaîne de connexion.

Pour que NetScaler Console identifie quelle appliance exporte les enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances NetScaler Gateway par lesquelles le trafic circule d'un client vers les serveurs. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

NetScaler Console utilise le nombre de sauts et l'ID de chaîne de connexion pour corréler les données des deux appliances NetScaler Gateway et générer les rapports.

Pour surveiller les appliances NetScaler Gateway déployées dans ce mode, vous devez d'abord ajouter le NetScaler Gateway à l'inventaire de NetScaler Console, activer AppFlow sur NetScaler Console, puis consulter les rapports sur le tableau de bord de NetScaler Console.

Activer la collecte de données sur NetScaler Console

Si vous activez NetScaler Console pour commencer à collecter les détails ICA des deux appliances, les détails collectés sont redondants. C'est-à-dire que les deux appliances signalent les mêmes métriques. Pour remédier à cette situation, vous devez activer AppFlow pour TCP sur l'une des premières appliances NetScaler Gateway, puis activer AppFlow pour ICA sur la deuxième appliance. Ce faisant, l'une des appliances exporte les enregistrements ICA AppFlow et l'autre appliance exporte les enregistrements TCP AppFlow. Cela permet également de gagner du temps de traitement lors de l'analyse du trafic ICA.

Pour activer la fonctionnalité AppFlow depuis NetScaler Console :

1. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer l'analyse.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans la liste **Action**, sélectionnez **Activer/Désactiver Insight**.
3. Sélectionnez les serveurs virtuels VPN, et cliquez sur **Activer AppFlow®**.
4. Dans le champ **Activer AppFlow**, tapez **true**, et sélectionnez **ICA/TCP** pour le trafic ICA et le trafic TCP respectivement.

   REMARQUE

   Si la journalisation AppFlow n'est pas activée pour les services ou les groupes de services sur l'appliance NetScaler, le tableau de bord NetScaler Console n'affiche pas les enregistrements, même si la colonne Insight indique Activé.

5. Cliquez sur **OK**.

Configurer les appliances NetScaler Gateway pour exporter des données

Après avoir installé les appliances NetScaler Gateway, vous devez configurer les paramètres suivants sur les appliances NetScaler Gateway pour exporter les rapports vers NetScaler Console :

- Configurez les serveurs virtuels des appliances NetScaler Gateway dans la première et la deuxième DMZ pour qu'ils communiquent entre eux.
- Lie le serveur virtuel NetScaler Gateway de la deuxième DMZ au serveur virtuel NetScaler Gateway de la première DMZ.
- Activez le double saut sur le NetScaler Gateway de la deuxième DMZ.
- Désactivez l'authentification sur le serveur virtuel NetScaler Gateway de la deuxième DMZ.
- Activez l'une des appliances NetScaler Gateway pour exporter les enregistrements ICA
- Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements TCP :
- Activez le chaînage de connexion sur les deux appliances NetScaler Gateway.

Configurer NetScaler Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel NetScaler Gateway dans la première DMZ pour communiquer avec le serveur virtuel NetScaler Gateway dans la deuxième DMZ.

   ajouter vpn nextHopServer \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure**(ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Lie le serveur virtuel NetScaler Gateway de la deuxième DMZ au serveur virtuel NetScaler Gateway de la première DMZ. Exécutez la commande suivante sur le NetScaler Gateway de la première DMZ :

   lier vpn vserver \<name\> **-nextHopServer** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. Activez le double saut et AppFlow sur le NetScaler Gateway de la deuxième DMZ.

   set vpn vserver \<name\> \[**- doubleHop** (ACTIVÉ |DÉSACTIVÉ)\] \[**-appflowLog** (ACTIVÉ |DÉSACTIVÉ)\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

4. Désactivez l'authentification sur le serveur virtuel NetScaler Gateway de la deuxième DMZ.

   set vpn vserver\<name\> \[**-authentication** (ACTIVÉ|DÉSACTIVÉ)\]

   ```
   set vpn vserver vs -authentication OFF
   ```

5. Activez l'un des appliances NetScaler Gateway pour exporter les enregistrements TCP.

   bind vpn vserver\<name\> \[**-stratégie**\<string\> **-priorité**\<positive_integer\>\] \[**-type**\<type\>\]

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
   ```

6. Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements ICA :

   bind vpn vserver\<name\> \[**-stratégie**\<string\> **-priorité**\<positive_integer\>\] \[**-type**\<type\>\]

   ```
   bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA\_REQUEST
   ```

7. Activez le chaînage de connexion sur les deux appliances NetScaler Gateway :

   définir appFlow param \[**-connectionChaining** (ENABLED|DISABLED)\]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set appflow param -connectionChaining ENABLED
```

Configuration de NetScaler Gateway à l'aide de l'utilitaire de configuration :

1. Configurez le NetScaler Gateway de la première DMZ pour qu'il communique avec le NetScaler Gateway de la deuxième DMZ et liez le NetScaler Gateway de la deuxième DMZ au NetScaler Gateway de la première DMZ.
   a. Sous l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
   b. Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe Avancé, développez **Applications publiées**.
   c. Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance NetScaler Gateway.
2. Activez le double saut sur le NetScaler Gateway de la deuxième DMZ.
   a. Sous l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
   b. Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
   c. Développez **Plus**, sélectionnez **Double saut** et cliquez sur **OK**.
3. Désactivez l'authentification sur le serveur virtuel du NetScaler Gateway de la deuxième DMZ.
   a. Sous l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
   b. Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
   c. Développez **Plus**, et décochez **Activer l'authentification**.
4. Activez l'une des appliances NetScaler Gateway pour exporter les enregistrements TCP.
   a. Sous l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.
   b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe Avancé, développez Stratégies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez **AppFlow**, et dans la liste déroulante **Choisir un type**, sélectionnez **Autre requête TCP**.

d. Cliquez sur **Continuer**.

e. Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.

5. Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements ICA :

a. Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Serveurs virtuels**.

b. Dans le volet droit, double-cliquez sur le serveur virtuel, et dans le groupe **Avancé**, développez **Stratégies**.

c. Cliquez sur l'icône + et dans la liste déroulante **Choisir une stratégie**, sélectionnez **AppFlow**, et dans la liste déroulante Choisir un type, sélectionnez **Autre requête TCP**.

d. Cliquez sur **Continuer**.

e. Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.

6. Activez le chaînage de connexion sur les deux appliances NetScaler Gateway.

a. Dans l'onglet **Configuration**, accédez à **Paramètres > Appflow**.

b. Dans le volet droit, dans le groupe **Paramètres**, cliquez sur **Modifier les paramètres Appflow**.

c. Sélectionnez **Chaînage de connexion** et cliquez sur **OK**.

Activer la collecte de données pour surveiller les NetScaler déployés en mode utilisateur LAN

Les utilisateurs externes qui accèdent aux applications Citrix Virtual App ou Desktop doivent s'authentifier sur le NetScaler Gateway. Les utilisateurs internes, cependant, pourraient ne pas avoir besoin d'être redirigés vers le NetScaler Gateway. De plus, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les politiques de routage, afin que les requêtes soient redirigées vers l'appliance NetScaler.

Pour surmonter ces défis et pour que les utilisateurs LAN se connectent directement aux applications Citrix Virtual Apps and Desktops, vous pouvez déployer l'appliance NetScaler en mode utilisateur LAN en configurant un serveur virtuel de redirection de cache, qui agit comme un proxy SOCKS sur l'appliance NetScaler Gateway.

Figure 4. NetScaler Console déployée en mode utilisateur LAN



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque L'appliance NetScaler Console et NetScaler Gateway résident dans le même sous-réseau.

Pour surveiller les appliances NetScaler déployées dans ce mode, ajoutez d'abord l'appliance NetScaler à l'inventaire NetScaler Insight, activez AppFlow, puis consultez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance NetScaler à l'inventaire NetScaler Console, vous devez activer AppFlow pour la collecte de données.

REMARQUE

- Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration NetScaler Console.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez la Référence des commandes.
- Pour des informations sur les expressions de politique, consultez Politiques et expressions.

Pour configurer la collecte de données sur une appliance NetScaler à l'aide de l'interface de ligne de commande :

À l'invite de commande, effectuez les opérations suivantes :

1. Connectez-vous à une appliance.
2. Ajoutez un serveur virtuel de redirection de cache proxy inverse avec l'adresse IP et le port du proxy, et spécifiez le type de service comme HDX.

   ```
   add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
   <cachetype>] [ - cltTimeout <secs>]
   ```

   Exemple :

   ```
   add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si vous accédez au réseau LAN à l'aide d'une appliance NetScaler Gateway, ajoutez une action à appliquer par une stratégie qui correspond au trafic VPN.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]



add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

Exemple :

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Ajoutez NetScaler Console en tant que collecteur AppFlow sur l'appliance NetScaler.

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Créez une action AppFlow® et associez le collecteur à l'action.

```
add appflow action** \<name\> **-collectors** \<string\> ...
```

Exemple :

```
add appflow action act -collectors MyInsight
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple :

```
add appflow policy pol true act
```

6. Lie la stratégie AppFlow à un point de liaison global.

```
bind appflow global** \<policyname\> \<priority\> **-type** \<type\>
```

Exemple :

```
bind appflow global pol 1 -type ICA\_REQ\_DEFAULT
```

REMARQUE

La valeur du type doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre flowRecordInterval pour AppFlow à 60 secondes.

```
set appflow param -flowRecordInterval 60
```

Exemple :

```
set appflow param -flowRecordInterval 60
```

8. Enregistrer la configuration.

```
save ns config
```

Créer des seuils et configurer des alertes pour HDX™ Insight

HDX Insight sur NetScaler Console vous permet de surveiller le trafic HDX transitant par les instances NetScaler. NetScaler Console vous permet de définir des seuils sur divers compteurs utilisés pour surveiller le trafic Insight. Vous pouvez également configurer des règles et créer des alertes dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le type de trafic HDX est associé à diverses entités telles que les applications, les bureaux, les passerelles, les licences et les utilisateurs. Chaque entité peut contenir différentes métriques qui lui sont associées. Par exemple, l'entité application est associée à divers accès, à la bande passante consommée par l'application et au temps de réponse du serveur. Une entité utilisateur peut être associée à la latence WAN, à la latence DC, à l'ICA® RTT et à la bande passante consommée par un utilisateur.

La gestion des seuils pour HDX Insight dans NetScaler Console vous permettait de créer des règles et de configurer des alertes de manière proactive chaque fois que les seuils définis étaient dépassés. Désormais, cette gestion des seuils est étendue pour configurer un groupe de règles de seuil. Vous pouvez désormais surveiller le groupe au lieu des règles individuelles. Un groupe de règles de seuil comprend une ou plusieurs règles de seuil définies par l'utilisateur pour des métriques choisies parmi des entités telles que les utilisateurs, les applications et les bureaux. Chaque règle est surveillée par rapport à une valeur attendue que vous saisissez lors de la création de la règle. Dans le cas de l'entité utilisateurs, le groupe de seuils peut également être associé à une géolocalisation.

Une alerte est générée sur NetScaler Console uniquement si toutes les règles du groupe de seuils configuré sont dépassées. Par exemple, vous pouvez surveiller une application sur le nombre total de lancements de session et également sur le nombre de lancements d'application en tant que groupe de seuils unique. Une alerte est générée uniquement si les deux règles sont dépassées. Cela vous permet de définir des seuils plus réalistes pour une entité.

Voici quelques exemples :

- Règle de seuil 1 : ICA RTT (métrique) pour les utilisateurs (entité) doit être \<= 100 ms
- Règle de seuil 2 : Latence WAN (métrique) pour les utilisateurs (entité) doit être \<= 100 ms

Un exemple de groupe de seuils peut être : {Règle de seuil 1 + Règle de seuil 2}

Pour créer une règle, vous devez d'abord sélectionner l'entité que vous souhaitez surveiller. Choisissez ensuite une métrique lors de la création d'une règle. Par exemple, vous pouvez sélectionner l'entité applications, puis sélectionner le nombre total de lancements de session ou le nombre de lancements d'applications. Vous pouvez créer une règle pour chaque combinaison d'une entité et d'une métrique. Utilisez les comparateurs fournis (\>, \<, \>= et \<=) et saisissez une valeur de seuil pour chaque métrique.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si vous ne souhaitez pas surveiller plusieurs entités dans un seul groupe, vous devez créer un groupe de règles de seuil distinct pour chaque entité.

Lorsque la valeur d'un compteur dépasse la valeur d'un seuil, NetScaler Console génère un événement pour signaler un dépassement de seuil, et une alerte est créée pour chaque événement.

Vous devez configurer la manière dont vous recevez l'alerte. Vous pouvez activer l'affichage de l'alerte sur NetScaler Console et/ou recevoir l'alerte par e-mail ou par SMS sur votre appareil mobile. Pour les deux dernières actions, vous devez configurer le serveur de messagerie ou le serveur SMS sur NetScaler Console.

Les groupes de seuils peuvent également être liés à des géolocalisations pour une surveillance géospécifique de l'entité utilisateur.

Exemples de cas d'utilisation

ABC Inc. est une entreprise mondiale qui possède des bureaux dans plus de 50 pays. L'entreprise dispose de deux centres de données, l'un à Singapour et l'autre en Californie, qui hébergent les applications et les bureaux virtuels Citrix. Les employés de l'entreprise accèdent aux applications et aux bureaux virtuels Citrix dans le monde entier à l'aide de NetScaler Gateway et de la redirection basée sur Citrix GSLB. Eric, l'administrateur des applications et des bureaux virtuels Citrix pour ABC Inc., souhaite suivre l'expérience utilisateur pour tous leurs bureaux afin d'optimiser la livraison des applications et des bureaux pour un accès partout et à tout moment. Eric souhaite également vérifier les métriques d'expérience utilisateur telles que les RTT ICA, les latences, et signaler de manière proactive toute déviation.

Les utilisateurs d'ABC Inc. ont une présence distribuée. Certains utilisateurs sont situés à proximité du centre de données, tandis que d'autres sont plus éloignés du centre de données. Comme la base d'utilisateurs est largement distribuée, les métriques et les seuils correspondants varient également d'un emplacement à l'autre. Par exemple, le RTT ICA pour un emplacement proche du centre de données peut être de 5 à 10 ms, tandis que le même pour un emplacement distant peut être d'environ 100 ms.

Grâce à la gestion des groupes de règles de seuil pour HDX Insight, Eric peut définir des groupes de règles de seuil géospécifiques pour chaque emplacement et être alerté par e-mail ou SMS en cas de dépassement par zone. Eric est également en mesure de combiner le suivi de plusieurs métriques au sein d'un groupe de règles de seuil et de réduire la cause première aux problèmes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de capacité, le cas échéant. Eric peut désormais suivre de manière proactive toute déviation sans avoir à se soucier de la complexité de l'examen manuel de toutes les métriques du portefeuille Citrix Virtual Apps and Desktops.

Pour créer un groupe de règles de seuil et configurer des alertes pour HDX Insight à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Paramètres > Paramètres d'analyse > Seuils**. Sur la page **Seuils** qui s'ouvre, cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils et des alertes**, spécifiez les détails suivants :

    a. **Nom**. Saisissez un nom pour créer un événement pour lequel NetScaler Console génère une alerte.

    b. **Type de trafic**. Dans la liste déroulante, sélectionnez HDX.

    c. **Entité**. Dans la liste déroulante, sélectionnez la catégorie ou le type de ressource. Les entités diffèrent pour chaque type de trafic que vous avez sélectionné précédemment.

    d. **Clé de référence**. Une clé de référence est automatiquement générée en fonction du type de trafic et de l'entité que vous avez sélectionnés.

    e. **Durée**. Dans la liste déroulante, sélectionnez l'intervalle de temps pendant lequel vous souhaitez surveiller l'entité. Vous pouvez surveiller les entités pendant une heure, une journée ou une semaine.

    

3. Création d'un groupe de règles de seuil pour toutes les entités :

    Pour le trafic HDX, vous devez créer une règle en cliquant sur **Ajouter une règle**. Saisissez les valeurs dans la fenêtre contextuelle **Ajouter des règles** qui s'ouvre.

    

    Vous pouvez créer plusieurs règles pour surveiller chaque entité. La création de plusieurs règles dans un seul groupe vous permet de surveiller les entités en tant que groupe de règles de seuil plutôt que des règles individuelles. Cliquez sur **OK** pour fermer la fenêtre.

    

4. Configuration du balisage de géolocalisation pour l'entité Utilisateurs

    Vous pouvez éventuellement créer une alerte basée sur la localisation pour l'entité utilisateur dans la section **Configurer les détails géographiques**. L'image suivante montre un exemple

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de création d'un balisage basé sur la géolocalisation pour surveiller les performances de latence WAN pour les utilisateurs de la côte ouest des États-Unis.



5. Cliquez sur **Activer les seuils** pour permettre à NetScaler Console de commencer à surveiller les entités.
6. Vous pouvez éventuellement configurer des actions telles que les notifications par e-mail et les notifications par SMS.
7. Cliquez sur **Créer** pour créer un groupe de règles de seuil.

Affichage des rapports et métriques HDX™ Insight

HDX Insight offre une visibilité complète des rapports et des métriques relatifs au trafic HDX sur vos instances NetScaler.

Vous pouvez afficher les métriques HDX pour toute entité sélectionnée. Les vues comprennent les catégories d'entités suivantes :

- **Utilisateurs** : Affiche les rapports pour tous les utilisateurs accédant à l'application ou au bureau virtuel Citrix dans l'intervalle de temps sélectionné.
- **Applications :** Affiche les rapports pour le nombre total d'applications, et toutes les informations pertinentes associées, telles que le nombre total de fois où les applications ont été lancées dans l'intervalle de temps spécifié.
- **Instances** : Affiche les rapports sur les instances NetScaler qui agissent comme des passerelles pour le trafic entrant.
- **Serveurs virtuels de passerelle** : Affiche les rapports pour tous les serveurs virtuels.
- **Bureaux** : Affiche les rapports pour les bureaux utilisés dans la période sélectionnée.
- **Licences** : Affiche les rapports pour le nombre total de licences SSL VPN utilisées dans le créneau horaire spécifié.

REMARQUE :

À partir de la version 14.1 build 51.x, vous pouvez surveiller les métriques clés telles que les sessions actives, les bureaux et les applications lancées au niveau du serveur virtuel VPN. Vous pouvez afficher une liste de tous les serveurs virtuels sous **Passerelle > HDX Insight > Serveurs virtuels de passerelle**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rapports et métriques de la vue utilisateur

Les rapports et métriques de cette vue sont affichés par utilisateur Citrix Virtual Apps and Desktops.

Pour accéder à la vue des utilisateurs :

1. Accédez à **Passerelle > HDX Insight > Utilisateurs**



Les rapports et métriques de la vue utilisateur comprennent les sections suivantes :

- Vue récapitulative
- Vue par utilisateur
- Vue par session utilisateur

Vue récapitulative

La vue récapitulative affiche les rapports pour tous les utilisateurs qui se sont connectés pendant la période sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs correspondantes pour la période sélectionnée, sauf indication contraire.

Pour modifier la période sélectionnée :

1. Utilisez la liste des périodes ou le curseur temporel pour définir l'intervalle de temps souhaité.
2. Cliquez sur **Accéder**.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
Sessions actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual Apps and Desktops.
Applications actives	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual App ou Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI OU CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.

RAPPORT DE SYNTHÈSE UTILISATEUR

Voici les métriques spécifiques à ce rapport.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Applications actives	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
RTT ICA	Le RTT ICA est le décalage d'affichage que l'utilisateur rencontre lorsqu'il interagit avec une application ou un bureau hébergé sur Citrix Virtual App ou Desktop respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.
Nombre total de lancements d'applications	Nombre total d'applications lancées par l'utilisateur pendant la période sélectionnée.
Total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Bureaux actifs	Nombre total de Citrix Virtual Desktops actifs pendant un intervalle de temps donné.

CANAUX

Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA® sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par octets totaux.

AGENTS UTILISATEURS

Les agents utilisateurs représentent la bande passante globale/les octets totaux consommés par chaque client d'espace de travail sous la forme d'un graphique en anneau. Chaque segment coloré du graphique représente un client d'espace de travail. La longueur du segment dépend du nombre d'utilisateurs lançant leurs applications sur ce client d'espace de travail. Vous pouvez également trier les métriques par bande passante ou par octets totaux.

Cliquez sur chaque segment pour afficher les détails des utilisateurs utilisant ce client d'espace de travail.

NOMBRE DE DÉPASSEMENTS DE SEUILS

Les métriques de nombre de dépassements de seuils représentent le nombre de seuils dépassés au cours de la période sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CARTE DU MONDE

La vue Carte du monde dans HDX Insight permet aux administrateurs d'afficher les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue globale du système, explorer un pays particulier et même des villes en cliquant simplement sur la région. Les administrateurs peuvent approfondir l'exploration pour afficher les informations par ville et par état. À partir de NetScaler Console version 12.0 et ultérieure, vous pouvez explorer les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être affichés sur la carte du monde dans HDX Insight, et la densité de chaque métrique est affichée sous la forme d'une carte thermique :

- ICA RTT
- Latence WAN
- Latence DC
- Bande passante
- Octets totaux

Carte du monde(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

Vue par utilisateur

La vue par utilisateur fournit des rapports détaillés sur l'expérience de l'utilisateur final pour tout utilisateur sélectionné.

Pour accéder aux métriques d'un utilisateur spécifique :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur web pris en charge.
2. Accédez à **Gateway > HDX Insight > Utilisateurs**.
3. Sélectionnez un utilisateur particulier dans le rapport récapitulatif des utilisateurs.

GRAPHIQUE LINÉAIRE

Le graphique linéaire affiche le résumé de toutes les métriques pour l'utilisateur sélectionné pendant la période sélectionnée.
Rapport sur les sessions actuelles/terminées
Ce rapport concerne toutes les sessions utilisateur actuelles/terminées pour l'utilisateur sélectionné. Ces métriques peuvent être triées par heure de début, reconnexions de session et nombre d'ACR.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les NetScalers, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de la session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur final.
Adresse IP du serveur	Adresse IP du serveur backend/Citrix Virtual App.
Adresse IP NetScaler	Adresse IP de gestion NetScaler (NSIP).
Type de client	Type d'espace de travail - Client Citrix Windows, etc.
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Comptes ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent de NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région depuis laquelle la session a été établie.
Ville	Ville depuis laquelle la session a été établie.
État USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où un basculement HA s'est produit.
Motif de la résiliation	Affiche le motif de la résiliation d'une session. Par exemple, Délai d'expiration de la session ICA, Session résiliée par l'utilisateur.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Citrix Virtual Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Octets totaux	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.

Prise en charge d'EDT dans HDX Insight

NetScaler Console prend désormais en charge le transport de données éclairé (EDT) pour l'affichage des analyses pour HDX Insight. Autrement dit, NetScaler Console prend désormais en charge les protocoles UDP et TCP. La prise en charge d'EDT pour NetScaler Gateway garantit une

© 1997–2026 Citrix Systems, Inc. All rights reserved.

expérience utilisateur en session haute définition des bureaux virtuels pour les utilisateurs exécutant Citrix Workspace.

HDX Insight affiche désormais le nombre de sessions EDT et de sessions non-EDT dans le cadre du rapport sur les sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. Le tableau présente des métriques telles que la latence WAN, la latence DC, les retransmissions, les RTO, et certaines de ces métriques ne sont pas disponibles pour les utilisateurs qui ont des sessions EDT car elles sont actuellement calculées à partir de la pile TCP. Par conséquent, elles apparaissent comme « NA ».

Un nouveau graphique en anneau a été introduit pour vous permettre de visualiser la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.

REMARQUE

EDT dans HDX Insight est pris en charge sur NetScaler Console à partir de la version 12.1 build 50.28 et est disponible sur les instances ADC à partir de la version 12.1 build 49.23.

Métriques HDX Insight disponibles à partir de NetScaler Console 12.0 et versions ultérieures :

LATENCE CÔTÉ CLIENT L7	LA LATENCE L7 MOYENNE OBSERVÉE ENTRE LE CLIENT ICA ET L'INSTANCE NETSCALER. CETTE MÉTRIQUE EST UTILE EN CAS DE PRÉSENCE DE PÉRIPHÉRIQUES NON-CITRIX DANS LE CHEMIN DE LIVRAISON.
Latence côté serveur L7	La latence L7 moyenne observée entre le périphérique NetScaler et l'application virtuelle Citrix. Cette métrique est utile en cas de présence de périphériques non-Citrix dans le chemin de livraison.
Latence de violation maximale	La valeur la plus élevée de la latence L7 lorsqu'une violation d'un seuil défini pour un intervalle de temps donné se produit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LATENCE CÔTÉ CLIENT L7	LA LATENCE L7 MOYENNE OBSERVÉE ENTRE LE CLIENT ICA ET L'INSTANCE NETSCALER. CETTE MÉTRIQUE EST UTILE EN CAS DE PRÉSENCE DE PÉRIPHÉRIQUES NON-CITRIX DANS LE CHEMIN DE LIVRAISON.
Latence moyenne de violation	La valeur moyenne de la latence L7 lorsque le système est dans un état de « latence L7 violée ».
Nombre de violations de seuil L7	Le nombre de fois qu'une violation de seuil L7 s'est produite.



UTILISATEURS DE BUREAU

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces métriques peuvent être triées par Nombre de lancements de bureau et Bande passante.

MÉTRIQUES	DESCRIPTION
Nom	Nom du Citrix Virtual Desktop.
Nombre de lancements de bureau	Nombre de fois que le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergé respectivement sur Citrix Virtual App ou Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utilisateurs de bureau(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)
Applications
Un graphique à barres représentant les applications triées par Actif, nombre total de lancements de session, nombre total de lancements d'applications et durée de lancement.

Graphique d'applications(/en-us/netscaler-application-delivery-management-software/media/hdx-application-graph.png)
Instances
Un graphique à barres représentant les instances NetScaler triées par Actif et applications totales.

Instances(/en-us/netscaler-application-delivery-management-software/media/hdx-instances-graph.png)
Canaux
Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par octets totaux.

Agents utilisateurs
Les agents utilisateurs représentent la bande passante globale/le nombre total d'octets consommés par chaque point d'extrémité sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par octets totaux.

VUE DE SESSION PAR UTILISATEUR

La vue de session par utilisateur fournit des rapports pour la session d'un utilisateur sélectionné en particulier.

Pour afficher les métriques d'une session utilisateur sélectionnée :

1. Accédez à **Gateway > HDX Insight > Utilisateurs**.
2. Sélectionnez un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
3. Sélectionnez une session dans la colonne **Sessions actuelles** ou **Sessions terminées**.

Graphique chronologique

MÉTRIQUES	DESCRIPTION
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nombre de sessions ACR	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
RTT ICA	Le RTT ICA est le décalage d'écran que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.

Application active

La section **Applications actives** affiche les applications actives de l'utilisateur sélectionné. Ces applications peuvent également être triées par nombre de sessions actives et durées de lancement.

Sessions associées

La section Sessions associées affiche les sessions associées aux sessions de l'utilisateur sélectionné. La relation peut être sélectionnée comme serveurs communs ou NetScaler commun.

Rapports et métriques de la vue Application

Les rapports et métriques de cette vue sont axés sur les applications virtuelles Citrix.

Pour accéder à la vue Application :

1. Accédez à **Gateway > HDX Insight > Applications**.

Vue récapitulative

La vue récapitulative affiche les rapports pour toutes les applications qui sont connectées pendant la période sélectionnée.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs correspondantes pour la période sélectionnée.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions	Nombre total de sessions pendant un intervalle de temps donné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Durée de lancement	Temps moyen nécessaire pour lancer une application.

RAPPORT RÉCAPITULATIF DES APPLICATIONS

MESURES	DESCRIPTION
Nom	Nom de l'application virtuelle Citrix.
Nombre total de lancements de session	Nombre total de sessions d'applications virtuelles Citrix actives pendant l'intervalle de temps donné.
Nombre total de lancements d'applications	Nombre total d'applications virtuelles Citrix lancées pendant l'intervalle de temps donné.
Durée de lancement	Temps moyen nécessaire pour lancer l'application virtuelle Citrix.

RAPPORT SUR LES APPLICATIONS ACTIVES

MÉTRIQUES	DESCRIPTION
Nom	Nom de l'application virtuelle Citrix.
État	Affiche l'état de l'application : Vert-Actif, Rouge-Inactif
#Sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
#Applications actives	Nombre de sessions actives pour cette application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Application pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual Apps and Desktops.
Durée de lancement	Temps moyen nécessaire pour lancer une application.

RAPPORT DES SESSIONS ACTUELLES

MÉTRIQUES	DESCRIPTION
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les NetScalers, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur final.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Adresse IP du serveur	IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type d'espace de travail - Client Citrix Windows et ainsi de suite
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nombre d'ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région depuis laquelle la session a été établie.
Ville	Ville depuis laquelle la session a été établie.
État USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où un basculement HA s'est produit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Motif de la terminaison	Affiche le motif de la terminaison d'une session. Par exemple, délai d'expiration de la session ICA, session terminée par l'utilisateur.
RTT ICA	Le RTT ICA est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI ou CVAD ou StoreFront.
Total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
RTO rapide côté client	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Nom d'utilisateur	Le nom d'utilisateur de l'utilisateur accédant à cette application virtuelle Citrix particulière.
ID de session	Identifiant unique pour la session de l'application virtuelle Citrix.
Type de session	Sera « Application ».
État	État de la session : Vert pour actif, Rouge pour inactif.
Latence de violation maximale	La valeur la plus élevée de la latence L7 lorsqu'une violation d'un seuil défini pour un intervalle de temps donné se produit.
Latence de violation moyenne	La valeur moyenne de la latence L7 lorsque le système est dans un état de « latence L7 violée ».
Nombre de violations de seuil L7	Le nombre de fois qu'une violation de seuil L7 s'est produite.
Latence L7 côté client	La latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Cette métrique est utile en cas de présence de périphériques non-Citrix dans le chemin de livraison.
Latence L7 côté serveur	La latence L7 moyenne observée entre l'appliance NetScaler et l'application virtuelle Citrix. Cette métrique est utile en cas de présence de périphériques non-Citrix dans le chemin de livraison.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vue de session par application

La vue par session d'application affiche les rapports pour une session d'application sélectionnée en particulier.

Pour afficher les rapports de session :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Gateway > HDX Insight > Applications**.
3. Sélectionnez un utilisateur particulier dans le rapport récapitulatif de l'application.
4. Session sélectionnée à partir du rapport des sessions actuelles.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
Reconnexions de session	Nombre de fois où la session a été reconnectée.
Comptes ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.



GRAPHIQUE À BARRES DE L'UTILISATEUR

Le graphique à barres de l'utilisateur représente les utilisateurs connectés à cette application particulière.



Rapports et métriques de la vue Bureau

Les rapports et métriques de cette vue sont axés sur les Citrix Virtual Desktops.

Pour accéder à la vue Bureau :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Gateway > HDX Insight > Desktop**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vue d'ensemble

La vue récapitulative affiche les rapports pour tous les bureaux virtuels Citrix connectés pendant la période sélectionnée.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs correspondantes pour la période sélectionnée.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions actives Citrix Virtual Apps and Desktops.
# Applications actives	Ce nombre indique le nombre de sessions d'applications virtuelles Citrix actives.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.

RAPPORT RÉCAPITULATIF DU BUREAU

MÉTRIQUES	DESCRIPTION
Sessions actives	Nombre total de sessions Citrix Virtual Desktop actives pendant un intervalle de temps donné.
Bureaux actifs	Nombre total de bureaux virtuels Citrix actifs pendant un intervalle de temps donné.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.

RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Bureau pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

Vue par bureau

La vue par bureau fournit des rapports détaillés sur l'expérience utilisateur final pour un bureau virtuel Citrix sélectionné.

Pour accéder à la vue Bureau spécifique :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics \> HDX Insight \> Bureau**.
3. Sélectionnez un **Bureau** spécifique dans le **Rapport récapitulatif des bureaux**.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
# Applications actives	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI ou CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.



RAPPORT SUR LES UTILISATEURS DE BUREAU

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces métriques peuvent être triées par nombre de lancements de bureau et bande passante.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nom	Nom du Citrix Virtual Desktop.
Nombre de lancements de bureau	Nombre de fois où le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.

RAPPORT SUR LES BUREAUX UTILISATEUR ACTIFS/INACTIFS

Ces métriques suivantes peuvent être triées par bande passante par intervalle, reconnexions de session et nombres ACR.

MÉTRIQUES	DESCRIPTION
ID de session	Identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les NetScalers, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Bande passante de la session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur final.
Adresse IP du serveur	Adresse IP du serveur backend/Citrix Virtual App.
Adresse IP NetScaler	Adresse IP de gestion NetScaler (NSIP).
Type de client	Type d'espace de travail - Client Citrix Windows, etc.
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session a été reconnectée.
Nombre d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent de NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région depuis laquelle la session a été établie.
Ville	Ville depuis laquelle la session a été établie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
État USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où un basculement HA s'est produit.
Motif de la terminaison	Affiche le motif de la terminaison d'une session. Par exemple, Délai d'expiration de la session ICA, Session terminée par l'utilisateur.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergés respectivement sur Citrix Virtual Apps et Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Total d'octets	Total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
	fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Nom de l'image VDI	Nom du bureau virtuel Citrix auquel l'utilisateur est connecté
Diagramme	



Vue par session de bureau

La vue par session de bureau fournit des rapports pour une session de bureau virtuel Citrix sélectionnée en particulier.

Pour accéder à la vue de session de bureau :

1. Connectez-vous à votre console NetScaler à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics \> HDX Insight \> Desktop**.
3. Sélectionnez un bureau particulier dans le **rapport récapitulatif du bureau**.
4. Sélectionnez une session dans le rapport des sessions actuelles.

GRAPHIQUE CHRONOLOGIQUE

La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné en particulier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour afficher les métriques d'une session utilisateur sélectionnée :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur web pris en charge.
2. Accédez à **Gateway > HDX Insight > Users**.
3. Sélectionnez un utilisateur particulier dans la section **Rapport récapitulatif des utilisateurs**.
4. Sélectionnez une session dans la colonne **Sessions actuelles** ou **Sessions terminées**.

MÉTRIQUES	DESCRIPTION
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Comptes ACR	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI ou CVAD ou StoreFront.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.



RAPPORT DES SESSIONS DE BUREAU ASSOCIÉES

Les métriques suivantes peuvent être triées par bande passante par intervalle, reconnexions de session et nombre d'ACR.

MÉTRIQUES	DESCRIPTION
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen dans le trafic ICA qui transite par les NetScalers, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de la session	La bande passante consommée par la session, quel que soit l'intervalle de temps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur.
Adresse IP du serveur	Adresse IP du serveur principal/Citrix Virtual App.
Adresse IP NetScaler	Adresse IP de gestion NetScaler (NSIP).
Type de client	Type d'espace de travail - Client Citrix Windows, etc.
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session a été reconnectée.
Comptes ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent de NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région à partir de laquelle la session a été établie.
Ville	Ville à partir de laquelle la session a été établie.
État USB	Actif/Inactif - Vert/Rouge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Raison de la résiliation	Affiche la raison de la résiliation d'une session. Par exemple, délai d'expiration de la session ICA, session terminée par l'utilisateur.
RTT ICA	Le RTT ICA est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.

Rapports et métriques de la vue d'instance

Les rapports et les métriques de la vue d'instance sont axés sur les instances NetScaler.

Pour accéder à la vue d'instance :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics \> HDX Insight \> Instances**.

Les rapports et les métriques de la vue d'instance se composent des sections suivantes :

- Vue récapitulative de l'instance
- Vue par instance

Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports pour toutes les instances NetScaler ajoutées à NetScaler Console.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs correspondantes pour la période sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GRAPHIQUE À BARRES D'INSTANCE

Ce graphique affiche l'instance par rapport au nombre total de lancements de session | Applications totales, qui peuvent être sélectionnées dans la liste en haut à droite sur la zone du graphique.



RAPPORT RÉCAPITULATIF DES INSTANCES/INSTANCES ACTIVES

MÉTRIQUES	DESCRIPTION
Nom	Nom d'hôte de l'instance NetScaler.
Adresse IP	Adresse IP NetScaler.
Nombre total de lancements de session	Nombre total de sessions utilisateur uniques créées pendant un intervalle de temps donné.
Applications totales	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.
Type	N/A



RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Instance dans la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

FLUX IGNORÉS

Un flux ignoré est un enregistrement qui n'a pas pu analyser la connexion ICA. Cela peut se produire pour plusieurs raisons, telles que l'utilisation de versions non prises en charge de Citrix Virtual Apps and Desktops, une version ou un type d'espace de travail non pris en charge, etc. Ce tableau affiche l'adresse IP et le nombre de flux ignorés. Ces espaces de travail peuvent ne pas faire partie des espaces de travail autorisés. Par conséquent, ces sessions sont ignorées de la surveillance.



VUE MONDIALE

La vue Carte du monde dans HDX Insight permet aux administrateurs d'afficher les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir

© 1997–2026 Citrix Systems, Inc. All rights reserved.

une vue mondiale du système, explorer un pays particulier et même des villes en cliquant simplement sur la région. Les administrateurs peuvent ensuite explorer davantage pour afficher les informations par ville et par état. À partir de NetScaler Console version 12.0 et ultérieure, vous pouvez explorer les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être affichés sur la Carte du monde dans HDX Insight, et la densité de chaque métrique est affichée sous la forme d'une carte thermique :

- ICA RTT
- Latence WAN
- Latence DC
- Bande passante
- Total d'octets



Vue par instance

La vue par instance fournit des rapports détaillés sur l'expérience utilisateur final pour une instance NetScaler sélectionnée.

Pour accéder à la vue par instance :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur web pris en charge.
2. Accédez à **Analytics \> HDX Insight \> Instances**.
3. Sélectionnez une instance particulière dans le **Rapport récapitulatif des instances**.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
Adresse IP	Ceci représente l'adresse IP NetScaler de l'instance sélectionnée.
Nombre total de lancements de session	Nombre total de sessions actives de Citrix Virtual App pendant l'intervalle de temps donné.
Total des applications	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

GRAPHIQUE À BARRES DES APPLICATIONS

Affiche les 5 principales applications en fonction des critères suivants : applications actives, nombre total de lancements de session, nombre total de lancements d'applications ou durée de lancement.



GRAPHIQUE À BARRES DES UTILISATEURS

Le graphique à barres des utilisateurs affiche les 5 principaux utilisateurs en fonction des critères suivants

- Bande passante
- Latence WAN
- Latence DC
- ICA RTT



RAPPORT SUR LES UTILISATEURS DE BUREAU

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces métriques peuvent être triées par Nombre de lancements de bureau et Bande passante.

MÉTRIQUES	DESCRIPTION
Nom	Nom du Citrix Virtual Desktop.
Nombre de lancements de bureau	Nombre de fois où le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, entre NetScaler Gateway et les serveurs VDI ou CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergé

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
	respectivement sur Citrix Virtual Apps and Desktops.

VUE MONDIALE

La vue Carte du monde dans HDX Insight permet aux administrateurs de consulter les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue mondiale du système, explorer un pays particulier et même des villes en cliquant sur la région. Les administrateurs peuvent ensuite explorer les informations par ville et par état. À partir de NetScaler Console version 12.0 et ultérieure, vous pouvez explorer les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être consultés sur la Carte du monde dans HDX Insight, et la densité de chaque métrique est affichée sous forme de carte thermique :

- ICA RTT
- Latence WAN
- Latence DC
- Bande passante
- Total d'octets

Rapports et métriques de la vue des licences

La vue des licences fournit des détails sur les informations de licence de NetScaler Gateway.

Pour naviguer vers la vue Licence :

1. Connectez-vous à votre NetScaler Console à l'aide d'un navigateur web pris en charge.
2. Accédez à **Analytics \> HDX Insight \> Licenses**.

Graphique linéaire

MÉTRIQUES	DESCRIPTION
Licences utilisées	Les licences CCU NetScaler Gateway utilisées pendant la période sélectionnée. Chaque décompte représente le nombre de sessions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
	utilisateur. Ceci est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences CCU NetScaler Gateway disponibles pour le client.



RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Licence pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

Rapports et métriques de la vue Application

Les rapports et métriques de cette vue sont axés sur les applications virtuelles Citrix.

Pour accéder à la vue Application :

1. Accédez à **Gateway > HDX™ Insight > Applications**.

Vue récapitulative

La vue récapitulative affiche les rapports pour toutes les applications connectées pendant la période sélectionnée.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, afficheront les valeurs correspondantes pour la période sélectionnée.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions	Nombre total de sessions pendant un intervalle de temps donné.
Durée de lancement	Temps moyen nécessaire pour lancer une application.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

RAPPORT RÉCAPITULATIF DES APPLICATIONS

MÉTRIQUES	DESCRIPTION
Nom	Nom de l'application virtuelle Citrix.
Nombre total de lancements de sessions	Nombre total de sessions d'applications virtuelles Citrix actives pendant l'intervalle de temps donné.
Nombre total de lancements d'applications	Nombre total d'applications virtuelles Citrix lancées pendant l'intervalle de temps donné.
Durée de lancement	Temps moyen nécessaire pour lancer l'application virtuelle Citrix.



RAPPORT SUR LES APPLICATIONS ACTIVES

MÉTRIQUES	DESCRIPTION
Nom	Nom de l'application virtuelle Citrix.
État	Affiche l'état de l'application : Vert-Actif, Rouge-Inactif
#Sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
#Applications actives	Nombre de sessions actives pour cette application.



RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Application pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Durée de lancement	Temps moyen nécessaire pour lancer une application.

RAPPORT DES SESSIONS ACTUELLES

MÉTRIQUES	DESCRIPTION
ID de session	Identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les NetScalers, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de la session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur.
Adresse IP du serveur	Adresse IP du serveur backend/Citrix Virtual App.
Adresse IP de NetScaler	IP de gestion NetScaler (NSIP).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Type de client	Type d'espace de travail - Client Citrix Windows, etc.
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Comptes ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région à partir de laquelle la session a été établie.
Ville	Ville à partir de laquelle la session a été établie.
État USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où un basculement HA s'est produit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Raison de la résiliation	Affiche la raison de la résiliation d'une session. Par exemple, expiration de la session ICA, session terminée par l'utilisateur.
RTT ICA	Le RTT ICA est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Total d'octets	Total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Nom d'utilisateur	Le nom d'utilisateur de l'utilisateur accédant à cette application virtuelle Citrix particulière.
ID de session	Identifiant unique pour la session de l'application virtuelle Citrix.
Type de session	Sera « Application ».
État	État de la session : Vert pour actif, Rouge pour inactif.
Latence de violation maximale	La valeur la plus élevée de la latence L7 lorsqu'une violation d'un seuil défini pour un intervalle de temps donné se produit.
Latence de violation moyenne	La valeur moyenne de la latence L7 lorsque le système est dans un état de « latence L7 violée ».
Nombre de violations de seuil L7	Le nombre de fois qu'une violation de seuil L7 s'est produite.
Latence L7 côté client	La latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Cette métrique est utile lorsque des périphériques non-Citrix sont présents dans le chemin de livraison.
Latence L7 côté serveur	La latence L7 moyenne observée entre le périphérique NetScaler et l'application virtuelle Citrix. Cette métrique est utile lorsque des périphériques non-Citrix sont présents dans le chemin de livraison.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

VUE DE SESSION PAR APPLICATION

La vue de session par application affiche les rapports pour une session d'application sélectionnée en particulier.

Pour afficher les rapports de session :

1. Accédez à **Gateway > HDX Insight > Applications**.
2. Sélectionnez un utilisateur spécifique à partir du rapport récapitulatif des applications.
3. Session sélectionnée à partir du rapport des sessions actuelles.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nombre d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergés respectivement sur Citrix Virtual Apps et Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
	pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur back-end.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.

GRAPHIQUE À BARRES DES UTILISATEURS

Le graphique à barres des utilisateurs représente les utilisateurs connectés à cette application particulière.

Rapports et métriques de la vue Bureau

Les rapports et les métriques de cette vue sont axés sur les bureaux virtuels Citrix.

Pour accéder à la vue Bureau :

1. Accédez à **Gateway > HDX™ Insight > Bureau**.

Vue d'ensemble

La vue d'ensemble affiche les rapports pour tous les bureaux virtuels Citrix connectés pendant la période sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs correspondantes pour la période sélectionnée.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
# Applications actives	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
ICA RTT	L'ICA RTT est le délai d'affichage que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
RTO rapide côté serveur	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et le serveur back-end.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.



RAPPORT RÉCAPITULATIF DU BUREAU

MÉTRIQUES	DESCRIPTION
Sessions actives	Nombre total de sessions Citrix Virtual Desktop actives pendant un intervalle de temps donné.
Bureaux actifs	Nombre total de Citrix Virtual Desktops actifs pendant un intervalle de temps donné.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps et Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence du DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Total d'octets	Total d'octets consommés par l'utilisateur pendant la période sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Bureau pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes.

Vue par bureau

La vue par bureau fournit des rapports détaillés sur l'expérience utilisateur final pour un bureau virtuel Citrix sélectionné.

Pour accéder à la vue Bureau particulière :

1. Accédez à **Analytics \> HDX Insight \> Desktop**.
2. Sélectionnez un **Bureau** particulier dans le **Rapport récapitulatif des bureaux**.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual Apps and Desktops.
# Applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.

RAPPORT DES UTILISATEURS DE BUREAU

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces métriques peuvent être triées par Nombre de lancements de bureau et Bande passante.

MÉTRIQUES	DESCRIPTION
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements du bureau	Nombre de fois où le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
RTT ICA	Le RTT ICA est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps et Desktops.

RAPPORT SUR LES BUREAUX UTILISATEUR ACTIFS/INACTIFS

Ces métriques peuvent être triées par bande passante par intervalle, reconnexions de session et nombre d'ACR.

MÉTRIQUES	DESCRIPTION
ID de session	Identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les instances NetScaler, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur.
Adresse IP du serveur	Adresse IP du serveur principal/Citrix Virtual App.
Adresse IP NetScaler	Adresse IP de gestion NetScaler (NSIP).
Type de client	Type d'espace de travail - Client Citrix Windows, etc.
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session a été reconnectée.
Comptes ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent de NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région depuis laquelle la session a été établie.
Ville	Ville depuis laquelle la session a été établie.
État USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où un basculement HA s'est produit.
Raison de la terminaison	Affiche la raison de la terminaison d'une session. Par exemple, Délai d'expiration de la session ICA, Session terminée par l'utilisateur.
ICA RTT	L'ICA RTT est le délai d'affichage que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Total d'octets	Total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
RTO rapide côté client	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Nom de l'image VDI	Nom du bureau virtuel Citrix auquel l'utilisateur est connecté
Diagramme	



Vue par session de bureau

La vue par session de bureau fournit des rapports pour une session de bureau virtuel Citrix particulière sélectionnée.

Pour accéder à la vue par session de bureau :

1. Accédez à **Gateway > HDX Insight > Desktop**.
2. Sélectionnez un bureau particulier à partir du **Rapport récapitulatif du bureau**.
3. Sélectionnez une session à partir du rapport des sessions actuelles.

GRAPHIQUE CHRONOLOGIQUE

La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné en particulier.

Pour afficher les métriques d'une session utilisateur sélectionnée :

1. Accédez à **Gateway > HDX Insight > Users**.
2. Sélectionnez un utilisateur particulier dans la section **User Summary Report**.
3. Sélectionnez une session dans la colonne **Current Sessions** ou **Terminated Sessions**.

MÉTRIQUES	DESCRIPTION
Reconnexions de session	Ce nombre indique le nombre de sessions actives de Citrix Virtual App et Desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nombre d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual App et Desktop.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence du DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.

RAPPORT DES SESSIONS DE BUREAU ASSOCIÉES

Les métriques suivantes peuvent être triées par bande passante par intervalle, reconnexions de session et nombre d'ACR.

MÉTRIQUES	DESCRIPTION
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les NetScalers, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de la session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Adresse IP NetScaler	Adresse IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Citrix Windows, etc.
Version du client	Version du Receiver.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Comptes ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent NetScaler Gateway.
Pays	Pays depuis lequel la session a été établie.
Région	Région depuis laquelle la session a été établie.
Ville	Ville depuis laquelle la session a été établie.
État USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Raison de la terminaison	Affiche la raison de la terminaison d'une session. Par exemple, délai d'expiration de la session ICA, session terminée par l'utilisateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
RTT ICA	Le RTT ICA est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur back-end.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.
RTO rapide côté serveur	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nom de l'image VDI	Nom du bureau virtuel Citrix auquel l'utilisateur est connecté

Rapports et métriques de la vue Utilisateur

Les rapports et métriques de cette vue sont affichés par utilisateur Citrix Virtual Apps™ et Desktop.

Pour accéder à la vue Utilisateurs :

1. Accédez à **Gateway > HDX™ Insight > Utilisateurs**

   Métriques utilisateur(/en-us/netscaler-application-delivery-management-software/media/analytics-hgx-users-graph.png)

Vue récapitulative

La vue récapitulative affiche les rapports pour tous les utilisateurs qui se sont connectés pendant la période sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs correspondantes pour la période sélectionnée, sauf indication contraire.

Pour modifier la période sélectionnée :

1. Utilisez la liste des périodes ou le curseur temporel pour définir l'intervalle de temps souhaité.
2. Cliquez sur **Go**.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual App et Desktop actives.
# Applications actives	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
RTT ICA	Le RTT ICA est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual App ou Desktop respectivement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs backend.
Bande passante	Total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur backend.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.

RAPPORT DE SYNTHÈSE UTILISATEUR

Voici les métriques spécifiques à ce rapport.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
# Sessions actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual Apps and Desktops.
# Applications actives	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual App ou Desktop.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs backend.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur backend.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de retransmission s'est produit sur la connexion entre NetScaler et le serveur principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP nulle.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP nulle.
Nombre total de lancements d'applications	Nombre total d'applications lancées par l'utilisateur pendant la période sélectionnée.
Total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Bureaux actifs	Nombre total de Citrix Virtual Desktops actifs pendant un intervalle de temps donné.

CANAUX

Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA® sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par nombre total d'octets.

AGENTS UTILISATEURS

Les agents utilisateurs représentent la bande passante globale/le nombre total d'octets consommés par chaque point d'extrémité sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par octets totaux.

NOMBRE DE DÉPASSEMENTS DE SEUILS

Les métriques de nombre de dépassements de seuils représentent le nombre de seuils dépassés pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes.

CARTE DU MONDE

La vue Carte du monde dans HDX Insight permet aux administrateurs d'afficher les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue globale du système, explorer un pays particulier et même des villes en cliquant sur la région. Les administrateurs peuvent ensuite explorer les informations par ville et par état. À partir

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de NetScaler Console version 12.0 et ultérieure, vous pouvez explorer les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être affichés sur la carte du monde dans HDX Insight, et la densité de chaque métrique est affichée sous la forme d'une carte thermique :

- ICA RTT
- Latence WAN
- Latence DC
- Bande passante
- Octets totaux



Vue par utilisateur

La vue par utilisateur fournit des rapports détaillés sur l'expérience de l'utilisateur final pour tout utilisateur sélectionné.

Pour accéder aux métriques d'un utilisateur spécifique :

1. Accédez à **Gateway > HDX Insight > Users**.
2. Sélectionnez un utilisateur particulier dans le rapport récapitulatif des utilisateurs.

GRAPHIQUE LINÉAIRE

Le graphique linéaire affiche le résumé de toutes les métriques pour l'utilisateur sélectionné pendant la période sélectionnée.

RAPPORT SUR LES SESSIONS ACTUELLES/TERMINÉES

Ce rapport concerne toutes les sessions utilisateur actuelles/terminées pour l'utilisateur sélectionné. Ces métriques peuvent être triées par heure de début, reconnexions de session et nombre d'ACR.

MÉTRIQUES	DESCRIPTION
ID de session	Identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/Rouge pour les sessions actives/inactives.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Délai de l'hôte	Délai moyen du trafic ICA qui transite par les instances NetScaler, causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de la session	La bande passante consommée par la session, quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Heure de début	Heure de début de la session.
Durée de fonctionnement	Durée de la session.
Adresse IP du client	IP utilisateur.
Adresse IP du serveur	Adresse IP du serveur backend/Citrix Virtual App.
Adresse IP NetScaler	Adresse IP de gestion NetScaler (NSIP).
Type de client	Type d'espace de travail - Client Citrix Windows, etc.
Version du client	Version de l'espace de travail.
MSI	Booléen (Oui/Non). Indique si la session est ICA multi-flux.
Reconnexions de session	Nombre de fois où la session a été reconnectée.
Comptes ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, mode utilisateur/transparent NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Pays	Pays depuis lequel la session a été établie.
Région	Région depuis laquelle la session a été établie.
Ville	Ville depuis laquelle la session a été établie.
Statut USB	Actif/Inactif - Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où un basculement HA s'est produit.
Raison de la résiliation	Affiche la raison de la résiliation d'une session. Par exemple, Délai d'expiration de la session ICA, Session terminée par l'utilisateur.
RTT ICA	Le RTT ICA est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Citrix Virtual Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs backend.
Total d'octets	Total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur backend.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté client	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre NetScaler et le serveur backend.

PRISE EN CHARGE D'EDT DANS HDX INSIGHT

NetScaler Console prend désormais en charge le transport de données éclairé (EDT) pour l'affichage des analyses pour HDX Insight. Autrement dit, NetScaler Console prend désormais en charge les protocoles UDP et TCP. La prise en charge d'EDT pour NetScaler Gateway garantit une expérience utilisateur en session haute définition des bureaux virtuels pour les utilisateurs exécutant Citrix Workspace.

HDX Insight affiche désormais le nombre de sessions EDT et de sessions non-EDT dans le cadre du rapport sur les sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. Le tableau présente des métriques telles que la latence WAN, la latence DC, les retransmissions et les RTO. Certaines de ces métriques ne sont pas disponibles pour les utilisateurs qui ont des sessions EDT, car elles sont actuellement calculées à partir de la pile TCP. Par conséquent, elles apparaissent comme « NA ».



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.

Métriques HDX Insight disponibles à partir de NetScaler Console 12.0 et versions ultérieures :

LATENCE CÔTÉ CLIENT L7	LA LATENCE L7 MOYENNE OBSERVÉE ENTRE LE CLIENT ICA ET L'INSTANCE NETSCALER. CETTE MÉTRIQUE EST UTILE LORSQUE DES PÉRIPHÉRIQUES NON-CITRIX SONT PRÉSENTS DANS LE CHEMIN DE LIVRAISON.
Latence côté serveur L7	La latence L7 moyenne observée entre le périphérique NetScaler et l'application virtuelle Citrix. Cette métrique est utile lorsque des périphériques non-Citrix sont présents dans le chemin de livraison.
Latence de dépassement maximale	La valeur la plus élevée de la latence L7 lorsqu'un dépassement d'un seuil défini pour un intervalle de temps donné se produit.
Latence de dépassement moyenne	La valeur moyenne de la latence L7 lorsque le système est dans un état de « latence L7 dépassée ».
Nombre de dépassements de seuil L7	Le nombre de fois qu'un dépassement de seuil L7 s'est produit.

Session terminée(/en-us/netscaler-application-delivery-management-software/media/hdx-teminated-sessions-1.png)

UTILISATEURS DE BUREAU

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces métriques peuvent être triées par nombre de lancements de bureau et par bande passante.

MÉTRIQUES	DESCRIPTION
Nom	Nom du bureau virtuel Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nombre de lancements de bureau	Nombre de fois où le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs backend.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
ICA RTT	Le RTT ICA est le délai d'affichage que l'utilisateur subit lorsqu'il interagit avec une application ou un bureau hébergé respectivement sur Citrix Virtual App ou Desktop.



APPLICATIONS

Un graphique à barres représentant les applications triées par Actif, nombre total de lancements de session, nombre total de lancements d'applications et durée de lancement.



INSTANCES

Un graphique à barres représentant les instances NetScaler triées par Actives et applications totales



CANAUX

Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par octets totaux.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

AGENTS UTILISATEURS

Les agents utilisateurs représentent la bande passante globale/le nombre total d'octets consommés par chaque point de terminaison sous la forme d'un graphique en anneau. Vous pouvez également trier les métriques par bande passante ou par octets totaux.



Vue de la session par utilisateur

La vue de la session par utilisateur fournit des rapports pour la session d'un utilisateur sélectionné en particulier.

Pour afficher les métriques d'une session utilisateur sélectionnée :

1. Accédez à **Gateway > HDX Insight > Users**.
2. Sélectionnez un utilisateur particulier dans la section **Rapport récapitulatif des utilisateurs**.
3. Sélectionnez une session dans la colonne **Sessions actuelles** ou **Sessions terminées**.

GRAPHIQUE CHRONOLOGIQUE

MÉTRIQUES	DESCRIPTION
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual App et Desktop actives.
Comptes ACR	Ce nombre indique le nombre de sessions Citrix Virtual App actives.
ICA RTT	L'ICA RTT est le décalage d'écran que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual App ou Desktop respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs backend.
Bande passante de session	La bande passante consommée par la session, quel que soit l'intervalle de temps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Retransmissions côté serveur	Le nombre de paquets retransmis sur la connexion entre NetScaler et le serveur backend.
Retransmissions côté client	Le nombre de paquets retransmis sur la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette métrique ne signifie pas que l'expérience utilisateur ne sera pas fluide, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'attente de retransmission s'est produit sur la connexion entre NetScaler et le serveur backend.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre zéro côté serveur	Ce compteur indique le nombre de fois où le serveur a annoncé une fenêtre TCP de taille zéro.
Événement de taille de fenêtre zéro côté client	Ce compteur indique le nombre de fois où le client a annoncé une fenêtre TCP de taille zéro.



APPLICATION ACTIVE

La section **Applications actives** affiche les applications actives de l'utilisateur sélectionné. Ces applications peuvent également être triées par nombre de sessions actives et par durées de lancement.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

SESSIONS ASSOCIÉES

La section Sessions associées affiche les sessions associées aux sessions de l'utilisateur sélectionné. La relation peut être sélectionnée comme serveurs communs ou NetScaler commun.



Rapports et métriques de la vue d'instance

Les rapports et les métriques de la vue d'instance sont axés sur les instances NetScaler.

Pour accéder à la vue d'instance :

1. Accédez à **Gateway > HDX™ Insight > Instances**.

Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports pour toutes les instances NetScaler ajoutées à NetScaler Console.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs correspondantes pour la période sélectionnée.

GRAPHIQUE À BARRES D'INSTANCE

Ce graphique affiche l'instance par rapport au nombre total de lancements de session et au nombre total d'applications, qui peuvent être sélectionnés dans la liste en haut à droite du canevas du graphique.



RAPPORT RÉCAPITULATIF DES INSTANCES/INSTANCES ACTIVES

MÉTRIQUES	DESCRIPTION
Nom	Nom d'hôte de l'instance NetScaler.
Adresse IP	Adresse IP de NetScaler.
Nombre total de lancements de session	Nombre total de sessions utilisateur uniques créées pendant un intervalle de temps donné.
Total des applications	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.
Type	N/A



© 1997–2026 Citrix Systems, Inc. All rights reserved.

RAPPORT DE SEUIL

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Instance pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes.

FLUX IGNORÉS

Un flux ignoré est un enregistrement qui n'a pas été analysé pour la connexion ICA. Cela peut se produire pour plusieurs raisons, telles que l'utilisation de versions non prises en charge de Citrix Virtual Apps and Desktops, une version ou un type d'espace de travail non pris en charge, etc. Ce tableau affiche l'adresse IP et le nombre de flux ignorés. Ces espaces de travail peuvent ne pas faire partie des espaces de travail autorisés. Par conséquent, ces sessions sont exclues de la surveillance.

Consultez **Erreur\! Référence de lien hypertexte non valide** pour plus de détails sur les problèmes liés à l'analyse ICA.



VUE MONDIALE

La vue Carte du monde dans HDX Insight permet aux administrateurs d'afficher les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue mondiale du système, explorer un pays particulier et même des villes en cliquant sur la région. Les administrateurs peuvent ensuite explorer les informations par ville et par état. À partir de NetScaler version 12.0 et ultérieure, vous pouvez explorer les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être affichés sur la Carte du monde dans HDX Insight, et la densité de chaque métrique est affichée sous forme de carte thermique :

- ICA® RTT
- Latence WAN
- Latence DC
- Bande passante
- Octets totaux



Vue par instance

La vue par instance fournit des rapports détaillés sur l'expérience utilisateur final pour une instance NetScaler sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour accéder à la vue d'instance :

1. Accédez à **Gateway > HDX Insight > Instances**.
2. Sélectionnez une instance particulière dans le **Rapport récapitulatif des instances**.

GRAPHIQUE LINÉAIRE

MÉTRIQUES	DESCRIPTION
Adresse IP	Ceci représente l'adresse IP NetScaler de l'instance sélectionnée.
Nombre total de lancements de session	Nombre total de sessions actives Citrix Virtual App pendant l'intervalle de temps donné.
Total des applications	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.



GRAPHIQUE À BARRES DES APPLICATIONS

Affiche les 5 principales applications basées sur les critères suivants : applications actives, nombre total de lancements de session, nombre total de lancements d'applications ou durée de lancement.



GRAPHIQUE À BARRES DES UTILISATEURS

Le graphique à barres des utilisateurs affiche les 5 principaux utilisateurs basés sur les critères suivants

- Bande passante
- Latence WAN
- Latence DC
- ICA RTT



RAPPORT SUR LES UTILISATEURS DE BUREAU

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces métriques peuvent être triées par Nombre de lancements de bureau et Bande passante.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Nom	Nom du Citrix Virtual Desktop.
Nombre de lancements de bureau	Nombre de fois où le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde utilisés pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de NetScaler aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de NetScaler à l'utilisateur final.
ICA RTT	L'ICA RTT est le décalage d'affichage que l'utilisateur subit lors de l'interaction avec une application ou un bureau hébergé respectivement sur Citrix Virtual App ou Desktop.



VUE MONDIALE

La vue Carte du monde dans HDX Insight permet aux administrateurs d'afficher les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue mondiale du système, explorer un pays particulier et même des villes en cliquant sur la région. Les administrateurs peuvent ensuite explorer les informations par ville et par état. À partir de NetScaler Console version 12.0 et ultérieure, vous pouvez explorer les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être affichés sur la Carte du monde dans HDX Insight, et la densité de chaque métrique est affichée sous forme de carte thermique :

- ICA RTT
- Latence WAN
- Latence DC
- Bande passante
- Total d'octets

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Rapports et métriques de la vue des licences

La vue des licences fournit des détails sur les informations de licence de NetScaler Gateway.

Pour accéder à la vue des licences :

1. Accédez à **Gateway > HDX™ Insight > Licences**.

Graphique linéaire

MÉTRIQUES	DESCRIPTION
Licences utilisées	Les licences CCU NetScaler Gateway utilisées pendant la période sélectionnée. Chaque décompte représente le nombre de sessions utilisateur. Ceci est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences CCU NetScaler Gateway disponibles pour le client.



Rapport de seuil

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée comme Licence pendant la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes.

Résoudre les problèmes de HDX™ Insight

Si la solution HDX Insight ne fonctionne pas comme prévu, le problème peut provenir de l'un des éléments suivants. Reportez-vous aux listes de contrôle des sections correspondantes pour le dépannage.

- Configuration de HDX Insight.
- Connectivité entre NetScaler et NetScaler Console.
- Génération d'enregistrements pour le trafic HDX/ICA dans NetScaler.
- Remplissage des enregistrements dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Liste de contrôle de la configuration de HDX Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans NetScaler. Pour plus de détails, consultez Activation d'AppFlow.
- Vérifiez la configuration de HDX Insight dans la configuration en cours d'exécution de NetScaler.

  Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration de HDX Insight. Assurez-vous que le type de liaison est ICA REQUEST. Par exemple :

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type ICA_REQUEST
  ```

  Pour le mode transparent, le type de liaison doit être ICA_REQ_DEFAULT. Par exemple :

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Pour un déploiement à saut unique/Access Gateway ou à double saut, assurez-vous que la stratégie AppFlow HDX Insight est liée au serveur virtuel VPN, où le trafic HDX/ICA circule.
- Pour le mode transparent ou le mode utilisateur LAN, assurez-vous que les ports ICA® 1494 et 2598 sont définis.
- Vérifiez que le paramètre `appflowlog` dans le serveur virtuel NetScaler Gateway ou VPN est activé pour le déploiement Access Gateway ou à double saut. Pour plus de détails, consultez Activation d'AppFlow pour les serveurs virtuels.
- Vérifiez que « Connection Chaining » est activé dans le NetScaler à double saut. Pour plus de détails, consultez Configuration des appliances NetScaler Gateway pour exporter des données.
- Après un basculement HA, si l'analyse des détails HDX Insight est ignorée, vérifiez que le paramètre ICA « enableSRonHAFailover » est activé. Pour plus de détails, consultez Fiabilité de session sur une paire haute disponibilité NetScaler.

Liste de contrôle de la connectivité entre NetScaler et NetScaler Console

- Vérifiez l'état du collecteur AppFlow dans NetScaler. Pour plus de détails, consultez Comment vérifier l'état de la connectivité entre NetScaler et le collecteur AppFlow.
- Vérifiez les correspondances de la stratégie AppFlow® HDX Insight.

  Exécutez la commande `show appflow policy <policy_name>` pour vérifier les correspondances de la stratégie AppFlow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également accéder à **Paramètres > AppFlow > Stratégies** dans l'interface graphique pour vérifier les correspondances de la stratégie AppFlow.

- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Liste de contrôle de la génération d'enregistrements pour le trafic HDX/ICA dans NetScaler

Exécutez la commande `tail -f /var/log/ns.log | grep -i "default ICA Message"` pour la validation des journaux. En fonction des journaux générés, vous pouvez utiliser ces informations pour le dépannage.

- Journal : **Analyse de la connexion ICA ignorée - HDX Insight non pris en charge pour cet hôte**

  Cause : Versions de Citrix Virtual Apps and Desktops non prises en charge

  Solution de contournement : Mettez à niveau les serveurs Citrix Virtual Apps and Desktops vers une version prise en charge.

- Journal : **Type de client reçu 0x53, NON PRIS EN CHARGE**

  Cause : Version non prise en charge de Citrix Workspace

  Solution : Mettez à niveau Citrix Workspace vers une version prise en charge. Pour plus de détails, consultez l'application Citrix Workspace.

- Journal : **Error from Expand Packet - Skipping all hdx processing for this flow**

  Cause : Problème de décompression du trafic ICA

  Solution : Aucun rapport n'est disponible pour cette session ICA tant qu'une nouvelle session n'est pas établie.

- Journal : **Invalid transition: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  Cause : Problème d'analyse de la négociation ICA

  Solution : Aucun rapport n'est disponible pour cette session ICA particulière tant qu'une nouvelle session n'est pas établie.

- Journal : **Missing EUEM ICA RTT**

  Cause : Impossible d'analyser les données du canal de surveillance de l'expérience utilisateur final

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solution : Assurez-vous que le service de surveillance de l'expérience utilisateur final est démarré sur les serveurs Citrix Virtual Apps and Desktops. Assurez-vous d'utiliser les versions prises en charge de l'application Citrix Workspace.

- Journal : **Invalid Channel Header**

  Cause : Impossible d'identifier l'en-tête du canal

  Solution : Aucun rapport n'est disponible pour cette session ICA particulière tant qu'une nouvelle session n'est pas établie.

- Journal : **Skip code**

  Si vous voyez l'une des valeurs suivantes pour le code de saut, alors les détails Insight sont analysés avec saut.

  Le code de saut 0 indique que l'enregistrement a été exporté avec succès depuis NetScaler.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
100	NS_ICA_ERR_NULL_FRAG	Erreur lors du traitement des fragments ICA, probablement due à des conditions de mémoire
101	NS_ICA_ERR_INVALID_HS_CMD	Commande de négociation (handshake) non valide reçue
102	NS_ICA_ERR_REDUC_PARAM_CNT	Paramètre non valide spécifié pour l'initialisation de l'extenseur V3
103	NS_ICA_ERR_REDUC_INIT	Impossible d'initialiser correctement l'extenseur V3
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Octets insuffisants pour attribuer un codeur à un canal
105	NS_ICA_ERR_INVALID_CHANNEL	Numéro de canal ICA invalide
106	NS_ICA_ERR_INVALID_DECODER	Décodeur invalide spécifié pour un canal

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
107	NS_ICA_ERR_INVALID_TW_PARAM	Nombre de paramètres invalide spécifié sur le canal Thinwire
108	NS_ICA_ERR_INVALID_TW_DECODER	Décodeur invalide pour le canal Thinwire
109	NS_ICA_ERR_REDUC_NO_DECODER	Aucun décodeur défini pour le canal
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Échec de l'expansion des données du canal
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	Erreur d'expander : Octets consommés supérieurs aux octets disponibles
112	NS_ICA_ERR_REDUC_BYTES_OOR	Erreur : Dépassement de données non compressées
113	NS_ICA_ERR_REDUC_INVALID_CMD	Commande Expander indéfinie
114	NS_ICA_ERR_CGP_FILL_HOLE	Erreur lors du traitement des trames CGP fractionnées
115	NS_ICA_ERR_MEM_NSB_ALLOC	Erreur d'allocation NSB – due à des conditions de mémoire faible
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Erreur d'allocation de mémoire pour le contexte d'expander
117	NS_ICA_ERR_ICA_OLD_SERVER	Ancien serveur, blocs de capacités non pris en charge
118	NS_ICA_ERR_PIR_MANY_FRAG	La requête d'initialisation de paquet est fragmentée, impossible à traiter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
119	NS_ICA_ERR_INIT_ICA_CAPS	Erreur d'initialisation des capacités ICA
120	NS_ICA_ERR_NO_MSI_SUPPORT	L'hôte ne prend pas en charge la fonctionnalité MSI. Indique une version de XenApp inférieure à 6.5 ou des versions de XenDesktop inférieures à 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Commande CGP non valide rencontrée
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Octets insuffisants sur le canal
123	NS_ICA_ERR_CHANNEL_DATA	Données incorrectes sur le canal EUEM, CONTROL ou SEAMLESS
124	NS_ICA_ERR_INVALID_PURE_CMD	Commande invalide reçue lors du traitement des données du canal ICA pur
125	NS_ICA_ERR_INVALID_PURE_LEN0	Longueur invalide rencontrée lors du traitement des données du canal ICA pur
126	NS_ICA_ERR_INVALID_PURE_LEN	Longueur invalide rencontrée lors du traitement des données du canal PURE ICA
127	NS_ICA_ERR_INVALID_CLNT_DATA	Longueur de données invalide reçue du client
128	NS_ICA_ERR_MSI_GUID_SZ	Erreur dans la taille du GUID MSI
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	En-tête de canal non valide détecté

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Échec de la récupération de la session reconnectée
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Erreur lors de la désactivation de SR
132	NS_ICA_ERR_REDUC_NOT_V3	Version de réducteur ICA non prise en charge
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression désactivée, non respectée par l'hôte
134	NS_ICA_ERR_IDENT_PROTO	Impossible d'identifier le protocole ICA ou CGP, observé avec des espaces de travail incorrects
135	NS_ICA_ERR_INVALID_SIGNATURE	Signature ICA ou chaîne magique incorrecte
136	NS_ICA_ERR_PARSE_RAW	Erreur lors de l'analyse du paquet de négociation ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquet incomplet reçu lors de la négociation
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	La trame ICA est trop grande, elle dépasse 1460 octets
139	NS_ICA_ERR_FORWARD	Erreur lors du transfert des données ICA
140	NS_ICA_ERR_MAX_HOLES	Impossible de traiter la commande CGP car elle est divisée au-delà de la limite prise en charge
141	NS_ICA_ERR_ASSEMBLE_FRAME	Impossible de réassembler correctement la trame ICA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Analyse ICA ignorée pour cet espace de travail (client) car il ne figure pas dans la liste d'autorisation
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Impossible de détecter l'état d'analyse pour le cookie de reconnexion client
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Longueur de cookie de reconnexion non valide détectée après la reconnexion du client
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Le cookie de reconnexion du client n'a pas respecté la contrainte requise
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Chaîne de version d'espace de travail non valide reçue du client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	ID de produit non valide reçu du client
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Longueur de canal invalide après expansion
149	NS_ICA_ERR_SPECIAL_THINWIRE	Erreur de décompression
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Nombre d'octets insuffisant rencontré pour la commande transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Nombre d'octets insuffisant rencontré pour la commande EUEM
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Événement invalide pour l'analyse du canal transparent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Événement invalide pour l'analyse du canal CTRL
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Événement invalide pour l'analyse du canal EUEM
155	NS_ICA_ERR_USB_INVALID_EVENT	Événement invalide pour l'analyse du canal USB
156	NS_ICA_ERR_PURE_INVALID_EVENT	Événement invalide pour l'analyse du canal pur
157	NS_ICA_ERR_VCP_INVALID_EVENT	Événement invalide pour l'analyse du canal virtuel
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Événement invalide pour l'analyse des données ICA
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Événement invalide pour l'analyse des données CGP
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	État invalide pour une commande de chiffrement dans le chiffrement de base
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Commande de chiffrement invalide dans le chiffrement de base
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	État invalide pour une commande de chiffrement dans le chiffrement RC5
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Commande de chiffrement invalide dans le chiffrement RC5
164	NS_ICA_ERR_ADVCRYPT_ENC	Erreur de chiffrement/déchiffrement RC5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
165	NS_ICA_ERR_ADVCRYPT_DEC	Erreur de chiffrement/déchiffrement RC5
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	Le VDA ne prend pas en charge la version 3 du réducteur
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	L'espace de travail ne prend pas en charge la version 3 du réducteur
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Nombre d'octets inattendu dans la négociation ICA
169	NS_ICA_ERR_HIGHER_RECONSEQ	Numéro de séquence de reprise CGP plus élevé du pair après les reconnexions
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Impossible de restaurer l'état d'analyse ICA après la reconnexion
171	NS_ICA_ERR_NSAP_PARSING	Erreur lors de l'analyse des données du canal Insight
172	NS_ICA_ERR_NSAP_APP	Erreur lors de l'analyse des détails de l'application à partir des données du canal Insight
173	NS_ICA_ERR_NSAP_ACR	Erreur lors de l'analyse des détails ACR à partir des données du canal Insight
174	NS_ICA_ERR_NSAP_SESSION_END	Erreur lors de l'analyse des détails de fin de session à partir des données du canal Insight
175	NS_ICA_ERR_NON_NSAP_SN	Analyse ICA ignorée sur le nœud de service en raison de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CODE DE SAUT	MESSAGE D'ERREUR	CAUSE DE L'ERREUR
		l'absence de prise en charge du canal Insight
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP n'est pas pris en charge par le client
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP n'est pas pris en charge par le VDA
178	NS_ICA_ERR_NSAP_NEG_FAIL	Erreur lors de la négociation des données NSAP
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Erreur lors de la récupération du ticket de reconnexion de service dans le nœud de service
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Erreur lors de la réception d'un numéro de séquence de reconnexion plus élevé dans le nœud de service
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Erreur lors de la désactivation de HDX Insight pour les connexions non-NSAP

Exemples de journaux :

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session setup time
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`[01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"`

Compteurs d'erreurs

Divers compteurs sont capturés lors de l'analyse ICA. Le tableau suivant répertorie les différents compteurs pour l'analyse ICA. Exécutez la commande `nsconmsg –g hdx –d statswt0` pour afficher les détails du compteur.

NOM DU COMPTEUR HDX	OBJECTIF	CATÉGORIE (STATISTIQUES/ERREUR/ DIAGNOSTIC)
hdx_tot_ica_conn	Indique le nombre total de connexions ICA pures détectées par NS. Incrémenté chaque fois qu'une connexion ICA basée sur la signature ICA sur un PCB client est détectée.	Statistiques
hdx_tot_cgp_conn	Indique le nombre total de connexions CGP détectées par NS (Fiabilité de session ACTIVÉE). Incrémenté chaque fois qu'une connexion CGP basée sur la signature CGP sur un PCB client est détectée.	Statistiques
hdx_dbg_tot_udt_conn	Indique le nombre total de connexions ICA UDP détectées par NS	Statistiques
hdx_dbg_tot_nsap_conn	Indique le nombre total de connexions prises en charge par NSAP détectées par NS	Statistiques
hdx_tot_skip_conn	Indique le nombre de connexions ICA ignorées par l'analyseur en raison d'une	Statistiques

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DU COMPTEUR HDX	OBJECTIF	CATÉGORIE (STATISTIQUES/ERREUR/ DIAGNOSTIC)
	signature ICA ou CGP non valide.	
hdx_dbg_active_conn	Nombre total de connexions EDT/CGP/ICA actives à cet instant.	Statistiques
hdx_dbg_active_nsap_conn	Nombre total de connexions NSAP EDT/CGP/ICA actives à cet instant.	Statistiques
hdx_dbg_skip_appflow_disabled	Nombre total d'instances où AppFlow a été détaché d'une session en raison de la désactivation d'AppFlow	Statistiques/Diagnostics
hdx_dbg_transparent_user	Nombre total d'accès utilisateur transparents	Statistiques/Diagnostics
hdx_dbg_ag_user	Nombre total d'accès utilisateur à Access Gateway	Statistiques/Diagnostics
hdx_dbg_lan_user	Nombre total d'accès en mode utilisateur LAN	Statistiques/Diagnostics
hdx_basic_enc	Indique le nombre de connexions ICA utilisant le chiffrement de base	Statistiques/Diagnostics
hdx_advanced_enc	Indique le nombre de connexions ICA utilisant le chiffrement avancé basé sur RC5	Statistiques/Diagnostics
hdx_dbg_reconnected_session	Nombre total de demandes de reconnexion du client sans aucune erreur NetScaler	Statistiques/Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DU COMPTEUR HDX	OBJECTIF	CATÉGORIE (STATISTIQUES/ERREUR/ DIAGNOSTIC)
hdx_dbg_host_rejected_ns_reconnect	Nombre total de requêtes de reconnexion rejetées par le client	Statistiques/Diagnostics
hdx_euem_available	Indique le nombre de connexions pour lesquelles le canal de surveillance de l'expérience utilisateur final est disponible. Le canal de surveillance de l'expérience utilisateur final est requis pour collecter des statistiques telles que l'ICA RTT.	Statistiques/Diagnostics
hdx_err_disabled_sr	La fiabilité de session est désactivée à l'aide du paramètre `nsapimgr`. La session ne fonctionne pas pour cette session.	Erreur
hdx_err_skip_no_msi	Le serveur XA/XD ne dispose pas de la capacité MSI. Cela indique une version de serveur plus ancienne et HDX Insight ignore cette connexion.	Erreur
hdx_err_skip_old_server	Ancienne version de serveur non prise en charge	Erreur
hdx_err_clnt_not_whitelist	L'espace de travail client n'est pas dans la liste d'autorisation, HDX Insight ignore cette connexion	Erreur
hdx_sm_ica_cam_channel_disabled	Nombre total de NS_ICA_CAM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DU COMPTEUR HDX	OBJECTIF	CATÉGORIE (STATISTIQUES/ERREUR/ DIAGNOSTIC)
hdx_sm_ica_usb_channel_disabled	Nombre total de NS_ICA_USB_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_clip_channel_disabled	Nombre total de NS_ICA_CLIP_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_ccm_channel_disabled	Nombre total de NS_ICA_CCM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_cdm_channel_disabled	Nombre total de NS_ICA_CDM_CHANNEL désactivés via la politique SmartAccess	Diagnostics
hdx_sm_ica_com1_channel_disabled	Nombre total de NS_ICA_COM1_CHANNEL désactivés via la politique SmartAccess	Diagnostics
hdx_sm_ica_com2_channel_disabled	Nombre total de NS_ICA_COM2_CHANNEL désactivés via la politique SmartAccess	Diagnostics
hdx_sm_ica_cpm_channel_disabled	Nombre total de NS_ICA_CPM_CHANNEL désactivés via la politique SmartAccess	Diagnostics
hdx_sm_ica_lpt1_channel_disabled	Nombre total de NS_ICA_LPT1_CHANNEL désactivés via la politique SmartAccess	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DU COMPTEUR HDX	OBJECTIF	CATÉGORIE (STATISTIQUES/ERREUR/ DIAGNOSTIC)
hdx_sm_ica_lpt2_channel_disabled	Nombre total de NS_ICA_LPT2_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
dx_dbg_sm_ica_msi_disabled	Nombre total de cas où MSI est désactivé via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_file_channel_disabled	Nombre total de NS_ICA_FILE_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_dbg_usb_accept_device	Nombre total de périphériques USB acceptés	Diagnostics
hdx_dbg_usb_reject_device	Nombre total de périphériques USB rejetés	Diagnostics
hdx_dbg_usb_reset_endpoint	Nombre total de points de terminaison USB réinitialisés	Diagnostics
hdx_dbg_usb_reset_device	Nombre total de périphériques USB réinitialisés	Diagnostics
hdx_dbg_usb_stop_device	Nombre total de périphériques USB arrêtés	Diagnostics
hdx_dbg_usb_stop_device_response	Nombre total de réponses des périphériques USB arrêtés	Diagnostics
hdx_dbg_usb_device_gone	Nombre total de périphériques USB disparus	Diagnostics
hdx_dbg_usb_device_stopped	Nombre total de périphériques USB arrêtés	Diagnostics

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validation nstrace

Vérifiez le protocole CFLOW pour voir tous les enregistrements AppFlow sortant de NetScaler.

Liste de contrôle du remplissage des enregistrements dans NetScaler Console

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` et vérifiez les journaux pour confirmer que NetScaler Console reçoit les enregistrements AppFlow.
- Confirmez que l'instance NetScaler est ajoutée à NetScaler Console.
- Validez que le serveur virtuel NetScaler Gateway/VPN est sous licence dans NetScaler Console.
- Assurez-vous que le paramètre multi-sauts est activé pour le double-saut.
- Assurez-vous que NetScaler Gateway est autorisé pour le deuxième saut dans un déploiement à double saut.

Avant de contacter le support technique Citrix

Pour une résolution rapide, assurez-vous de disposer des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie réseau.
- Versions de NetScaler et NetScaler Console.
- Versions des serveurs Citrix Virtual Apps and Desktops.
- Versions de l'espace de travail client.
- Nombre de sessions ICA actives au moment où le problème est survenu.
- Bundle de support technique capturé en exécutant la commande `show techsupport` à l'invite de commande NetScaler.
- Bundle de support technique capturé pour NetScaler Console.
- Traces de paquets capturées sur tous les NetScaler. Pour démarrer une trace de paquets, tapez `start nstrace -size 0'` Pour arrêter une trace de paquets, tapez `stop nstrace`
- Collectez les entrées de la table ARP du système en exécutant la commande `show arp`.

Problèmes connus

Consultez les notes de publication de NetScaler pour les problèmes connus concernant HDX Insight.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure

NetScaler Console offre des capacités de gestion et d'analyse de l'infrastructure pour découvrir, surveiller et gérer vos instances NetScaler. Les rubriques suivantes vous aident à gérer votre infrastructure NetScaler :

- Analyse de l'infrastructure
- Gestion des instances
- Gestion des certificats SSL
- Événements
- Fonctions réseau
- Rapports réseau
- Configuration
- Avis de sécurité
- Avis de mise à niveau
- Orchestration

Analyse de l'infrastructure

Un objectif clé pour les administrateurs réseau est de surveiller les instances NetScaler. Les instances NetScaler offrent des informations intéressantes sur l'utilisation et les performances des applications et des bureaux accessibles via celles-ci. Les administrateurs doivent surveiller l'instance NetScaler et analyser les flux d'applications traités par chaque instance NetScaler. Ils peuvent ainsi remédier à tout problème probable de configuration, d'installation, de connectivité, de certificats et autres qui pourrait avoir un impact sur l'utilisation ou les performances des applications. Par exemple, un changement soudain dans le modèle de trafic d'application peut être dû à une modification de la configuration SSL, comme la désactivation d'un protocole SSL. Les administrateurs doivent être en mesure d'identifier rapidement la corrélation entre ces points de données pour garantir les éléments suivants :

- La disponibilité des applications est dans un état optimal
- Il n'y a pas de problèmes de consommation de ressources, de matériel, de capacité ou de modification de configuration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Il n'y a pas d'inventaires inutilisés
- Il n'y a pas de certificats expirés

La fonctionnalité d'analyse de l'infrastructure simplifie le processus d'analyse des données en corrélant plusieurs sources de données et en les quantifiant en un score mesurable qui définit la santé d'une instance. Grâce à cette fonctionnalité, les administrateurs disposent d'un point d'accès unique pour comprendre s'il y a un problème, l'origine du problème et les remédiations probables qu'ils peuvent effectuer.

Analyse de l'infrastructure

La fonctionnalité d'analyse de l'infrastructure de NetScaler Console rassemble toutes les données collectées à partir des instances NetScaler et les quantifie en un **score d'instance** qui définit la santé des instances. Le score d'instance est résumé sous forme de tableau ou de visualisation en cercle. La fonctionnalité d'analyse de l'infrastructure vous aide à visualiser les facteurs qui ont entraîné ou pourraient entraîner un problème sur les instances. Cette visualisation vous aide également à déterminer les actions à effectuer pour prévenir le problème et sa récurrence.

Score d'instance

Le score d'instance indique la santé d'une instance NetScaler. Un score de 100 signifie une instance parfaitement saine sans aucun problème. Le score d'instance capture différents niveaux de problèmes potentiels sur l'instance. C'est une mesure quantifiable de la santé de l'instance et plusieurs « indicateurs de santé » contribuent au score.

Les **indicateurs de santé** sont les éléments constitutifs du score d'instance, où le score est calculé périodiquement pour une « période de surveillance » prédéfinie, en fonction de tous les indicateurs détectés dans cette fenêtre temporelle. Actuellement, l'analyse de l'infrastructure calcule le score d'instance une fois par heure en fonction des données collectées à partir des instances. Un indicateur peut être défini comme toute activité (un événement ou un problème) appartenant à l'une des catégories suivantes sur les instances.

- Indicateurs de ressources système
- Indicateurs d'événements critiques
- Indicateurs de configuration SSL
- Indicateurs d'écart de configuration

Indicateurs de santé

- Indicateurs de ressources système

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voici les problèmes critiques de ressources système qui peuvent survenir sur les instances NetScaler et qui sont surveillés par NetScaler Console.

- **Utilisation élevée du CPU**. L'utilisation du CPU a dépassé la valeur seuil supérieure dans l'instance NetScaler.
- **Utilisation élevée de la mémoire**. L'utilisation de la mémoire a dépassé la valeur seuil supérieure dans l'instance NetScaler.
- **Utilisation élevée du disque**. L'utilisation du disque a dépassé la valeur seuil supérieure dans l'instance NetScaler.
- **Erreurs de disque**. Il y a des erreurs sur le disque dur 0 ou le disque dur 1 de l'hyperviseur où l'instance NetScaler est installée.
- **Panne de courant**. L'alimentation électrique a échoué ou a été déconnectée de l'instance NetScaler.
- **Défaillance de la carte SSL**. La carte SSL installée sur l'instance a échoué.
- **Erreurs Flash**. Des erreurs Compact Flash sont détectées sur l'instance NetScaler.
- **Rejets NIC**. Les paquets rejetés par la carte NIC ont dépassé la valeur seuil supérieure dans l'instance NetScaler.

Pour plus d'informations sur ces erreurs de ressources système, consultez Le tableau de bord de l'instance.

- Indicateurs d'événements critiques

  Les événements critiques suivants sont identifiés par les événements de la fonction de gestion des événements de NetScaler Console qui sont configurés avec une gravité critique.

  - **Échec de la synchronisation HA**. La synchronisation de la configuration entre les instances NetScaler en haute disponibilité a échoué sur le serveur secondaire.
  - **Absence de pulsations HA**. Le serveur principal d'une paire d'instances NetScaler en haute disponibilité ne reçoit pas de pulsations du serveur secondaire.
  - **Mauvais état secondaire HA**. Le serveur secondaire d'une paire d'instances NetScaler en haute disponibilité est dans l'état Arrêté, Inconnu ou Secondaire permanent.
  - **Incompatibilité de version HA**. La version des images logicielles NetScaler installées sur une paire d'instances NetScaler en haute disponibilité ne correspond pas.
  - **Échec de la synchronisation du cluster**. La synchronisation de la configuration entre les instances NetScaler en mode cluster a échoué.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Incompatibilité de version du cluster**. La version des images logicielles NetScaler installées sur les instances NetScaler en mode cluster ne correspond pas.
- **Échec de la propagation du cluster**. La propagation des configurations à toutes les instances d'un cluster a échoué.

REMARQUE

Vous pouvez obtenir votre liste d'événements SNMP critiques en modifiant les niveaux de gravité des événements. Pour plus d'informations sur la modification des niveaux de gravité, consultez Modifier la gravité signalée des événements qui se produisent sur les instances NetScaler.

Pour plus d'informations sur les événements dans NetScaler Console, consultez Événements.

- Indicateurs de configuration SSL
  - **Force de clé non recommandée**. La force de clé des certificats SSL n'est pas conforme aux normes NetScaler®
  - **Émetteur non recommandé**. L'émetteur du certificat SSL n'est pas recommandé par Citrix.
  - **Certificats SSL expirés**. Le certificat SSL installé dans l'instance NetScaler a expiré.
  - **Expiration des certificats SSL imminente**. Le certificat SSL installé dans l'instance NetScaler est sur le point d'expirer dans la semaine à venir.
  - **Algorithmes non recommandés**. Les algorithmes de signature des certificats SSL installés dans l'instance NetScaler ne sont pas conformes aux normes NetScaler.

Pour plus d'informations sur les certificats SSL, consultez Tableau de bord SSL.

- Indicateurs d'écart de configuration
  - **Modèle de dérive de configuration**. Il y a une dérive (modifications non enregistrées) dans la configuration par rapport aux modèles d'audit que vous avez créés avec des configurations spécifiques que vous souhaitez auditer sur certaines instances.
  - **Dérive de configuration par défaut**. Il y a une dérive (modifications non enregistrées) dans la configuration par rapport aux fichiers de configuration par défaut.

Pour plus d'informations sur les écarts de configuration et sur la façon d'exécuter des rapports d'audit pour vérifier les écarts de configuration, consultez Afficher les rapports d'audit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les problèmes de capacité NetScaler

Lorsqu'une instance NetScaler a consommé la majeure partie de sa capacité disponible, une perte de paquets peut se produire lors du traitement du trafic client. Ce problème entraîne de faibles performances dans une instance NetScaler. En comprenant ces problèmes de capacité NetScaler, vous pouvez allouer des licences supplémentaires de manière proactive pour stabiliser les performances de NetScaler.

Pour afficher les problèmes de capacité NetScaler,

1. Accédez à **Infrastructure > Infrastructure Analytics**.
2. Développez l'instance pour laquelle vous souhaitez afficher les problèmes de capacité.

La console NetScaler interroge ces événements toutes les cinq minutes à partir de l'instance NetScaler et affiche les pertes de paquets ou les incréments de compteur de limite de débit, le cas échéant. Les problèmes sont classés selon les paramètres de capacité suivants :

- **Limite de débit atteinte** – Le nombre de paquets perdus dans l'instance après que la limite de débit a été atteinte.
- **Limite de CPU PE atteinte** - Le nombre de paquets perdus sur toutes les cartes réseau après que la limite de CPU PE a été atteinte.
- **Limite PPS atteinte** – Le nombre de paquets perdus dans l'instance après que la limite PPS a été atteinte.
- **Limite de débit SSL** – Le nombre de fois où la limite de débit SSL a été atteinte.
- **Limite de TPS SSL** – Le nombre de fois où la limite de TPS SSL a été atteinte.

La console NetScaler calcule le score de l'instance en fonction du seuil de capacité défini.

- Seuil bas – 1 perte de paquet ou incrément du compteur de limite de débit
- Seuil haut – 10000 pertes de paquets ou incrément du compteur de limite de débit

Par conséquent, lorsqu'une instance NetScaler dépasse le seuil de capacité, le score de l'instance est affecté.

Lorsque des paquets sont perdus ou que le compteur de limite de débit s'incrémente, un événement est généré sous la catégorie `NetScalerCapacityBreach`. Pour afficher ces événements, accédez à **Comptes > Événements système**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Valeur des indicateurs de santé

Les indicateurs sont classés en indicateurs de haute priorité et indicateurs de faible priorité en fonction de leurs valeurs, comme suit :

Les indicateurs de santé au sein du même groupe d'indicateurs ont des poids différents. Un indicateur peut contribuer davantage à la diminution du score de l'instance qu'un autre indicateur. Par exemple, une utilisation élevée de la mémoire réduit davantage le score de l'instance qu'une utilisation élevée du disque, une utilisation élevée du CPU et un rejet de la carte réseau. Si un plus grand nombre d'indicateurs sont détectés sur une instance, plus le score de l'instance est faible.

La valeur d'un indicateur est calculée selon les règles suivantes. L'indicateur est considéré comme détecté de l'une des trois manières suivantes :

1. **Basé sur une activité**. Par exemple, un indicateur de ressource système est déclenché chaque fois qu'il y a une panne de courant sur l'instance, et cet indicateur réduit la valeur du score de l'instance. Lorsque l'indicateur est effacé, la pénalité est levée et le score de l'instance augmente.
2. **Basé sur le dépassement de la valeur seuil**. Par exemple, un indicateur de ressource système est déclenché lorsque la carte réseau rejette des paquets et que le niveau de seuil est dépassé.
3. **Basé sur le dépassement des valeurs de seuil bas et haut**. Ici, un indicateur peut être déclenché de deux manières :
    - Lorsque la valeur de l'indicateur se situe entre les seuils bas et haut, auquel cas une pénalité partielle est appliquée au score de l'instance.
    - Lorsque la valeur dépasse le seuil haut, auquel cas une pénalité complète est appliquée au score de l'instance.
    - Aucune pénalité n'est appliquée au score de l'instance si la valeur tombe en dessous d'un seuil bas.

Par exemple, l'utilisation du CPU est un indicateur de ressource système déclenché lorsque la valeur d'utilisation dépasse le seuil bas et également lorsque la valeur dépasse le seuil haut.

Tableau de bord d'analyse de l'infrastructure

Accédez à **Infrastructure > Infrastructure Analytics**.

L'analyse de l'infrastructure peut être affichée au format **Circle Pack** ou au format **Tabulaire**. Vous pouvez basculer entre les deux formats.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Dans la vue Tabulaire, vous pouvez rechercher une instance en saisissant le nom d'hôte ou l'adresse IP dans la barre de recherche.
- Par défaut, la page Analyse de l'infrastructure affiche le panneau Récapitulatif sur le côté droit de la page.
- Cliquez sur l'icône **Paramètres** pour afficher le panneau **Paramètres**.
- Dans les deux formats d'affichage, le panneau Récapitulatif affiche les détails de toutes les instances de votre réseau.

Vue Circle Pack

Les diagrammes Circle Pack affichent les groupes d'instances sous forme de cercles étroitement organisés. Ils montrent souvent des hiérarchies où les groupes d'instances plus petits sont soit colorés de manière similaire aux autres de la même catégorie, soit imbriqués dans des groupes plus grands. Les Circle Packs représentent des ensembles de données hiérarchiques et montrent différents niveaux dans la hiérarchie et comment ils interagissent les uns avec les autres.



Cercles d'instances

Couleur. Chaque instance est représentée dans le Circle Pack comme un cercle coloré. La couleur du cercle indique l'état de santé de cette instance.

- **Vert** - le score de l'instance est compris entre 100 et 80. L'instance est saine.
- **Jaune** - le score de l'instance est compris entre 80 et 50 ; certains problèmes ont été détectés et nécessitent un examen.
- **Rouge** - le score de l'instance est inférieur à 50. L'instance est dans un état critique car plusieurs problèmes ont été détectés sur cette instance.



Taille. La taille de ces cercles colorés indique le nombre de serveurs virtuels configurés sur cette instance. Un cercle plus grand indique un plus grand nombre de serveurs virtuels.

Vous pouvez survoler chacun des cercles d'instances (cercles colorés) avec le pointeur de la souris pour afficher un résumé. L'info-bulle affiche le nom d'hôte de l'instance, le nombre de serveurs virtuels actifs et le nombre d'applications configurées sur cette instance.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cercles d'instances groupés

Le Circle Pack, au départ, comprend des cercles d'instances qui sont regroupés, imbriqués ou emballés à l'intérieur d'un autre cercle selon les critères suivants :

- le site où ils sont déployés
- le type d'instances déployées - VPX, MPX, SDX et CPX
- le modèle virtuel ou physique de l'instance NetScaler
- la version de l'image NetScaler installée sur les instances

L'image suivante montre un Circle Pack où les instances sont d'abord regroupées par le site ou le centre de données où elles sont déployées, puis elles sont regroupées en fonction de leur type, VPX et MPX.

Cercles regroupés(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-5.png)

Tous ces cercles imbriqués sont délimités par deux cercles extérieurs. Les deux cercles extérieurs représentent les quatre catégories d'événements surveillés par la NetScaler Console (ressources système, événements critiques, configuration SSL et déviation de configuration) et les indicateurs de santé contributifs.

Cercles d'instances en cluster

NetScaler Console surveille de nombreuses instances. Pour faciliter la surveillance et la maintenance de ces instances, Infrastructure Analytics vous permet de les regrouper à deux niveaux. Autrement dit, les regroupements d'instances peuvent être imbriqués dans un autre regroupement.

Par exemple, le centre de données BLR contient deux types d'instances NetScaler - VPX et MPX - qui y sont déployées. Vous pouvez d'abord regrouper les instances NetScaler par leur type, puis regrouper toutes les instances par le site où elles sont regroupées. Vous pouvez maintenant facilement identifier combien de types d'instances sont déployés dans les sites que vous gérez.

Cluster(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-6.png)

Sélectionner le pack de cercles(/en-us/netscaler-application-delivery-management-software/media/circle-pack-select.png)

Voici quelques autres exemples de clustering à deux niveaux :

Site et modèle :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Site(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-7.png)

Type et version :

Modèle(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-8.png)

Site et version :

Version(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-9.png)

Comment utiliser Circle Pack

Cliquez sur chacun des cercles colorés pour mettre en surbrillance cette instance.

Selon les événements qui se sont produits dans cette instance, seuls ces indicateurs de santé sont mis en surbrillance sur les cercles extérieurs. Par exemple, les deux images suivantes du Circle Pack affichent différents ensembles d'indicateurs de risque, bien que les deux instances soient dans un état critique.

Vous pouvez également cliquer sur les indicateurs de santé pour obtenir plus de détails sur le nombre d'instances ayant signalé cet indicateur de risque. Par exemple, cliquez sur `Not recommended Algo` pour afficher le rapport récapitulatif de cet indicateur de risque.

Vue tabulaire

La vue tabulaire affiche les instances et les détails de ces instances dans un format tabulaire. Les détails affichés sont les suivants :

- Nom d'hôte de l'instance
- L'adresse IP de l'instance
- État de l'instance
- Score de l'instance
- Nombre de serveurs virtuels configurés sur cette instance
- Nombre d'applications configurées sur cette instance
- Nombre total d'indicateurs de risque
- L'événement qui contribue le plus à la baisse du score d'une instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les instances qui sont dans un état critique se trouvent en haut du tableau, suivies des instances qui doivent être examinées, puis des instances plus saines.

Cliquez sur l'adresse IP de l'instance dans la vue tabulaire pour afficher plus de détails sur cette instance sous forme de tableau de bord. Le tableau de bord de l'instance présente un aperçu de l'instance où vous pouvez voir l'utilisation du CPU, de la mémoire et du disque de l'instance. Vous pouvez également voir les détails liés à la gestion des certificats SSL, à l'audit de configuration, aux fonctions réseau et à un rapport réseau qui affiche l'utilisation détaillée du réseau de l'instance. Faites défiler vers le bas pour voir la liste des fonctionnalités et des modes activés sur cette instance.

Vous pouvez également cliquer sur la flèche au début de chaque ligne pour développer la ligne et afficher plus de détails.

La ligne de tableau développée affiche les erreurs survenues sur l'instance pour toutes les catégories. Dans l'exemple ci-dessus, vous pouvez constater qu'il y a eu des erreurs dans les ressources système, la configuration SSL et des écarts dans les fichiers de configuration. Cependant, aucun événement critique n'est signalé par l'instance.

Comment utiliser le panneau de résumé

Le **Panneau de résumé** vous aide à vous concentrer efficacement et rapidement sur les instances qui nécessitent un examen ou qui sont dans un état critique. Le panneau est divisé en trois onglets : aperçu, informations sur l'instance et profil de trafic. Les modifications que vous apportez dans ce panneau modifient l'affichage dans les formats Circle Pack et Vue tabulaire. Les sections suivantes décrivent ces onglets plus en détail. Les exemples des sections suivantes vous aident à utiliser efficacement les différents critères de sélection pour analyser les problèmes signalés par les instances.

Aperçu :

L'onglet **Aperçu** vous permet de surveiller les instances en fonction des erreurs matérielles, de l'utilisation, des certificats expirés et d'indicateurs similaires pouvant survenir dans les instances. Les indicateurs que vous pouvez surveiller ici sont les suivants :

- Utilisation du CPU
- Utilisation de la mémoire
- Utilisation du disque

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pannes système
- Événements critiques
- Expiration des certificats SSL

Les exemples suivants illustrent comment interagir avec le panneau **Vue d'ensemble** pour isoler les instances qui signalent des erreurs.

Exemple 1 : Afficher les instances en état de révision :

Cochez la case **Révision** pour afficher uniquement les instances qui ne signalent pas d'erreurs critiques, mais qui nécessitent tout de même une attention particulière.

Les histogrammes du panneau **Vue d'ensemble** représentent un nombre agrégé d'instances basées sur des événements d'utilisation élevée du CPU, d'utilisation élevée de la mémoire et d'utilisation élevée du disque. Les histogrammes sont gradués à 10 %, 20 %, 30 %, 40 %, 50 %, 60 %, 70 %, 80 %, 90 % et 100 %. Passez le pointeur de votre souris sur l'un des histogrammes. La légende au bas du graphique affiche la plage d'utilisation et le nombre d'instances dans cette plage. Vous pouvez également cliquer sur l'histogramme pour afficher toutes les instances de cette plage.

Exemple 2 : Afficher les instances qui consomment entre 10 % et 20 % de la mémoire allouée :

Dans la section d'utilisation de la mémoire, cliquez sur l'histogramme. La légende indique que la plage sélectionnée est de 10 à 20 % et qu'il y a 29 instances fonctionnant dans cette plage.

Vous pouvez également sélectionner plusieurs plages dans ces histogrammes.

Exemple 3 : Afficher les instances qui consomment beaucoup d'espace disque dans plusieurs plages :

Pour afficher les instances qui ont consommé de l'espace disque entre 0 et 10 %, faites glisser le pointeur de la souris sur les deux plages.



REMARQUE

Cliquez sur « X » pour supprimer la sélection. Vous pouvez également cliquer sur **Réinitialiser** pour supprimer plusieurs sélections.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les graphiques à barres horizontales du panneau **Vue d'ensemble** indiquent le nombre d'instances qui signalent des erreurs système, des événements critiques et l'état d'expiration des certificats SSL. Cochez la case pour afficher ces instances.

Exemple 4 : Afficher les instances pour les certificats SSL expirés :

1 - Cliquez sur la liste **Filtrer**.

2 - Dans la section **Expiration des certificats SSL**, cochez la case **Expiré** pour afficher les instances.

Informations sur l'instance

Le panneau **Informations sur l'instance** vous permet d'afficher les instances en fonction du type de déploiement, du type d'instance, du modèle et de la version du logiciel. Vous pouvez cocher plusieurs cases pour affiner votre sélection.

Exemple 5 : Afficher les instances NetScaler VPX avec un numéro de build spécifique :

Sélectionnez la version que vous souhaitez afficher.

Profil de trafic

Les histogrammes du panneau **Profil de trafic** représentent un nombre agrégé d'instances basé sur le débit sous licence des instances, le nombre de requêtes, de connexions et de transactions gérées par les instances. Sélectionnez le graphique à barres pour afficher les instances dans cette plage.

Exemple 6 : Afficher les instances prenant en charge les connexions TCP :

L'image suivante montre le nombre d'instances prenant en charge les connexions TCP.

Comment utiliser le panneau de paramètres

Le panneau **Paramètres** vous permet de définir la vue par défaut de l'Analyse de l'infrastructure. Il vous permet également de définir les valeurs de seuil basses et élevées pour une utilisation élevée du CPU, une utilisation élevée du disque et une utilisation élevée de la mémoire. Le panneau de paramètres est divisé en deux onglets : Vue et Seuils de score.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vue

- **Vue par défaut**. Sélectionnez le format **Circle Pack** ou Tabulaire comme vue par défaut sur la page d'analyse. Le format que vous sélectionnez est celui que vous voyez chaque fois que vous accédez à la page dans NetScaler Console.
- **Circle Pack - Taille de l'instance**. Permet de définir la taille du cercle d'instance en fonction du nombre de serveurs virtuels ou du nombre de serveurs virtuels actifs.
- **Circle Pack - Regrouper par**. Décidez du regroupement à deux niveaux des cercles d'instance. Pour plus d'informations sur le regroupement d'instances, consultez Cercles d'instances regroupés.



Seuils de score

Vous pouvez modifier les valeurs de seuil basses et élevées pour une utilisation élevée du CPU, de la mémoire et du disque en fonction des exigences de trafic de votre organisation. Faites glisser les poignées dans chaque Histogramme de sélection pour définir les valeurs.



REMARQUE

Cliquez sur **Appliquer les paramètres** pour appliquer ces modifications, ou cliquez sur **Réinitialiser** pour annuler toutes les modifications.

Comment visualiser les données sur le tableau de bord

Grâce à l'Analyse de l'infrastructure, les administrateurs réseau peuvent désormais identifier les instances nécessitant le plus d'attention en quelques secondes. Pour comprendre la visualisation des données plus en détail, prenons le cas de Chris, un administrateur réseau d'ExampleCompany.

Chris gère de nombreuses instances NetScaler au sein de l'organisation. Quelques-unes de ces instances traitent un trafic élevé, et Chris doit les surveiller de près. Chris remarque que quelques instances à fort trafic ne traitent plus l'intégralité du trafic qui les traverse. Pour analyser cette réduction, Chris devait auparavant lire plusieurs rapports de données provenant de diverses sources. Chris devait passer plus de temps à essayer de corréler manuellement les données et à déterminer quelles instances n'étaient pas dans un état optimal et nécessitaient une attention particulière.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Chris utilise la fonctionnalité Infrastructure Analytics pour visualiser l'état de santé de toutes les instances.

Les deux exemples suivants illustrent comment Infrastructure Analytics aide Chris dans ses activités de maintenance :

Exemple 1 - Pour surveiller le trafic SSL :

Chris remarque sur le Circle Pack qu'une instance a un score d'instance faible et qu'elle est dans un état « Critique ». Chris clique sur cette instance pour voir quel est le problème. Le résumé de l'instance indique qu'il y a une défaillance de la carte SSL sur cette instance et que l'instance est incapable de traiter le trafic SSL (le trafic SSL a diminué). Chris extrait ces informations et envoie un rapport à l'équipe pour qu'elle examine le problème immédiatement.

Exemple 2 - Pour surveiller les modifications de configuration :

Chris remarque également qu'une autre instance est en état « Révision » et qu'il y a eu un écart de configuration récemment. Lorsque Chris clique sur l'indicateur de risque d'écart de configuration, Chris remarque que des modifications de configuration liées à RC4 Cipher, SSL v3, TLS 1.0 et TLS 1.1 ont été effectuées, ce qui pourrait être dû à des préoccupations de sécurité. Chris remarque également que le profil de trafic de transaction SSL pour cette instance a diminué. Chris exporte ce rapport et l'envoie à l'administrateur pour qu'il enquête plus en détail.

Afficher les détails de l'instance dans Infrastructure Analytics

1. Accédez à **Infrastructure > Infrastructure Analytics**
2. Cliquez sur la vue en pack de cercles et sélectionnez l'adresse IP.

   Vous pouvez également cliquer sur une adresse IP à partir de la vue tableau.

- **Nom d'hôte** – Indique le nom d'hôte attribué à l'instance NetScaler
- **Adresse IP** – Indique l'adresse IP de l'instance NetScaler
- **Score** – Indique le score de l'instance NetScaler et l'état tel que Critique, Bon et Passable
- **Disponibilité** – Indique l'état de l'instance NetScaler, tel que **Actif**, **Inactif** ou **Hors service**.
- **Contribution maximale** – Indique la catégorie de problème pour laquelle l'instance NetScaler a le nombre maximal d'erreurs.
- **Utilisation du CPU** – Indique le pourcentage actuel d'utilisation du CPU par l'instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Utilisation de la mémoire** – Indique le pourcentage actuel d'utilisation de la mémoire par l'instance
- **Utilisation du disque** – Indique le pourcentage actuel d'utilisation du disque par l'instance
- **Défaillance système** – Indique le nombre total d'erreurs pour le système de l'instance
- **Événements critiques** – Indique la catégorie d'événements pour laquelle l'instance NetScaler a le plus grand nombre d'événements
- **Expiration SSL** – Indique l'état du certificat SSL installé sur l'instance NetScaler
- **Type** – Indique le type d'instance NetScaler, tel que VPX, SDX, MPX ou CPX
- **Déploiement** – Indique si l'instance NetScaler est déployée en tant qu'instance autonome ou en paire HA
- **Modèle** – Indique le numéro de modèle de l'instance NetScaler
- **Version** – Indique la version et le numéro de build de l'instance NetScaler
- **Débit** – Indique le débit réseau actuel de l'instance NetScaler
- **Requêtes HTTPS/sec** – Indique le nombre actuel de requêtes HTTPS/sec reçues par l'instance NetScaler
- **Connexion TCP** – Indique les connexions TCP actuelles établies
- **Transaction SSL** – Indique les transactions SSL actuelles traitées par l'instance NetScaler
- **Site** – Indique le nom du site où l'instance NetScaler est déployée.

REMARQUE

Toutes les 5 minutes, les valeurs actuelles d'utilisation du CPU, d'utilisation de la mémoire, d'utilisation du disque, de débit, etc., sont mises à jour.

Cliquez sur **Détails de l'instance** pour afficher les détails.



Les détails suivants sont affichés :

- **Informations** - Détails de l'instance tels que le type d'instance, le type de déploiement, la version, le modèle.

  

- **Fonctionnalités** – Par défaut, les fonctionnalités non sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Modes** – Par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.



Le tableau de bord de l'instance présente un aperçu de l'instance où vous pouvez voir les détails suivants :

- **Score de l'instance**

  

  1 – Indique le score actuel de l'instance NetScaler pour la durée sélectionnée. Le score final est calculé comme **100 moins les pénalités totales**. Le graphique affiche les plages de scores pour la durée sélectionnée.

  2 – Indique l'état de l'instance NetScaler, tel que **Actif**, **Inactif** et **Hors service**.

  3 – Indique la durée pendant laquelle l'instance NetScaler est opérationnelle.

  4 – Indique le nombre total d'interfaces réseau activées et désactivées pour l'instance. Cliquez pour afficher les détails tels que le nom de l'interface réseau et l'état (activé ou désactivé).

  5 – Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

  6 – Affiche le nombre total de problèmes et la catégorie de problèmes de l'instance NetScaler.

- **Métriques clés**

  Cliquez sur chaque onglet pour afficher les détails. Pour chaque métrique, vous pouvez afficher la valeur moyenne et la valeur de différence pour la période sélectionnée.

  L'image suivante est un exemple pour les requêtes HTTPS/sec et la durée sélectionnée est de 1 heure. La valeur **692** est la moyenne des requêtes HTTPS/sec pour la durée d'un mois et la valeur **20** est la valeur de différence. Dans le graphique, la première valeur est **139** et la dernière valeur est **119**. La valeur de différence est **139 – 119 = 20**.

  

  Vous pouvez afficher les métriques d'instance suivantes sous forme de graphique pour la durée sélectionnée :

  - **Utilisation du CPU** – Le pourcentage moyen d'utilisation du CPU de l'instance pour la durée sélectionnée (affiché pour le CPU de paquets et le CPU de gestion).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Utilisation de la mémoire** – Le pourcentage moyen d'utilisation de la mémoire de l'instance pour la durée sélectionnée.
- **Utilisation du disque** – Le pourcentage moyen d'espace disque de l'instance pour la durée sélectionnée.
- **Débit** – Le débit réseau moyen traité par l'instance pour la durée sélectionnée.
- **Requêtes HTTPS/sec** – Le nombre moyen de requêtes HTTPS reçues par l'instance pour la durée sélectionnée.
- **Connexions TCP** – Le nombre moyen de connexions TCP établies par le client et le serveur pour la durée sélectionnée.
- **Transactions SSL** – Le nombre moyen de transactions SSL traitées par l'instance pour la durée sélectionnée.

- **Problèmes**

  Vous pouvez afficher les problèmes suivants qui se produisent dans l'instance NetScaler :

CATÉGORIE DE PROBLÈME	DESCRIPTION	PROBLÈMES
Ressources système	Affiche tous les problèmes liés aux ressources système NetScaler telles que le CPU, la mémoire, l'utilisation du disque.	- Utilisation élevée du CPU
		- Utilisation élevée de la mémoire
		- Utilisation élevée du disque
		- Défaillances de la carte SSL
		- Panne de courant
		- Erreur de disque
		- Erreur Flash
		- Rejets NIC

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIE DE PROBLÈME	DESCRIPTION	PROBLÈMES
Configuration SSL	Affiche tous les problèmes liés à la configuration SSL sur l'instance NetScaler.	- Certificats SSL expirés
		- Émetteur non recommandé
		- Algorithme non recommandé
		- Force de clé non recommandée
Déviation de configuration	Affiche tous les problèmes liés aux tâches de configuration appliquées dans l'instance NetScaler.	- Dérive de configuration
		- Exécution vs Modèle
Événements critiques	Affiche tous les événements critiques liés aux instances NetScaler configurées en paire HA et en cluster.	- Échec de propagation du cluster
		- Échec de synchronisation du cluster
		- Incompatibilité des versions du cluster
		- État secondaire HA incorrect
		- HA Pas de battements de cœur
		- Échec de synchronisation HA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIE DE PROBLÈME	DESCRIPTION	PROBLÈMES
		- Incompatibilité de version HA
Réseau	Affiche les problèmes opérationnels qui se produisent dans les instances.	Pour plus d'informations, consultez Analyse d'infrastructure améliorée avec de nouveaux indicateurs.

Cliquez sur chaque onglet pour analyser et résoudre le problème. Par exemple, considérez qu'une instance présente les erreurs suivantes pour la durée sélectionnée :

- L'onglet **Actuel** affiche les problèmes qui affectent actuellement le score de l'instance.
- L'onglet **Tous** affiche tous les problèmes d'infrastructure détectés pour la durée sélectionnée.

Afficher les problèmes de capacité dans une instance NetScaler

Lorsqu'une instance NetScaler a consommé la majeure partie de sa capacité disponible, une perte de paquets peut se produire lors du traitement du trafic client. Ce problème entraîne de faibles performances dans une instance NetScaler. En comprenant ces problèmes de capacité NetScaler, vous pouvez allouer de manière proactive des licences supplémentaires pour stabiliser les performances de NetScaler.

Dans la **vue en pack de cercles**, vous pouvez afficher les problèmes de capacité de l'instance NetScaler s'ils existent.

Pour afficher les problèmes de capacité de NetScaler,

1. Accédez à **Infrastructure > Infrastructure Analytics**.
2. Sélectionnez la vue en pack de cercles.

REMARQUE

Dans **Infrastructure Analytics**, les vues en pack de cercles et tabulaires affichent les événements et les problèmes qui se sont produits au cours de la dernière heure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'illustration suivante suggère que des problèmes de capacité existent dans l'instance sélectionnée :



Les problèmes sont classés selon les paramètres de capacité suivants :

- **Limite de débit atteinte** – Le nombre de paquets abandonnés dans l'instance après que la limite de débit a été atteinte.
- **Limite de CPU PE atteinte** - Le nombre de paquets abandonnés sur toutes les cartes réseau après que la limite de CPU PE a été atteinte.
- **Limite PPS atteinte** – Le nombre de paquets abandonnés dans l'instance après que la limite PPS a été atteinte.
- **Limite de débit SSL** – Le nombre de fois où la limite de débit SSL a été atteinte.
- **Limite de débit TPS SSL** – Le nombre de fois où la limite de TPS SSL a été atteinte.

Afficher les actions recommandées pour résoudre les problèmes de capacité

NetScaler Console recommande des actions qui peuvent résoudre les problèmes de capacité. Pour afficher les actions recommandées, procédez comme suit :

1. Dans **Infrastructure > Infrastructure Analytics**, sélectionnez la vue tabulaire.
2. Sélectionnez l'instance qui présente des problèmes de capacité et cliquez sur **Détails**.

   
3. Dans la page de l'instance, faites défiler jusqu'à la section **Problèmes**.
4. Sélectionnez chaque problème et affichez les actions recommandées pour résoudre les problèmes de capacité.

   

NetScaler Console interroge ces événements toutes les cinq minutes depuis l'instance NetScaler et affiche les pertes de paquets ou les incréments de compteur de limite de débit, s'ils existent.

NetScaler Console calcule le score de l'instance en fonction du seuil de capacité défini.

- **Seuil bas** – 1 perte de paquet ou incrément de compteur de limite de débit
- **Seuil élevé** – 10000 pertes de paquets ou incréments de compteur de limite de débit

Par conséquent, lorsqu'une instance NetScaler dépasse le seuil de capacité, le score de l'instance est affecté.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque des paquets sont perdus ou que le compteur de limite de débit s'incrémente, un événement est généré sous la catégorie `ADCCapacityBreach`. Pour afficher ces événements, accédez à **Comptes > Événements système**.

Analyse d'infrastructure améliorée avec de nouveaux indicateurs

En utilisant l'analyse d'infrastructure de NetScaler Console, vous pouvez :

- Afficher un nouvel ensemble de problèmes opérationnels qui se produisent dans les instances NetScaler.
- Afficher les messages d'erreur et consulter les recommandations pour résoudre les problèmes.

En tant qu'administrateur, vous pouvez rapidement identifier l'analyse des causes profondes des problèmes.

REMARQUE

Les indicateurs de règles ne sont pas pris en charge pour :

- Les instances NetScaler configurées en mode cluster.
- Les instances NetScaler configurées avec des partitions d'administration.

Dans NetScaler Console, accédez à **Infrastructure > Infrastructure Analytics** pour afficher les indicateurs pour :

NOM DE L'INDICATEUR DANS INFRASTRUCTURE ANALYTICS	DESCRIPTION
Échec d'allocation de port	Détecte quand NetScaler utilise un SNIP pour communiquer avec une nouvelle connexion de serveur et que le nombre total de ports disponibles sur ce SNIP est épuisé. L'action recommandée est d'ajouter un autre SNIP dans le même sous-réseau.
Aucune configuration de route par défaut	Détecte quand le trafic est abandonné en raison de l'indisponibilité des routes.
Conflit d'adresses IP	Détecte si une même adresse IP est configurée ou appliquée sur deux instances ou plus dans un réseau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE L'INDICATEUR DANS INFRASTRUCTURE ANALYTICS	DESCRIPTION
Conflit de VRID	Détecte quand des problèmes d'accès intermittents se produisent pour le VRID spécifié.
Incompatibilité de VLAN	Détecte si des erreurs se produisent lors de la configuration VLAN liée aux sous-réseaux IP.
Attaque par petite fenêtre TCP	Détecte quand une attaque par petite fenêtre est potentiellement en cours. Cette alerte est uniquement informative, car NetScaler atténue déjà cette attaque.
Seuil de contrôle de débit	Détecte quand des paquets sont abandonnés en fonction du seuil de contrôle de débit configuré.
Limite de persistance	Détecte quand le nombre maximal d'accès est imposé à la mémoire NetScaler.
Incompatibilité de nom de site GSLB	Détecte quand des échecs de synchronisation de configuration GSLB se produisent en raison d'une incompatibilité de nom de site.
En-tête IP malformé	Détecte les échecs des contrôles de cohérence sur les paquets IPv4.
Sommes de contrôle L4 incorrectes	Détecte les échecs de validation de la somme de contrôle pour les paquets TCP.
Augmentation de l'utilisation du CPU due au déplacement d'IP	Détecte si un grand nombre de MAC doivent être mis à jour.
Direction excessive des paquets	Détecte des niveaux élevés de direction logicielle des paquets en raison de l'utilisation d'un type de clé RSS asymétrique.
Boucle de couche 2	Détecte la présence de boucles de couche 2 dans le réseau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE L'INDICATEUR DANS INFRASTRUCTURE ANALYTICS	DESCRIPTION
Incompatibilité VLAN étiqueté	Détecte la réception de paquets VLAN étiquetés sur une interface non étiquetée.



Vue tabulaire

Vous pouvez également afficher les anomalies à l'aide de l'option de vue tabulaire dans **Infrastructure Analytics**. Accédez à **Infrastructure > Infrastructure Analytics**, puis cliquez sur

pour afficher toutes les instances gérées. Cliquez sur

pour développer les détails.



Afficher les détails d'une anomalie

Par exemple, si vous souhaitez afficher les détails d'un **conflit d'adresses IP** dans le réseau, cliquez sur l'anomalie affichée pour le conflit d'adresses IP afin d'en afficher les détails.



- **Détails** - Indique quelle anomalie est détectée
- **Message de détection** - Indique l'adresse MAC pour laquelle l'adresse IP présente le conflit
- **Recommandations** - Indique l'élément d'action pour résoudre ce conflit d'adresses IP

Gestion des instances

Les instances sont des appliances Citrix NetScaler que vous pouvez gérer, surveiller et dépanner à l'aide de NetScaler Console. Vous devez ajouter des instances à NetScaler Console pour les surveiller. Les instances peuvent être ajoutées lors de la configuration initiale de NetScaler Console ou ultérieurement. Une fois les instances ajoutées à NetScaler Console, elles sont interrogées en continu pour collecter des informations qui pourront ensuite être utilisées pour résoudre des problèmes ou comme données de rapport.

Les instances peuvent être regroupées en tant que groupe statique ou en tant que bloc d'adresses IP privées. Un groupe statique d'instances peut être utile lorsque vous souhaitez exécuter des tâches spécifiques telles que des travaux de configuration, etc. Un bloc d'adresses IP privées regroupe vos instances en fonction de leur emplacement géographique.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter une instance

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler Console ou ultérieurement. Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance NetScaler, ou une plage d'adresses IP.

Pour savoir comment ajouter une instance à NetScaler Console, consultez Ajouter des instances à NetScaler Console.

Lorsque vous ajoutez une instance au serveur NetScaler Console, le serveur s'ajoute implicitement en tant que destination de trap pour l'instance et collecte l'inventaire de l'instance. Pour en savoir plus, consultez Comment NetScaler Console découvre les instances.

Après avoir ajouté une instance, vous pouvez la supprimer en accédant à **Infrastructure > Instances** et en cliquant sur **Toutes les instances**. Sur la page Instances, sélectionnez l'instance que vous souhaitez supprimer et cliquez sur **Supprimer**.

Comment utiliser le tableau de bord des instances

Le tableau de bord par instance dans NetScaler Console affiche les données sous forme tabulaire et graphique pour l'instance sélectionnée. Les données collectées à partir de votre instance pendant le processus d'interrogation sont affichées sur le tableau de bord.

Par défaut, les instances gérées sont interrogées toutes les minutes pour la collecte de données. Des informations statistiques telles que l'état, les requêtes HTTP par seconde, l'utilisation du CPU, l'utilisation de la mémoire et le débit sont collectées en continu à l'aide d'appels NITRO. En tant qu'administrateur, vous pouvez afficher toutes ces données collectées sur une seule page, identifier les problèmes dans l'instance et prendre des mesures immédiates pour les corriger.

Pour afficher le tableau de bord d'une instance spécifique, accédez à **Infrastructure > Instances**. À partir du résumé, choisissez le type d'instance, puis sélectionnez l'instance que vous souhaitez afficher et cliquez sur **Tableau de bord**.

L'illustration suivante donne un aperçu des différentes données affichées sur le tableau de bord par instance :



- **Vue d'ensemble**. L'onglet Vue d'ensemble affiche l'utilisation du CPU et de la mémoire de l'instance choisie. Vous pouvez également afficher les événements générés par l'instance et les données de débit. Des informations spécifiques à l'instance telles que l'adresse IP, ses versions matérielles et LOM, les détails du profil, le numéro de série, la personne de contact,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

etc., sont également affichées ici. En faisant défiler vers le bas, les fonctionnalités sous licence disponibles sur l'instance choisie ainsi que les modes configurés sur celle-ci.

Pour plus d'informations, consultez Détails de l'instance.

- **Tableau de bord SSL**. Vous pouvez utiliser l'onglet SSL du tableau de bord par instance pour afficher ou surveiller les détails des certificats SSL, des serveurs virtuels SSL et des protocoles SSL de l'instance choisie. Vous pouvez cliquer sur les « chiffres » dans les graphiques pour afficher plus de détails.
- **Audit de configuration**. Vous pouvez utiliser l'onglet d'audit de configuration pour afficher toutes les modifications de configuration qui se sont produites sur l'instance choisie. Les graphiques **État de la configuration NetScaler® enregistrée** et **Dérive de la configuration NetScaler** du tableau de bord affichent des détails de haut niveau sur les modifications de configuration entre les configurations enregistrées et non enregistrées.
- **Fonctions réseau**. À l'aide du tableau de bord des fonctions réseau, vous pouvez surveiller l'état des entités configurées sur l'instance NetScaler sélectionnée. Vous pouvez afficher des graphiques pour vos serveurs virtuels qui affichent des données telles que les connexions client, le débit et les connexions serveur.
- **Utilisation du réseau**. Vous pouvez afficher les données de performances réseau de l'instance sélectionnée dans l'onglet Utilisation du réseau. Vous pouvez afficher des rapports pour une heure, un jour, une semaine ou un mois. La fonction de curseur de chronologie peut être utilisée pour personnaliser la durée des rapports réseau générés. Par défaut, seuls huit rapports sont affichés, mais vous pouvez cliquer sur l'icône « plus » dans le coin inférieur droit de l'écran pour ajouter un rapport de performances supplémentaire.

Surveiller les sites répartis mondialement

En tant qu'administrateur réseau, vous pourriez avoir à surveiller et gérer des instances réseau déployées sur différentes zones géographiques. Cependant, il n'est pas facile d'évaluer les exigences du réseau lors de la gestion d'instances réseau dans des centres de données géographiquement distribués.

Les géocartes dans NetScaler Console vous offrent une représentation graphique de vos sites et décomposent votre expérience de surveillance réseau par géographie. Avec les géocartes, vous pouvez visualiser la distribution de vos instances réseau par emplacement et surveiller les problèmes réseau.

La section suivante explique comment vous pouvez surveiller les centres de données dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un site NetScaler Console est un regroupement logique d'instances Citrix NetScaler dans un emplacement géographique spécifique. Par exemple, un site est attribué à Amazon Web Services (AWS) et un autre site peut être attribué à Azure. Un autre site encore est hébergé sur les locaux du locataire. NetScaler Console gère et surveille toutes les instances NetScaler connectées à tous les sites. Vous pouvez utiliser NetScaler Console pour surveiller et collecter les données syslog, AppFlow, SNMP et toute autre donnée provenant des instances gérées.

Les géocartes dans NetScaler Console vous offrent une représentation graphique de vos sites. Les géocartes décomposent également votre expérience de surveillance réseau par géographie. Avec les géocartes, vous pouvez visualiser la distribution de vos instances réseau par emplacement et surveiller tous les problèmes réseau. Vous pouvez accéder à la page **Infrastructure > Instances** pour une représentation visuelle des sites créés sur la carte du monde.

Cas d'utilisation

Une entreprise de téléphonie mobile de premier plan, ExampleCompany, s'appuyait sur des fournisseurs de services privés pour héberger ses ressources et applications. L'entreprise disposait déjà de deux sites : l'un à Minneapolis aux États-Unis et l'autre à Alice Springs en Australie. Dans cette image, vous pouvez voir que deux marqueurs représentent les deux sites existants.



Les marqueurs affichent également un nombre, qui indique le nombre d'applications sur chaque site. Vous pouvez cliquer sur ces marqueurs pour obtenir plus d'informations sur chaque site.



Cliquez sur les onglets pour afficher plus d'informations :

- Onglet **Instances** : Affichez les éléments suivants dans cet onglet :
  - Adresse IP de chaque instance réseau
  - Type de l'instance
  - Nombre d'événements critiques sur ceux-ci
  - Événements significatifs et tous les événements générés sur une instance NetScaler.
- Onglet **Événements** : Affichez une liste des événements critiques et significatifs générés sur les instances.
- Onglet **Certificats** : Affichez les éléments suivants dans cet onglet :
  - Liste des certificats de toutes les instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Statut d'expiration
- Informations vitales et les 10 premières instances par nombre de certificats utilisés.

- Onglet **Agents** : Affichez une liste des agents auxquels les instances sont liées.



Configuration des géocartes

ExampleCompany a décidé de créer un troisième site à Bangalore, en Inde. L'entreprise souhaitait tester le cloud en déchargeant certaines de ses applications informatiques internes moins critiques vers le bureau de Bangalore. L'entreprise a décidé d'utiliser les services de cloud computing AWS.

En tant qu'administrateur, vous devez d'abord créer un site, puis ajouter les instances NetScaler dans NetScaler Console. Vous devez également ajouter l'instance au site, ajouter un agent et lier l'agent au site. NetScaler Console reconnaît alors le site auquel appartiennent l'instance NetScaler et l'agent.

Pour plus d'informations sur l'ajout d'instances NetScaler, consultez Ajout d'instances.

Pour créer des sites :

Créez des sites avant d'ajouter des instances dans NetScaler Console. La fourniture d'informations de localisation vous permet de localiser le site avec précision.

Accédez à **Infrastructure > Instances > Sites**, puis cliquez sur **Ajouter**.

1. Dans la page **Créer un site**, spécifiez les informations suivantes :

   a. **Type de site** : Sélectionnez **Centre de données**.

   REMARQUE

   Le site peut fonctionner comme centre de données principal ou comme succursale. Choisissez en conséquence.

   b. **Type** : Sélectionnez AWS comme fournisseur de cloud dans la liste.

   REMARQUE

   Cochez la case **Utiliser le VPC existant comme site** en conséquence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **Nom du site** : Saisissez le nom du site.

d. **Ville** : Saisissez la ville.

e. **Code postal** : Saisissez le code postal.

f. **Région** : Saisissez la région.

g. **Pays** : Saisissez le pays

h. **Latitude** : Saisissez la latitude de l'emplacement.

i. **Longitude** : Saisissez la longitude de l'emplacement.

2. Cliquez sur **Créer**.



Pour ajouter des instances et sélectionner des sites :

Après avoir créé des sites, vous devez ajouter des instances dans NetScaler Console. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

Après avoir créé des sites, vous devez ajouter des instances dans NetScaler Console. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

1. Dans NetScaler Console, accédez à **Infrastructure > Instances**.
2. Sélectionnez le type d'instance que vous souhaitez créer, puis cliquez sur **Ajouter**.
3. Sur la page **Ajouter NetScaler VPX**, saisissez l'adresse IP et sélectionnez le profil dans la liste.
4. Sélectionnez le site dans la liste. Vous pouvez cliquer sur le signe + en regard du champ **Site** pour créer un site ou cliquer sur l'icône de modification pour modifier les détails du site par défaut.
5. Cliquez sur la flèche droite et sélectionnez l'agent dans la liste qui s'affiche.



6. Après avoir choisi l'agent, vous devez associer l'agent au site. Cette étape permet de lier l'agent au site. Sélectionnez l'agent et cliquez sur **Attacher le site**.



Sélectionnez le site dans la liste et cliquez sur **Enregistrer**.

Cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également attacher un agent à un site en naviguant vers **Infrastructure > Instances > Agents**.

Pour associer un agent NetScaler au site :

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > Agents**.
2. Sélectionnez l'agent, puis cliquez sur **Attacher le site**.



\1. Vous pouvez associer le site et cliquer sur **Enregistrer**.

NetScaler Console commence à surveiller les instances NetScaler ajoutées sur le site de Bangalore, ainsi que les instances des deux autres sites.

Comment créer des balises et les attribuer aux instances

NetScaler Console vous permet désormais d'associer vos instances Citrix NetScaler à des balises. Une balise est un mot-clé ou un terme d'un seul mot que vous pouvez attribuer à une instance. Les balises ajoutent des informations supplémentaires sur l'instance. Les balises peuvent être considérées comme des métadonnées qui aident à décrire une instance. Les balises vous permettent de classer et de rechercher des instances en fonction de ces mots-clés spécifiques. Vous pouvez également attribuer plusieurs balises à une seule instance.

Les cas d'utilisation suivants vous aident à comprendre comment le balisage des instances vous aide à mieux les surveiller.

- **Cas d'utilisation 1** : Vous pouvez créer une balise pour identifier toutes les instances au Royaume-Uni. Ici, vous pouvez créer une balise avec la clé « Pays » et la valeur « Royaume-Uni ». Cette balise vous aide à rechercher et à surveiller toutes ces instances au Royaume-Uni.
- **Cas d'utilisation 2** : Vous souhaitez rechercher des instances qui se trouvent dans l'environnement de préproduction. Ici, vous pouvez créer une balise avec la clé « Objectif » et la valeur « Staging_NS ». Cette balise vous aide à séparer toutes les instances utilisées dans l'environnement de préproduction des instances qui traitent les requêtes client.
- **Cas d'utilisation 3** : Imaginez une situation où vous souhaitez trouver la liste des instances NetScaler qui se trouvent dans la zone « Swindon » au Royaume-Uni et qui vous appartiennent, David T. Vous pouvez créer des balises pour toutes ces exigences et les attribuer à toutes les instances qui remplissent ces conditions.

Pour attribuer des balises à l'instance NetScaler VPX :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > NetScaler**.
2. Sélectionnez l'onglet **NetScaler VPX**.
3. Sélectionnez l'instance NetScaler VPX requise.
4. Cliquez sur **Balises**.
5. Créez des balises et cliquez sur **OK**.

La fenêtre **Balises** qui apparaît vous permet de créer vos propres paires « clé-valeur » en attribuant des valeurs à chaque mot-clé que vous créez.

Par exemple, les images suivantes montrent quelques mots-clés créés et leurs valeurs. Vous pouvez ajouter vos propres mots-clés et saisir une valeur pour chacun d'eux.

Vous pouvez également ajouter plusieurs balises en cliquant sur « + ». L'ajout de balises multiples et significatives vous permet de rechercher efficacement les instances.

Vous pouvez ajouter plusieurs valeurs à un mot-clé en les séparant par des virgules.

Par exemple, vous attribuez le rôle d'administrateur à un autre collègue, Greg T. Vous pouvez ajouter son nom séparé par une virgule. L'ajout de plusieurs noms vous aide à effectuer une recherche par l'un ou l'autre des noms, ou par les deux noms. NetScaler Console reconnaît les valeurs séparées par des virgules comme deux valeurs différentes.

Pour en savoir plus sur la recherche d'instances basée sur des balises, consultez Comment rechercher des instances à l'aide des valeurs des balises et des propriétés.

REMARQUE

Vous pouvez ultérieurement ajouter de nouvelles balises ou supprimer des balises existantes. Il n'y a aucune restriction sur le nombre de balises que vous créez.

Comment rechercher des instances en utilisant les valeurs des balises et des propriétés

Il peut arriver que NetScaler Console gère de nombreuses instances NetScaler. En tant qu'administrateur, vous pourriez souhaiter la flexibilité de rechercher dans l'inventaire des instances en fonction de certains paramètres. NetScaler Console offre désormais une capacité de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

recherche améliorée pour rechercher un sous-ensemble d'instances NetScaler en fonction des paramètres que vous définissez dans le champ de recherche. Vous pouvez rechercher les instances en fonction de deux critères : les balises et les propriétés.

- **Balises**. Les balises sont des termes ou des mots-clés que vous pouvez attribuer à une instance NetScaler pour ajouter une description supplémentaire à cette instance. Vous pouvez désormais associer vos instances NetScaler à des balises. Ces balises peuvent être utilisées pour mieux identifier et rechercher les instances NetScaler.
- **Propriétés**. Chaque instance NetScaler ajoutée dans NetScaler Console possède quelques paramètres ou propriétés par défaut qui lui sont associés. Par exemple, chaque instance a son propre nom d'hôte, adresse IP, version, ID d'hôte, ID de modèle matériel, etc. Vous pouvez rechercher des instances en spécifiant des valeurs pour l'une de ces propriétés.

Par exemple, imaginez une situation où vous souhaitez trouver la liste des instances NetScaler qui sont en version 12.0 et qui sont à l'état UP. Ici, la version et l'état de l'instance sont définis par les propriétés par défaut.

Outre la version 12.0 et l'état UP des instances, vous pouvez également rechercher les instances qui vous appartiennent. Vous pouvez créer une balise « Propriétaire » et lui attribuer la valeur « David T ». Pour plus d'informations sur la création et l'attribution de balises, consultez Comment créer des balises et les attribuer aux instances.

Vous pouvez utiliser une combinaison de balises et de propriétés pour créer vos propres critères de recherche.

Pour rechercher des instances NetScaler VPX

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > NetScaler** > onglet **VPX**.
2. Cliquez sur le champ de recherche. Vous pouvez créer une expression de recherche en utilisant des balises ou des propriétés, ou en combinant les deux.

   Les exemples suivants montrent comment vous pouvez utiliser efficacement l'expression de recherche pour trouver l'instance.

   a. Sélectionnez l'option **Balises** et sélectionnez **Propriétaire**. Sélectionnez « David T. »

   NetScaler Console prend en charge les expressions régulières et les caractères génériques dans les expressions de recherche.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Vous pouvez utiliser des expressions régulières pour étendre davantage les critères de recherche. Par exemple, vous souhaitez rechercher des instances appartenant à David ou à Stephen. Dans ce cas, vous pouvez saisir les valeurs en les séparant par une expression « \| ».



c. Vous pouvez également utiliser des caractères génériques pour remplacer ou représenter un ou plusieurs caractères. Par exemple, vous pouvez taper `Dav*` pour rechercher toutes les instances appartenant à David T et Dave P.



REMARQUE

Pour plus d'informations sur les expressions régulières et les caractères génériques et comment les utiliser, cliquez sur l'icône « informations » dans la barre de recherche.

Mises à jour centralisées de la base de données GeoIP via NetScaler® Console

NetScaler Console permet aux administrateurs de télécharger le fichier GeoIP DB (base de données de géolocalisation) depuis MaxMind directement via NetScaler Console. Vous pouvez soit pousser le fichier GeoIP DB immédiatement vers les instances NetScaler gérées, soit planifier la mise à jour pour plus tard. Ces fichiers sont essentiels pour un mappage IP-vers-localisation précis, couramment utilisé dans les politiques GSLB et de sécurité.

Cette amélioration vous offre également le suivi de l'historique des mises à jour, ce qui vous permet de voir si une mise à jour a réussi ou échoué. De plus, vous pouvez afficher, supprimer ou télécharger les versions GeoIP DB précédemment téléchargées ou poussées depuis NetScaler Console. Cette amélioration introduit également la mise à jour manuelle du fichier GeoIP DB dans NetScaler Console, le contrôle de version et les workflows de mise à jour automatisés, permettant des mises à jour GeoIP DB transparentes sans impacter les services GSLB.

Auparavant, NetScaler ne disposait pas de mécanisme centralisé pour gérer les mises à jour de la base de données GeoIP sur NetScaler. Les administrateurs devaient effectuer les mises à jour manuellement sur chaque appareil, ce qui était chronophage, sujet aux erreurs et perturbateur dans les environnements de production.

Cette amélioration offre les avantages suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Automatisation** : Le processus de mise à jour est automatisé et effectué sans temps d'arrêt planifié, ce qui réduit la surcharge opérationnelle.
- **Évolutivité efficace** : La gestion des mises à jour sur plusieurs instances NetScaler est efficace et facile à faire évoluer.
- **Contrôle de version** : En cas de problème, vous pouvez suivre les versions historiques, télécharger et synchroniser un fichier GeoIP DB plus ancien.

Limitations

- **Prise en charge de la conversion de format limitée à MaxMind** : La conversion automatique de format n'est prise en charge que pour les fichiers MaxMind. Pour les autres fournisseurs, les fichiers doivent déjà être dans le format pris en charge.
- **Restriction de suppression** : La suppression d'un fichier en cours d'utilisation n'est pas autorisée. Assurez-vous qu'il n'y a aucune dépendance active avant la suppression.

Configuration des mises à jour centralisées de la base de données GeoIP via NetScaler Console

Prérequis

- Assurez-vous de disposer d'une licence MaxMind valide requise pour utiliser les fichiers GeoIP DB.
- Si vous utilisez le format de fichier pour d'autres fichiers de fournisseurs, assurez-vous que les fichiers sont dans un format pris en charge.

Effectuez les étapes suivantes pour télécharger le fichier GeoIP DB de MaxMind ou de tout autre fournisseur :

1. Accédez à **Infrastructure > Synchronisation GeoIP DB** et cliquez sur **Démarrer**.

   

2. Sélectionnez l'une des options suivantes :

   - **Télécharger un nouveau fichier** : Vous pouvez télécharger un fichier depuis votre système local.
   - **Utiliser un fichier existant** : Vous pouvez choisir un fichier déjà présent sur une console NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Si vous téléchargez le fichier GeoIP DB pour la première fois, l'option **Utiliser un fichier existant** n'apparaît pas. Ce n'est que si le fichier est déjà téléchargé que l'option **Utiliser un fichier existant** apparaît lors des téléchargements ultérieurs.
- Si vous téléchargez un fichier MaxMind, le service NetScaler Console convertit automatiquement le fichier au format recommandé par NetScaler pendant le téléchargement. Si vous téléchargez un fichier d'autres fournisseurs, il doit être au format CSV et respecter l'ordre des champs suivant recommandé par NetScaler : plage d'adresses IP, code de pays, région, ville.

3. Une fois le fichier téléchargé, vous pouvez effectuer l'une des actions suivantes :

   - Cliquez sur **Synchroniser maintenant**, puis sur **Démarrer la synchronisation** : Toutes les instances NetScaler sont mises à jour immédiatement.
   - Cliquez sur **Créer un calendrier** - Vous pouvez sélectionner une date et une heure futures pour la mise à jour des instances NetScaler.

   

4. Affichez la progression de la synchronisation et l'état de la synchronisation par instance sur la page **Synchronisation GeoIP DB**.

   

5. Selon vos besoins, vous pouvez effectuer les actions suivantes :

   - **Sélectionner un nouveau fichier** : Cliquez sur **Sélectionner un nouveau fichier** pour télécharger un fichier de base de données GeoIP depuis votre machine locale ou sélectionner un fichier déjà téléchargé depuis NetScaler Console.
   - **Afficher les informations du fichier** : Cliquez sur **Afficher les informations du fichier** pour afficher les fichiers précédemment téléchargés. En cas de problème, vous pouvez suivre les versions historiques, télécharger et synchroniser un ancien fichier de base de données GeoIP.
   - **Planification active** : Cliquez sur **Planification active** pour afficher les planifications à venir qui n'ont pas encore été exécutées.
   - **Planification historique** : Cliquez sur **Planification historique** pour afficher les activités de synchronisation de la base de données GeoIP précédentes qui sont terminées.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gérer les partitions d'administration des instances NetScaler

Vous pouvez configurer des partitions d'administration sur vos instances Citrix NetScaler afin que différents groupes de votre organisation se voient attribuer différentes partitions sur la même instance NetScaler. Un administrateur réseau peut être affecté à la gestion de plusieurs partitions sur plusieurs instances NetScaler.

NetScaler Console offre un moyen transparent de gérer toutes les partitions appartenant à un administrateur à partir d'une seule console. Vous pouvez gérer ces partitions sans perturber les autres configurations de partition.

Pour permettre à plusieurs utilisateurs de gérer différentes partitions d'administration, vous devez créer des groupes, puis attribuer des utilisateurs et des partitions à ces groupes. Chaque utilisateur ne peut afficher et gérer que les partitions du groupe auquel il appartient. Chaque partition d'administration est considérée comme une instance dans NetScaler Console. Lorsque vous découvrez une instance NetScaler, les partitions d'administration configurées sur cette instance NetScaler sont automatiquement ajoutées au système.

Considérez que vous avez deux instances NetScaler VPX avec deux partitions configurées sur chaque instance. Par exemple, l'instance NetScaler 10.102.216.49 a Partition_1, Partition_2 et Partition_3, et l'instance NetScaler 10.102.29.120 a p1 et p2 comme indiqué dans l'image suivante.

Pour afficher les partitions, accédez à **Infrastructure > Instances > NetScaler > VPX**, puis cliquez sur **Partitions**.

Vous pouvez attribuer à user-p1 les partitions suivantes : 10.102.29.120-p1 et 10.102.216.49-Partition_1. Et vous pouvez attribuer à user-p2 la gestion des partitions 10.102.29.80-p2, 10.102.216.49-Partition_2 et 10.102.216.49-Partition_3.

Ensuite, vous devez créer les deux utilisateurs, user-p1 et user-p2, et vous devez attribuer les utilisateurs aux groupes que vous avez créés pour eux.

Tout d'abord, vous devez créer deux groupes avec les autorisations appropriées (exemple : autorisations d'administrateur) et inclure les instances de partition d'administration requises dans chaque groupe. Par exemple, créez le groupe système partition1-admin et ajoutez les partitions d'administration NetScaler 10.102.29.120-p1 et 10.102.216.49-Partition_1 à ce groupe. Créez également le groupe système partition2-admin et ajoutez les partitions d'administration NetScaler 10.102.29.120-p2, 10.102.216.49-Partition_2 et 10.102.216.49-Partition_3 à ce groupe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir créé la partition d'administration, vous pouvez également utiliser la fonctionnalité de différence d'historique des révisions et le modèle d'audit pour la fonctionnalité de partition d'administration à des fins d'audit.

La **différence d'historique des révisions** pour la partition d'administration vous permet d'afficher la différence entre les cinq derniers fichiers de configuration d'une instance NetScaler partitionnée. Vous pouvez comparer les fichiers de configuration entre eux (par exemple, Révision de configuration - 1 avec Révision de configuration - 2) ou par rapport à la configuration en cours d'exécution/enregistrée avec la Révision de configuration. Outre les différences de configuration, les configurations de correction sont également affichées. Vous pouvez exporter toutes les commandes correctives vers votre dossier local et corriger les configurations.

Pour afficher la différence d'historique des révisions :

1. Accédez à **Infrastructure > Audit de configuration.** Cliquez à l'intérieur du graphique en anneau qui représente l'état de la configuration de l'instance. Dans la page **Rapports d'audit** qui s'ouvre, cliquez sur l'instance NetScaler partitionnée.

   

2. Dans le menu **Action**, cliquez sur **Diff. historique des révisions.**

   

3. Sur la page **Différence de l'historique des révisions**, sélectionnez les fichiers que vous souhaitez comparer. Par exemple, comparez la configuration enregistrée avec la révision de configuration -1, puis cliquez sur **Afficher la différence de configuration**.

   

4. Vous pouvez ensuite afficher la différence entre les cinq derniers fichiers de configuration pour l'instance NetScaler partitionnée sélectionnée, comme indiqué ci-dessous. Vous pouvez également afficher les commandes de configuration correctives et les exporter vers votre dossier local. Ces commandes correctives sont les commandes qui doivent être exécutées sur le fichier de base afin d'amener la configuration à l'état souhaité (fichier de configuration utilisé pour la comparaison).

   

Modèles d'audit pour partition vous permettent de créer un modèle de configuration personnalisé et de l'associer à une instance de partition. Toute variation dans la configuration en cours d'exécution de l'instance par rapport au modèle d'audit est affichée dans la colonne **Différence modèle vs exécution** de la page **Rapports d'audit**. Outre les différences de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configuration, les configurations de correction sont également affichées. Vous pouvez également exporter toutes les commandes correctives vers votre dossier local et corriger les configurations.

Pour afficher la différence entre le modèle et l'exécution :

1. Depuis la page **Rapports d'audit**, cliquez sur l'instance NetScaler partitionnée.

   

2. S'il existe une différence entre le modèle d'audit et la différence d'exécution, la différence est affichée sous forme de lien hypertexte. Cliquez sur le lien hypertexte pour afficher les différences, le cas échéant. Outre les différences de configuration, les configurations de correction sont également affichées. Vous pouvez également exporter toutes les commandes correctives vers votre dossier local et corriger les configurations.

Pour créer des groupes :

1. Accédez à **Paramètres > Administration des utilisateurs > Groupes**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer un utilisateur système**, spécifiez les éléments suivants :

   - Onglet **Paramètres du groupe** : Saisissez le nom du groupe et les autorisations de rôle. Pour autoriser l'accès à des instances spécifiques, décochez la case **Toutes les instances**, puis choisissez vos instances sur la page **Sélectionner les instances**.
   - Onglet **Applications et modèles** : Vous pouvez choisir d'utiliser ce groupe pour toutes les applications et tous les modèles de configuration.
   - Onglet **Sélectionner les utilisateurs** : Sélectionnez les utilisateurs que vous souhaitez ajouter à ce groupe. Vous pouvez cliquer sur le lien **Nouveau** dans le tableau **Disponible** pour créer de nouveaux utilisateurs. Si vous le souhaitez, configurez le délai d'expiration de la session, où vous pouvez définir la durée pendant laquelle un utilisateur peut rester actif.

3. Cliquez sur **Terminer**.

   

Pour créer des utilisateurs :

1. Accédez à **Paramètres > Administration des utilisateurs > Utilisateurs**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer un utilisateur système**, spécifiez le nom d'utilisateur et le mot de passe. Si vous le souhaitez, vous pouvez activer l'authentification externe et configurer le délai d'expiration de la session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Attribuez l'utilisateur à un groupe en ajoutant le nom du groupe de la liste **Disponible** à la liste **Configuré**.
4. Cliquez sur **Créer**.

Déconnectez-vous maintenant et connectez-vous avec les informations d'identification de l'utilisateur-p1. Vous pouvez afficher et gérer uniquement les partitions d'administration qui vous sont attribuées pour la gestion et la surveillance.

Créer une paire haute disponibilité NetScaler

Une paire haute disponibilité (HA) NetScaler peut assurer un fonctionnement ininterrompu pendant les temps d'arrêt ou les pannes réseau. Vous pouvez créer une paire HA d'instances NetScaler à l'aide de NetScaler Console. Pour plus d'informations, consultez Haute disponibilité NetScaler.

Suivez les étapes suivantes pour créer une paire HA d'instances NetScaler dans NetScaler Console :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Sélectionnez une instance NetScaler dans la liste avec laquelle vous souhaitez créer une paire HA.

   L'instance sélectionnée devient une instance principale dans la paire HA.
3. Cliquez sur Sélectionner **Action > Créer une paire HA**.
4. Dans **Sélection d'instance**, suivez les étapes suivantes :

   a. Dans **Adresse IP secondaire**, cliquez pour sélectionner une instance secondaire.

   b. Sélectionnez une instance NetScaler que vous souhaitez configurer comme secondaire dans la paire HA.

   c. Facultatif, sélectionnez **Activer le mode INC (Independent Network Configuration)** si les instances de la paire HA se trouvent dans deux sous-réseaux.

   d. Cliquez sur **Suivant**.

   
5. Dans **Exécuter**, vous pouvez décider de créer une paire HA maintenant ou plus tard.

   a. Dans **Mode d'exécution**, sélectionnez l'un des modes d'exécution suivants :

   - **Maintenant** - Sélectionnez cette option pour créer une paire HA maintenant.
   - **Plus tard** - Sélectionnez cette option pour créer une paire HA à une date et une heure spécifiques.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Si vous avez sélectionné **Plus tard** dans la liste **Mode d'exécution**, sélectionnez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez exécuter cette tâche.

REMARQUE

L'heure d'exécution est affichée dans le fuseau horaire défini dans NetScaler Console.

Vous pouvez recevoir un rapport d'exécution de cette tâche par les moyens suivants :

- **E-mail** - Sélectionnez la distribution par e-mail dans la liste.

  Pour ajouter une liste de distribution, cliquez sur **Ajouter**. Spécifiez les paramètres requis pour ajouter la liste de distribution et cliquez sur **Créer**.

- **Slack** - Sélectionnez le profil Slack dans la liste.

  Pour ajouter un profil Slack, cliquez sur **Ajouter**. Spécifiez le **Nom du profil**, le **Nom du canal** et le **Jeton**, puis cliquez sur **Créer**.

Sauvegarder et restaurer les instances NetScaler

Vous pouvez sauvegarder l'état actuel d'une instance NetScaler et utiliser ultérieurement les fichiers sauvegardés pour la restaurer au même état. Sauvegardez toujours une instance avant de la mettre à niveau ou par mesure de précaution. Une sauvegarde d'un système stable vous permet de le restaurer à un point stable s'il devient instable.

Il existe plusieurs façons d'effectuer des sauvegardes et des restaurations sur une instance NetScaler. Vous pouvez sauvegarder et restaurer manuellement les configurations NetScaler à l'aide de l'interface graphique et de la CLI. Vous pouvez également utiliser NetScaler Console pour effectuer des sauvegardes automatiques et des restaurations manuelles.

NetScaler Console sauvegarde l'état actuel de vos instances NetScaler gérées en utilisant les appels NITRO et les protocoles Secure Shell (SSH) et Secure Copy (SCP).

NetScaler Console crée une sauvegarde complète et restaure les types d'instances NetScaler suivants :

- NetScaler SDX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

REMARQUE :

- Assurez-vous que le profil NetScaler Console dispose des droits d'administrateur pour sauvegarder et restaurer les instances NetScaler.
- Depuis NetScaler Console, vous ne pouvez pas effectuer l'opération de sauvegarde et de restauration sur un cluster NetScaler.
- Vous ne pouvez pas utiliser le fichier de sauvegarde d'une instance pour restaurer une instance différente.

Les fichiers sauvegardés sont stockés sous forme de fichier TAR compressé dans le répertoire suivant :

```
/var/mps/tenants/root/device_backup/
```

Pour éviter les problèmes dus au manque d'espace disque, vous pouvez enregistrer un maximum de 50 fichiers de sauvegarde par instance NetScaler dans ce répertoire.

Pour sauvegarder et restaurer les instances NetScaler, vous devez d'abord configurer les paramètres de sauvegarde sur NetScaler Console. Après avoir configuré les paramètres, vous pouvez sélectionner une seule instance NetScaler ou plusieurs instances et créer une sauvegarde des fichiers de configuration de ces instances. Si nécessaire, vous pouvez également restaurer les instances NetScaler à l'aide de ces fichiers de sauvegarde.

Configurer les paramètres de sauvegarde des instances

La page **Paramètres de sauvegarde des instances** vous permet de configurer les paramètres sur NetScaler Console pour sauvegarder une instance NetScaler sélectionnée ou plusieurs instances :

1. Dans NetScaler Console, accédez à **Paramètres** \> **Administration**.
2. Dans **Sauvegarde**, sélectionnez **Configurer la sauvegarde du système et des instances**.
3. Sélectionnez **Instance** et spécifiez les éléments suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Activer les sauvegardes d'instances** : Par défaut, NetScaler Console est activé pour la sauvegarde des instances NetScaler. Désactivez cette option si vous ne souhaitez pas créer de fichiers de sauvegarde pour les instances.
- **Protéger le fichier par mot de passe** : (facultatif) Sélectionnez l'option de protection par mot de passe pour chiffrer le fichier de sauvegarde. Le chiffrement du fichier de sauvegarde garantit la sécurité de toutes les informations sensibles contenues dans le fichier de sauvegarde.

  REMARQUE :

  Vous pouvez télécharger le fichier de sauvegarde chiffré sur votre machine locale, mais vous ne pouvez pas l'ouvrir avec l'interface graphique de NetScaler Console ni avec un éditeur de texte. Il vous sera demandé de fournir le mot de passe lors de la restauration du fichier de sauvegarde chiffré. Vous pouvez, cependant, ouvrir un fichier de sauvegarde non chiffré sur votre système.

- **Nombre de fichiers de sauvegarde à conserver** : Spécifiez le nombre de fichiers de sauvegarde à conserver dans NetScaler Console. Vous pouvez conserver jusqu'à 50 fichiers de sauvegarde par instance NetScaler. La valeur par défaut est trois fichiers de sauvegarde.

  REMARQUE :

  Chaque fichier de sauvegarde représente une certaine exigence de stockage. Nous vous recommandons de stocker un nombre optimal de fichiers de sauvegarde NetScaler sur NetScaler Console, selon vos besoins.

  

- **Paramètres de planification de la sauvegarde** : (facultatif) Deux options sont disponibles pour la création de fichiers de sauvegarde, bien que vous ne puissiez utiliser qu'une seule option à la fois :

  a. L'option de planification de sauvegarde par défaut est « basée sur un intervalle ». Un fichier de sauvegarde est créé dans NetScaler Console après l'expiration de l'intervalle spécifié. L'intervalle de sauvegarde par défaut est de 12 heures.

  b. Vous pouvez également modifier le type de sauvegardes planifiées en « basées sur l'heure ». Dans cette option, spécifiez l'heure au format `hours:minutes` pour

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sauvegarder les instances à l'heure spécifiée. NetScaler Console autorise un maximum de quatre sauvegardes quotidiennes sur les instances.

- **Paramètres NetScaler** : (facultatif) Par défaut, NetScaler Console ne crée pas de fichier de sauvegarde lorsqu'il reçoit le trap « NetScalerConfigSave ». Cependant, vous pouvez activer l'option de créer un fichier de sauvegarde chaque fois qu'une instance NetScaler envoie un trap « NetScalerConfigSave » à NetScaler Console. Une instance NetScaler envoie « NetScalerConfigSave » chaque fois que la configuration de l'instance est enregistrée.
- **Fichiers de géodatabase** : (facultatif) Par défaut, NetScaler Console ne sauvegarde pas les fichiers de géodatabase. Vous pouvez activer l'option de créer également une sauvegarde de ces fichiers.
- **Transfert externe** : (facultatif) NetScaler Console vous permet de transférer les fichiers de sauvegarde de l'instance NetScaler vers un emplacement externe :

  a. Spécifiez l'adresse IP de l'emplacement.

  b. Spécifiez le nom d'utilisateur et le mot de passe du serveur externe vers lequel vous souhaitez transférer les fichiers de sauvegarde.

  c. Spécifiez le protocole de transfert et le numéro de port.

  d. Vous pouvez spécifier le chemin du répertoire où le fichier doit être stocké.

  e. Facultatif, vous pouvez également supprimer le fichier de sauvegarde de NetScaler Console après l'avoir transféré vers le serveur externe.

REMARQUE

.

NetScaler Console s'envoie un trap SNMP ou une notification Syslog en cas d'échec de sauvegarde pour l'une des instances NetScaler sélectionnées.

Créer une sauvegarde pour une instance NetScaler sélectionnée à l'aide de NetScaler Console

Effectuez cette tâche si vous souhaitez sauvegarder une instance NetScaler sélectionnée ou plusieurs instances :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans NetScaler Console, accédez à **Infrastructure > Instances**. Sous **Instances**, sélectionnez le type d'instances (par exemple, NetScaler VPX) à afficher à l'écran.
2. Sélectionnez l'instance que vous souhaitez sauvegarder.
   - Pour les instances MPX, VPX et BLX, sélectionnez **Sauvegarde/Restauration** dans la liste **Sélectionner une action**.
   - Pour une instance SDX, cliquez sur **Sauvegarde/Restauration**.
3. Sur la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.
4. Vous pouvez spécifier si vous souhaitez chiffrer votre fichier de sauvegarde pour plus de sécurité. Vous pouvez soit saisir votre mot de passe, soit utiliser le mot de passe global que vous avez précédemment spécifié sur la page Paramètres de sauvegarde d'instance.
5. Cliquez sur **Continuer**.

Restaurer une instance NetScaler à l'aide de NetScaler Console

REMARQUE :

Si vous avez des instances NetScaler dans une paire HA, vous devez noter ce qui suit :

- Restaurez la même instance à partir de laquelle le fichier de sauvegarde a été créé. Par exemple, considérons un scénario où une sauvegarde a été effectuée à partir de l'instance principale de la paire HA. Pendant le processus de restauration, assurez-vous de restaurer la même instance, même si elle n'est plus l'instance principale.
- Lorsque vous lancez le processus de restauration sur l'instance NetScaler principale, vous ne pouvez pas accéder à l'instance principale et l'instance secondaire passe à l'état **STAYSECONDARY**. Une fois le processus de restauration terminé sur l'instance principale, l'instance NetScaler secondaire passe du mode **STAYSECONDARY** au mode **ENABLED** et redevient une partie de la paire HA. Vous pouvez vous attendre à une éventuelle interruption de service sur l'instance principale jusqu'à ce que le processus de restauration soit terminé.

Effectuez cette tâche pour restaurer une instance NetScaler à l'aide du fichier de sauvegarde que vous avez créé précédemment :

1. Accédez à **Infrastructure > Instances**, sélectionnez l'instance que vous souhaitez restaurer, puis cliquez sur **Sélectionner l'action > Sauvegarder/Restaurer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sur la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde contenant les paramètres que vous souhaitez restaurer, puis cliquez sur **Restaurer**.



Restaurer une appliance NetScaler SDX à l'aide de NetScaler Console

Dans NetScaler Console, la sauvegarde de l'appliance NetScaler SDX inclut les éléments suivants :

- Instances NetScaler hébergées sur l'appliance
- Certificats et clés SSL SVM
- Paramètres d'élagage d'instance (au format XML)
- Paramètres de sauvegarde d'instance (au format XML)
- Paramètres d'interrogation des certificats SSL (au format XML)
- Fichier db SVM
- Fichiers de configuration NetScaler des périphériques présents sur SDX
- Images de build NetScaler
- Images XVA NetScaler, ces images sont stockées à l'emplacement suivant : `/var/mps/sdx_images/`
- Image de bundle unique SDX (SVM+XS)
- Images d'instances tierces (si provisionnées)

Restaurez votre appliance NetScaler SDX à la configuration disponible dans le fichier de sauvegarde. Pendant la restauration de l'appliance, l'intégralité de la configuration actuelle est supprimée.

Si vous restaurez l'appliance NetScaler SDX à l'aide d'une sauvegarde d'une autre appliance NetScaler SDX, assurez-vous d'ajouter les licences et de configurer les paramètres réseau du service de gestion de la nouvelle appliance pour qu'ils correspondent aux paramètres du fichier de sauvegarde avant de démarrer le processus de restauration. Autrement dit, la nouvelle appliance doit être sous licence et répondre aux exigences minimales de licence du fichier de sauvegarde. Par exemple, si la sauvegarde contenait cinq instances VPX avec un total de 5 Go, la nouvelle appliance doit également être en mesure de prendre en charge ces exigences. Ou si l'appliance de sauvegarde avait une licence Platinum, la nouvelle appliance doit avoir la même licence ou une licence supérieure. Les paramètres réseau, tels que l'adresse IP, le masque de sous-réseau, la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

passerelle, l'adresse IP XenServer et le serveur DNS, doivent être correctement configurés sur la nouvelle appliance.

Avant de restaurer l'appliance SDX, assurez-vous que la variante de plateforme de l'appliance SDX sauvegardée est la même que celle de l'appliance. Vous ne pouvez pas restaurer à partir d'une variante de plateforme différente.

REMARQUE :

Avant de restaurer une appliance SDX RMA, assurez-vous que la version sauvegardée est identique ou supérieure à la version RMA.

Pour restaurer l'appliance SDX à partir du fichier de sauvegarde :

1. Dans l'interface graphique de NetScaler Console, accédez à **Infrastructure > Instances > NetScaler > SDX**. Sélectionnez une instance.
2. Cliquez sur **Sauvegarde/Restauration**.
3. Sélectionnez le fichier de sauvegarde de la même instance que vous souhaitez restaurer.
4. Cliquez sur **Reconditionner la sauvegarde**.

   Lorsque l'appliance SDX est sauvegardée, les fichiers et images XVA sont stockés séparément pour économiser la bande passante réseau et l'espace disque. Par conséquent, vous devez reconditionner le fichier sauvegardé avant de restaurer l'appliance SDX.

   Lorsque vous reconditionnez le fichier de sauvegarde, il inclut tous les fichiers sauvegardés ensemble pour restaurer l'appliance SDX. Le fichier de sauvegarde reconditionné garantit la réussite de la restauration de l'appliance SDX.
5. Sélectionnez le fichier de sauvegarde reconditionné et cliquez sur **Restaurer**.

Forcer un basculement vers l'instance NetScaler secondaire

Vous pourriez vouloir forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau l'instance principale de Citrix NetScaler. Vous pouvez forcer le basculement depuis l'instance principale ou l'instance secondaire. Lorsque vous forcez un basculement sur l'instance principale, la principale devient la secondaire et la secondaire devient la principale. Le basculement forcé n'est possible que lorsque l'instance principale peut déterminer que l'instance secondaire est ACTIVE.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Un basculement forcé n'est ni propagé ni synchronisé. Pour afficher l'état de synchronisation après un basculement forcé, vous pouvez consulter l'état de l'instance.

Un basculement forcé échoue dans l'une des circonstances suivantes :

- Vous forcez un basculement sur un système autonome.
- L'instance secondaire est désactivée ou inactive. Si l'instance secondaire est dans un état inactif, vous devez attendre que son état soit ACTIF pour forcer un basculement.
- L'instance secondaire est configurée pour rester secondaire.

L'instance NetScaler affiche un message d'avertissement si elle détecte un problème potentiel lorsque vous exécutez la commande de basculement forcé. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Vous pouvez forcer un basculement sur une instance principale ou sur une instance secondaire.

Pour forcer un basculement vers l'instance NetScaler secondaire à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à l'onglet **Infrastructure > Instances > NetScaler > VPX**, puis sélectionnez une instance.
2. Sélectionnez les instances dans une configuration HA parmi les instances répertoriées sous le type d'instance sélectionné.
3. Dans le menu **Action**, sélectionnez **Forcer le basculement.**
4. Cliquez sur **Oui** pour confirmer l'action de basculement forcé.



Forcer une instance NetScaler secondaire à rester secondaire

Dans une configuration HA, le nœud secondaire peut être forcé à rester secondaire, quel que soit l'état du nœud principal.

Par exemple, supposons que le nœud principal doive être mis à niveau et que le processus prenne quelques secondes. Pendant la mise à niveau, le nœud principal peut tomber en panne pendant quelques secondes, mais vous ne voulez pas que le nœud secondaire prenne le relais. Vous voulez qu'il reste le nœud secondaire même s'il détecte une défaillance dans le nœud principal.

Lorsque vous forcez le nœud secondaire à rester secondaire, il reste secondaire même si le nœud principal tombe en panne. De plus, lorsque vous forcez le statut d'un nœud dans une paire HA à

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rester secondaire, il ne participe pas aux transitions de la machine d'état HA. Le statut du nœud est affiché comme STAYSECONDARY.

REMARQUE

Lorsque vous forcez un système à rester secondaire, le processus de forçage n'est ni propagé ni synchronisé. Il n'affecte que le nœud sur lequel vous exécutez la commande.

Pour configurer une instance NetScaler secondaire afin qu'elle reste secondaire à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Instances** > onglet **NetScaler** > **VPX**, puis sélectionnez une instance.
2. Sélectionnez les instances dans une configuration HA parmi les instances répertoriées sous le type d'instance sélectionné.
3. Dans le menu **Action**, sélectionnez **Rester secondaire**.
4. Cliquez sur **Oui** pour confirmer l'exécution de l'action « Rester secondaire ».



Créer des groupes d'instances

Pour créer un groupe d'instances, vous devez d'abord ajouter toutes vos instances NetScaler à NetScaler Console. Une fois les instances ajoutées avec succès, créez des groupes d'instances en fonction de leur famille d'instances. La création d'un groupe d'instances vous aide à mettre à niveau, sauvegarder ou restaurer les instances groupées en une seule fois.

La **Vue des instances** vous permet de visualiser toutes les instances gérées ainsi que leurs groupes associés, ce qui facilite l'identification des instances non mappées. Vous pouvez attribuer des instances non mappées à un groupe.

Pour créer un groupe d'instances à l'aide de NetScaler Console

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > Groupes d'instances**, puis cliquez sur **Ajouter**.
2. Spécifiez un nom pour votre groupe d'instances et sélectionnez **NetScaler** dans la liste **Famille d'instances**.
3. Dans **Catégorie**, sélectionnez l'option **Par défaut**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez sur **Sélectionner des instances**. Sur la page **Sélectionner des instances**, sélectionnez les instances que vous souhaitez regrouper et cliquez sur **Sélectionner**.

   Le tableau répertorie les instances sélectionnées et leurs détails. Si vous souhaitez supprimer une instance du groupe, sélectionnez l'instance dans le tableau et cliquez sur **Supprimer**.
5. Cliquez sur **Créer**.

Créer des groupes d'instances(/en-us/netscaler-application-delivery-management-software/media/024_instancegroups.png)

Pour identifier et ajouter des instances non mappées à un groupe

1. Accédez à **Infrastructure > Instances > Groupes d'instances > Vue des instances**.
2. Sélectionnez une ou plusieurs instances non mappées.
3. Cliquez sur **Ajouter un groupe d'instances**.
4. Sélectionnez le **groupe d'instances** requis dans la liste. L'interface affiche également :
   - Groupes d'instances disponibles.
   - Instances déjà mappées à chaque groupe, ce qui permet d'éviter les affectations en double ou incorrectes.
5. Cliquez sur **Enregistrer**. Les instances sélectionnées sont affectées au groupe choisi.

Provisionner des instances NetScaler VPX sur SDX à l'aide de NetScaler Console

Vous pouvez provisionner une ou plusieurs instances NetScaler VPX sur l'appliance SDX à l'aide de NetScaler Console. Le nombre d'instances que vous pouvez déployer dépend de la licence que vous avez achetée. Si le nombre d'instances ajoutées est égal au nombre spécifié dans la licence, NetScaler Console vous empêche de provisionner davantage d'instances NetScaler.

Avant de commencer, assurez-vous d'ajouter une instance SDX dans NetScaler Console où vous souhaitez provisionner des instances VPX.

Pour provisionner une instance VPX, procédez comme suit :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Dans l'onglet **SDX**, sélectionnez une instance SDX où vous souhaitez provisionner une instance VPX.
3. Dans **Sélectionner une action**, sélectionnez **Provisionner VPX**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 1 - Ajouter une instance VPX

NetScaler Console utilise les informations suivantes pour configurer les instances VPX dans une appliance SDX :

- **Nom** - Spécifiez un nom pour une instance NetScaler.
- Établissez un réseau de communication entre SDX et VPX. Pour ce faire, sélectionnez les options requises dans la liste :
  - **Gérer via le réseau interne** - Cette option établit un réseau interne pour une communication entre NetScaler Console et une instance VPX.
  - **Adresse IP** - Vous pouvez sélectionner une adresse **IPv4** ou **IPv6**, ou les deux, pour gérer l'instance NetScaler VPX. Une instance VPX ne peut avoir qu'une seule adresse IP de gestion (également appelée adresse IP NetScaler). Vous ne pouvez pas supprimer l'adresse IP NetScaler.

    Pour l'option sélectionnée, attribuez un masque de sous-réseau, une passerelle par défaut et un saut suivant au serveur NetScaler Console pour l'adresse IP.
- **Fichier XVA** - Sélectionnez le fichier XVA à partir duquel vous souhaitez provisionner une instance VPX. Utilisez l'une des options suivantes pour sélectionner le fichier XVA.
  - **Local** - Sélectionnez le fichier XVA depuis votre machine locale.
  - **Appliance** - Sélectionnez le fichier XVA depuis l'explorateur de fichiers de la console.
- **Profil d'administrateur** - Ce profil permet d'accéder au provisionnement des instances VPX. Avec ce profil, NetScaler Console récupère les données de configuration d'une instance. Si vous devez ajouter un profil, cliquez sur **Ajouter**.
- **Agent** - Sélectionnez l'agent auquel vous souhaitez associer les instances
- **Site** - Sélectionnez le site où vous souhaitez ajouter l'instance.

Étape 2 - Allouer des licences

Dans la section **Allocation de licences**, spécifiez la licence VPX. Vous pouvez utiliser des licences Standard, Advanced et Premium.

- **Mode d'allocation** - Vous pouvez choisir les modes **Fixe** ou **Évolutif** pour le pool de bande passante.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si vous choisissez le mode **Évolutif**, vous pouvez utiliser une bande passante supplémentaire lorsque la bande passante fixe est atteinte.

- **Débit** - Attribuez le débit total (en Mbps) à une instance.

REMARQUE

Achetez une licence distincte (Pack d'extension SDX 2 instances pour Secure Web Gateway) pour les instances Citrix Secure Web Gateway™ (SWG) sur les appliances SDX. Ce pack d'instances est différent de la licence de plateforme SDX ou du pack d'instances SDX.

À partir de la version SDX 12.0 57.19, l'interface de gestion de la capacité cryptographique a changé.

Étape 3 - Allouer des ressources

Dans la section **Allocation des ressources**, allouez des ressources à une instance VPX pour maintenir le trafic.

- **Mémoire totale (Mo)** - Allouez la mémoire totale à une instance. La valeur minimale est de `2048` Mo.
- **Paquets par seconde** - Spécifiez le nombre de paquets à transmettre par seconde.
- **CPU** - Spécifiez le nombre de cœurs de CPU pour une instance. Vous pouvez utiliser des cœurs de CPU partagés ou dédiés.

  Lorsque vous sélectionnez un cœur partagé pour une instance, les autres instances peuvent utiliser le cœur partagé en cas de pénurie de ressources.

  Redémarrez les instances sur lesquelles les cœurs de CPU sont réaffectés pour éviter toute dégradation des performances.

  Si vous utilisez la plateforme SDX 25000xx, vous pouvez attribuer un maximum de 16 cœurs à une instance. De même, si vous utilisez la plateforme SDX 2500xxx, vous pouvez attribuer un maximum de 11 cœurs à une instance.

  REMARQUE

  Pour une instance, le débit maximal que vous configurez est de 180 Gbit/s.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le tableau suivant répertorie les versions d'image VPX, Single Bundle prises en charge et le nombre de cœurs que vous pouvez attribuer à une instance :

NOM DE LA PLATEFORME	NOMBRE TOTAL DE CŒURS	NOMBRE TOTAL DE CŒURS DISPONIBLES POUR LE PROVISIONNEMENT VPX	NOMBRE MAXIMAL DE CŒURS POUVANT ÊTRE ATTRIBUÉS À UNE SEULE INSTANCE
SDX 8015, SDX 8400 et SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 et SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540 et SDX 11542	12	10	5
SDX 17500, SDX 19500, et SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550, et SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 et SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100, et SDX 22120	16	14	7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA PLATEFORME	NOMBRE TOTAL DE CŒURS	NOMBRE TOTAL DE CŒURS DISPONIBLES POUR LE PROVISIONNEMENT VPX	NOMBRE MAXIMAL DE CŒURS POUVANT ÊTRE ATTRIBUÉS À UNE SEULE INSTANCE
SDX 24100 et SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G et SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS et SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S et SDX 14100 40S	12	10	5
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (si la version est 11.1-51.x ou supérieure) ; 9 (si la version est 11.1-50.x ou inférieure ; toutes les versions de 11.0 et 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA PLATEFORME	NOMBRE TOTAL DE CŒURS	NOMBRE TOTAL DE CŒURS DISPONIBLES POUR LE PROVISIONNEMENT VPX	NOMBRE MAXIMAL DE CŒURS POUVANT ÊTRE ATTRIBUÉS À UNE SEULE INSTANCE
15000-50G	16	14	7
SDX 16000	32	30	16
SDX 9100	10	9	9

REMARQUE

Sur la plateforme SDX 26xxx, un maximum de 26 cœurs de CPU peut être attribué à une instance VPX. Si des unités de chiffrement sont attribuées à l'instance, le nombre maximal de cœurs dépend du nombre d'unités de chiffrement et d'interfaces de données.

Par exemple, si vous attribuez 24000 unités de chiffrement à une instance, vous pouvez attribuer 24 cœurs de CPU et un maximum de deux interfaces de données à l'instance. L'appliance SDX considère les interfaces de données et les unités de chiffrement comme des périphériques PCI. Pour 26000 unités de chiffrement, le provisionnement de l'instance VPX échoue en raison du manque d'espace pour ajouter des interfaces de données.

Étape 4 - Ajouter l'administration de l'instance

Vous pouvez créer un utilisateur administrateur pour l'instance VPX. Pour ce faire, sélectionnez **Ajouter l'administration de l'instance** dans la section **Administration de l'instance**.

Spécifiez les détails suivants :

- **Nom d'utilisateur** : Le nom d'utilisateur de l'administrateur de l'instance NetScaler. Cet utilisateur dispose d'un accès superutilisateur mais n'a pas accès aux commandes réseau pour configurer les VLAN et les interfaces.
- **Mot de passe** : Spécifiez le mot de passe pour le nom d'utilisateur.
- **Accès Shell/Sftp/Scp** : L'accès autorisé à l'administrateur de l'instance NetScaler. Cette option est sélectionnée par défaut.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 5 - Spécifier les paramètres réseau

Sélectionnez les paramètres réseau requis pour une instance :

- **Autoriser le mode L2 sous les paramètres réseau** - Vous pouvez autoriser le mode L2 sur l'instance NetScaler. Sélectionnez Autoriser le mode L2 sous Paramètres réseau. Avant de vous connecter à l'instance et d'activer le mode L2.

  REMARQUE

  Si vous désactivez le mode L2 pour une instance, vous devez vous connecter à l'instance et désactiver le mode L2 à partir de cette instance. Dans le cas contraire, cela pourrait entraîner la désactivation de tous les autres modes NetScaler après le redémarrage de l'instance.

- **0/1** - Dans **Balise VLAN**, spécifiez un ID VLAN pour l'interface de gestion.
- **0/2** - Dans **Balise VLAN**, spécifiez un ID VLAN pour l'interface de gestion.

Par défaut, les interfaces **0/1** et **0/2** sont sélectionnées.

Paramètres réseau(/en-us/netscaler-application-delivery-management-software/media/network-settings.png)

Dans **Interfaces de données**, cliquez sur **Ajouter** pour ajouter des interfaces de données et spécifiez les éléments suivants :

- **Interfaces** - Sélectionnez l'interface dans la liste.

  REMARQUE

  Les ID d'interface des interfaces que vous ajoutez à une instance ne correspondent pas nécessairement à la numérotation des interfaces physiques sur l'appliance SDX.

  Par exemple, la première interface que vous associez à l'instance-1 est l'interface SDX 1/4 ; elle apparaît comme interface 1/1 lorsque vous affichez les paramètres d'interface dans cette instance. Cette interface indique qu'il s'agit de la première interface que vous avez associée à l'instance-1.

- **VLAN autorisés** - Spécifiez une liste d'ID de VLAN pouvant être associés à une instance NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Mode d'adresse MAC** - Attribuez une adresse MAC à une instance. Sélectionnez l'une des options suivantes :
  - **Par défaut** - Citrix Workspace attribue une adresse MAC.
  - **Personnalisé** - Choisissez ce mode pour spécifier une adresse MAC qui remplace l'adresse MAC générée.
  - **Généré** - Générez une adresse MAC en utilisant l'adresse MAC de base définie précédemment.
- **Paramètres VMAC (VRID IPv4 et IPv6 pour configurer le MAC virtuel)**
  - **VRID IPV4** - Le VRID IPv4 qui identifie le VMAC. Valeurs possibles : 1 à 255. Pour plus d'informations, consultez Configuration des VMAC sur une interface.
  - VRID IPV6 - Le VRID IPv6 qui identifie le VMAC. Valeurs possibles : 1 à 255. Pour plus d'informations, consultez Configuration des VMAC sur une interface.

Cliquez sur **Ajouter**.

Étape 6 - Spécifier les paramètres VLAN de gestion

Le service de gestion et l'adresse de gestion (NSIP) de l'instance VPX se trouvent dans le même sous-réseau, et la communication s'effectue via une interface de gestion.

Si le service de gestion et l'instance se trouvent dans des sous-réseaux différents, spécifiez un ID de VLAN lorsque vous provisionnez une instance VPX. Ainsi, l'instance est accessible sur le réseau lorsqu'elle est active.

Si votre déploiement exige que le NSIP soit accessible uniquement via l'interface sélectionnée lors du provisionnement de l'instance VPX, sélectionnez **NSVLAN**. De plus, le NSIP devient inaccessible via d'autres interfaces.

- Les pulsations HA sont envoyées uniquement sur les interfaces qui font partie du NSVLAN.
- Vous pouvez configurer un NSVLAN uniquement à partir de la version VPX XVA `9.3-53.4` et ultérieure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

- Vous ne pouvez pas modifier ce paramètre après avoir provisionné l'instance VPX.
- La commande `clear config full` sur l'instance VPX supprime la configuration VLAN si **NSVLAN** n'est pas sélectionné.

Cliquez sur **Terminé** pour provisionner une instance VPX.

Afficher l'instance VPX provisionnée

Pour afficher l'instance nouvellement provisionnée, procédez comme suit :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Dans l'onglet **VPX**, recherchez une instance par la propriété **Adresse IP de l'hôte** et spécifiez-lui l'adresse IP de l'instance SDX.

Afficher l'instance VPX provisionnée(/en-us/netscaler-application-delivery-management-software/media/provisioned-vpx-on-sdx.png)

Provisionner des instances NetScaler VPX sur VMware ESX

Vous pouvez utiliser NetScaler Console pour automatiser le déploiement et la gestion d'une instance NetScaler VPX dans VMware ESX. Lorsque vous utilisez NetScaler Console pour provisionner une instance NetScaler VPX sur VMware ESX, l'instance est immédiatement disponible pour être gérée dans l'interface graphique de NetScaler Console.

NetScaler Console utilise les modèles NetScaler des instances déjà déployées pour provisionner une nouvelle instance dans VMware ESX. Il stocke le centre de données du VMware vCenter où les détails requis du serveur VMware ESX sont présents sur un site. De plus, il utilise un profil d'accès au cloud pour accéder au VMware vCenter et déployer le VPX sur le VMware ESX.

Prérequis

Avant de provisionner une instance NetScaler VPX dans VMware ESX, assurez-vous d'effectuer les opérations suivantes :

1. Installez une version prise en charge de VMware ESXi (6.0, 6.5 et 6.7).
2. Installez VMware Client sur un poste de travail de gestion qui répond aux exigences minimales du système.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Téléchargement des fichiers d'installation de NetScaler VPX.
4. Convertir les fichiers NetScaler VPX en modèles dans ESX.
5. Créer des autorisations pour que NetScaler Console accède à VMware vCenter.
6. Créer un site dans NetScaler Console.

Convertir les fichiers NetScaler VPX en modèles

NetScaler Console utilise le modèle NetScaler dans ESX converti par un fichier NetScaler VPX. Effectuez les étapes suivantes pour convertir les fichiers VPX en modèles.

1. Déployez une instance NetScaler VPX sur VMware à l'aide des fichiers d'installation de NetScaler.

   Pour la première fois, utilisez les fichiers d'installation de NetScaler pour déployer l'instance VPX. Pour plus d'informations, consultez Installer une instance NetScaler VPX sur VMware.
2. Cliquez avec le bouton droit sur la VM déployée et sélectionnez **Modèle**.
3. Cliquez sur **Convertir en modèle**.



Créer des autorisations pour que NetScaler Console accède à VMware vCenter

Pour activer NetScaler Console pour le provisionnement et la gestion dans VMware vCenter, suivez ces étapes :

1. Créer un rôle personnalisé avec des privilèges
   a. Connectez-vous à VMware vCenter et accédez à la section **Rôles**.
   b. Créez un rôle personnalisé adapté à NetScaler Console.
   c. Attribuez les privilèges suivants :

```
Datastore.AllocateSpace

Resource.AssignVMToPool

VirtualMachine.Config.AdvancedConfig

VirtualMachine.Inventory.CreateFromExisting

VirtualMachine.Inventory.Delete
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
VirtualMachine.Interact.PowerOff

VirtualMachine.Interact.PowerOn

VirtualMachine.Provisioning.DeployTemplate
```

2. Créer un utilisateur
    a. Une fois le rôle défini, accédez à la section **Utilisateurs et groupes**.
    b. Créez un utilisateur pour que NetScaler Console accède à VMware vCenter.
    c. Fournissez un mot de passe pour l'utilisateur nouvellement créé.
3. Associer le rôle à l'utilisateur
    a. Accédez à la section **Autorisations globales** et associez le rôle personnalisé à l'utilisateur.
    b. Cette association fournit des privilèges à NetScaler Console pour effectuer les actions nécessaires sur VMware vCenter.

REMARQUE :

Les privilèges listés sont les exigences minimales pour que NetScaler Console puisse accéder à VMware vCenter. La création d'un utilisateur avec des privilèges limités est facultative. Si un utilisateur dispose de privilèges qui incluent un sur-ensemble des privilèges spécifiés, il peut fournir ces informations d'identification à la place.

Pour plus d'informations sur la configuration des rôles d'utilisateur avec des privilèges dans VMware vCenter, consultez Configurer l'accès utilisateur.

Créer un site dans NetScaler Console

Créez un site dans NetScaler Console et ajoutez les détails de VMware ESX.

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > Sites**.
2. Cliquez sur **Ajouter**.
3. Dans le volet **Sélectionner un cloud**,
    a. Sélectionnez **Centre de données** comme type de **Site**.
    b. Choisissez **VMware vCenter** dans la liste **Type**.
    c. Cliquez sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Dans le volet **Choisir une région**,

   a. Dans le volet **Profil d'accès au cloud**, sélectionnez le profil créé pour votre VMware ESX. S'il n'y a pas de profils, créez-en un.

   b. Pour créer un profil d'accès au cloud, cliquez sur **Ajouter** et spécifiez les éléments suivants :

      - **Nom** – Spécifiez un nom pour identifier votre profil d'accès au cloud dans NetScaler Console.
      - **Adresse IP** – Spécifiez l'adresse IP du serveur VMware vCenter où vous souhaitez provisionner des instances VPX.
      - **Nom d'utilisateur** – Spécifiez le nom d'utilisateur pour accéder au serveur VMware vCenter.
      - **Mot de passe** – Spécifiez le mot de passe pour accéder au serveur VMware vCenter et confirmez le mot de passe.

   c. Dans **Réseau (Centre de données)**, sélectionnez le centre de données où se trouvent vos modèles NetScaler.

   d. Spécifiez le **Nom du site**.

   e. Spécifiez la **Région**, la **Latitude** et la **Longitude** pour identifier la géolocalisation de votre centre de données.

   f. Cliquez sur **Terminer**.

Provisionner une instance sur VMware ESX

Utilisez le site que vous avez associé à votre VMware ESX pour provisionner les instances NetScaler VPX.

REMARQUE :

Actuellement, NetScaler Console ne prend en charge que le provisionnement d'instances NetScaler autonomes.

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > NetScaler**.
2. Dans l'onglet **VPX**, cliquez sur **Provisionner**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cette option affiche la page **Provisionner NetScaler VPX sur le cloud**.

3. Sélectionnez **VMware vCenter** et cliquez sur **Suivant**.



4. Dans **Paramètres de base**, spécifiez les éléments suivants :

   - **Nom** – Spécifiez le nom d'une instance.
   - **Site** – Sélectionnez le site que vous avez créé précédemment.
   - **Profil d'accès au cloud** – Sélectionnez le profil d'accès au cloud créé lors de la création du site.
   - **Profil NetScaler** – Sélectionnez le profil NetScaler pour fournir l'authentification.
   - **Licence** – Utilisez la licence de capacité groupée pour appliquer des licences à une instance.



5. Cliquez sur **Suivant**.
6. Dans **Paramètres de provisionnement**, spécifiez les détails suivants :

   - **Clusters** – Sélectionnez le cluster où vous souhaitez provisionner une instance.
   - **Hôtes** – Sélectionnez l'hôte requis dans la liste.
   - **Modèles** – Sélectionnez le modèle dans la liste que vous souhaitez appliquer à une instance.
   - **Banque de données** – Sélectionnez la banque de données dans la liste.
   - **Adresse IP** – Spécifiez une adresse IP pour une instance.
   - **Masque de sous-réseau** – Spécifiez un masque de sous-réseau pour une instance.
   - **Passerelle** – Spécifiez une passerelle pour une instance.



7. Cliquez sur **Terminer** pour provisionner une instance VPX.

Redécouvrir plusieurs instances NetScaler VPX

Vous pouvez redécouvrir plusieurs instances NetScaler VPX dans votre configuration NetScaler Console. De plus, vous pouvez redécouvrir plusieurs instances NetScaler VPX lorsque vous souhaitez afficher les derniers états et configurations de ces instances. Le serveur NetScaler Console redécouvre toutes les instances NetScaler VPX et vérifie si les instances Citrix NetScaler sont accessibles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour redécouvrir plusieurs instances NetScaler VPX :

1. Dans un navigateur web, saisissez l'adresse IP du serveur NetScaler Console (par exemple, `<http://192.168.100.1>`).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur. Les informations d'identification de l'administrateur par défaut sont `nsroot` et `nsroot`.
3. Accédez à l'onglet **Infrastructure > Instances > NetScaler** > **VPX** et sélectionnez les instances que vous souhaitez redécouvrir.
4. Dans le menu **Sélectionner une action**, cliquez sur **Redécouvrir**.
5. Lorsque le message de confirmation pour l'exécution de l'utilitaire de redécouverte apparaît, cliquez sur **Oui**.

   L'écran affiche la progression de la redécouverte de chacune des instances NetScaler VPX.

Dégérer une instance

Si vous souhaitez arrêter l'échange d'informations entre NetScaler Console et les instances de votre réseau, vous pouvez dégérer les instances.

Dégérer une instance NetScaler la rend non gérée ou désenregistrée de NetScaler Console. NetScaler Console ne peut plus contacter ou communiquer avec l'instance NetScaler pour exécuter des fonctionnalités basées sur NetScaler Console.

En ce qui concerne la licence basée sur LAS, dégérer une instance NetScaler fait perdre à l'instance NetScaler sa licence basée sur LAS.

Pour dégérer une instance :

Accédez à l'onglet **Infrastructure > Instances > NetScaler** \> **VPX**. Dans la liste des instances, faites un clic droit sur une instance et sélectionnez **Dégérer**, ou sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Dégérer**.

Le statut de l'instance sélectionnée passe à **Hors service**, comme illustré dans la figure suivante.



Tracer l'itinéraire vers une instance

En traçant l'itinéraire d'un paquet de la NetScaler Console vers une instance, vous pouvez trouver des informations telles que le nombre de sauts nécessaires pour atteindre l'instance. Traceroute

© 1997–2026 Citrix Systems, Inc. All rights reserved.

trace le chemin du paquet de la source à la destination. Il affiche la liste des sauts réseau ainsi que le nom d'hôte et l'adresse IP de chaque entité sur l'itinéraire.

Traceroute enregistre également le temps mis par un paquet pour voyager d'un saut à l'autre. S'il y a une interruption dans le transfert des paquets, traceroute indique où se situe le problème.

Pour tracer l'itinéraire d'une instance :

1. Dans NetScaler Console, accédez à **Infrastructure > Instances > NetScaler** > onglet **VPX**.
2. Dans la liste des instances, faites un clic droit sur une instance, puis sélectionnez **TraceRoute** ou sélectionnez l'instance et, dans le menu **Sélectionner une action**, cliquez sur **TraceRoute**.

La boîte de message **TraceRoute** affiche l'itinéraire vers l'instance et le temps, en millisecondes, consommé par chaque saut.



Afficher les adresses IP appartenant à NetScaler

Vous pouvez afficher les adresses IP configurées sur les instances NetScaler directement depuis l'interface graphique de NetScaler Console. Vous ne pouvez effectuer les modifications de configuration et d'autres opérations que sur les instances NetScaler.

Pour afficher les adresses IP appartenant à NetScaler, accédez à **Infrastructure > Instances > NetScaler Owned IPs**.

Cette fonctionnalité affiche les adresses IPv4 et IPv6 configurées sur les instances NetScaler. Les types d'adresses IP incluent :

- Adresse IP NetScaler
- Adresse IP de sous-réseau
- Adresse IP virtuelle
- Adresse IP de service ADNS
- Adresse IP GSLB
- Adresse IP de cluster
- Adresse IP mappée



Exporter les adresses IP appartenant à NetScaler

Pour exporter les adresses IP appartenant à NetScaler :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Infrastructure > Instances > NetScaler Owned IPs**.
2. Sur la page **Adresses IP détenues par NetScaler**, cliquez sur l'icône d'exportation dans le coin supérieur droit.
3. Sur la page **Exporter les rapports**, cliquez sur **Exporter maintenant**.
4. Sur la page **Exporter maintenant**, sélectionnez l'option d'exportation :

   Pour l'exportation **Instantané** :

   a. Sélectionnez le format de fichier d'exportation : PDF, JPG ou PNG.

   

   Pour l'exportation **Tabulaire** :

   a. Sélectionnez le format de fichier d'exportation : PDF ou CSV.
   b. Sélectionnez le nombre d'enregistrements de données à exporter à partir de la liste.

   

5. Cliquez sur **Exporter**.

Planifier l'exportation des adresses IP détenues par NetScaler

Pour planifier l'exportation des adresses IP détenues par NetScaler :

1. Accédez à **Infrastructure > Instances > Adresses IP détenues par NetScaler**.
2. Sur la page **Adresses IP détenues par NetScaler**, cliquez sur l'icône d'exportation dans le coin supérieur droit.
3. Sur la page **Rapports d'exportation**, cliquez sur **Planifier l'exportation**.
4. Sur la page **Planifier l'exportation**, saisissez les détails suivants :

   a. Saisissez l'objet et la description.
   b. Sélectionnez le type d'exportation.

      Pour le type d'exportation **Instantané** :

      - Sélectionnez le format de fichier d'exportation : PDF, JPG ou PNG.

      Pour le type d'exportation **Tabulaire** :

      - Sélectionnez le format de fichier d'exportation : PDF ou CSV.
      - Sélectionnez le nombre d'enregistrements de données à exporter de la liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Sélectionnez la récurrence : Quotidienne, Hebdomadaire ou Mensuelle.

d. Sélectionnez l'heure d'exportation.

e. Sélectionnez comment envoyer les adresses IP exportées : E-mail, Slack ou les deux.

Pour l'e-mail :

- Sélectionnez **E-mail** et choisissez la liste de distribution d'e-mails pour envoyer la liste des adresses IP appartenant à NetScaler.
  - Pour ajouter une liste de distribution d'e-mails, cliquez sur **Ajouter** et spécifiez les détails du serveur de messagerie.
  - Pour modifier une liste de distribution d'e-mails, cliquez sur **Modifier**.
  - Pour vérifier que la liste de distribution d'e-mails fonctionne, cliquez sur **Tester**. Cela enverra un e-mail de test à la liste de distribution d'e-mails sélectionnée.

Pour Slack :

- Sélectionnez **Slack** et choisissez la liste de profils Slack pour envoyer la liste des adresses IP appartenant à NetScaler.
  - Pour ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **Nom du profil**, le **Nom du canal** et le **Jeton** du canal Slack.
  - Pour modifier un canal Slack existant, cliquez sur **Modifier**.

5. Cliquez sur **Planifier** pour planifier l'exportation.

Une fois planifiée, votre planification d'exportation apparaît sur la page **Rapports d'exportation**, et vous pouvez sélectionner la planification pour effectuer l'opération de modification ou de suppression. Après avoir modifié la planification sélectionnée, cliquez sur **Enregistrer** pour enregistrer les modifications. **Supprimer** supprime la planification.

Répliquer les configurations d'une instance NetScaler à une autre

Vous pouvez utiliser la fonctionnalité de réplication de configuration de NetScaler Console pour copier les configurations d'une instance NetScaler et les répliquer sur une seule instance ou sur plusieurs instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour répliquer les configurations d'une instance vers d'autres instances NetScaler

1. Accédez à **Infrastructure > Instances > NetScaler**. Sélectionnez l'instance source dont vous souhaitez répliquer les configurations sur d'autres instances et, dans la liste **Sélectionner une action**, cliquez sur **Répliquer la configuration**.
2. Dans **Répliquer la configuration**, sélectionnez l'instance cible sur laquelle vous souhaitez appliquer les configurations de l'instance source. Vous pouvez répliquer les configurations d'une seule instance source vers une seule instance ou plusieurs instances cibles.

   
3. Cliquez sur **Créer**.

Les configurations répliquées sont ajoutées à la liste des instances NetScaler®. Pour afficher l'état des instances répliquées, cliquez sur l'icône d'actualisation.

REMARQUE :

Pendant la réplication, toutes les adresses IP réseau de l'instance source sont répliquées vers l'instance cible. Si l'instance cible se trouve dans un réseau différent de celui de l'instance source, les adresses IP de l'instance cible peuvent ne pas être accessibles. Lorsque les adresses IP ne sont pas accessibles, l'état des entités de l'instance cible est affiché comme Hors service (Down).

Pour afficher l'état des entités configurées sur votre instance NetScaler gérée, accédez à **Infrastructure > Fonctions réseau**.

Gestion des certificats SSL

Toute organisation ou site web individuel qui doit traiter des informations confidentielles ou sensibles doit disposer d'un certificat SSL. Le certificat SSL sur un serveur web contribue à garantir l'authenticité du serveur web au client qui se connecte. Il n'authentifie pas seulement l'identité d'un site web, mais aide également à générer la clé de session, qui est ensuite utilisée pour le chiffrement de l'ensemble de la session.

Un certificat SSL (Secure Socket Layer), qui fait partie de toute transaction SSL, est une forme de données numériques (X509) qui identifie une entreprise (domaine) ou un individu. Le certificat possède un composant de clé publique qui est visible par tout client souhaitant initier une transaction sécurisée avec le serveur. La clé privée correspondante, qui réside en toute sécurité

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sur l'appliance Citrix NetScaler, est utilisée pour effectuer le chiffrement et le déchiffrement à clé asymétrique (ou clé publique).

NetScaler Console vous offre une console unifiée pour automatiser l'installation, la mise à jour, la suppression, la liaison et le téléchargement des certificats SSL. Cela contribue à préserver la réputation du site web et la confiance des clients. NetScaler Console simplifie désormais tous les aspects de la gestion des certificats pour vous. Grâce à une console unifiée, vous pouvez configurer des politiques automatisées pour garantir l'émetteur, la force de clé, le protocole et les algorithmes recommandés conformément aux politiques informatiques de l'organisation. Ce faisant, vous pouvez surveiller de près les certificats inutilisés ou sur le point d'expirer.

Vous pouvez obtenir un certificat et une clé SSL de l'une des manières suivantes :

- Auprès d'une autorité de certification (CA) autorisée, telle que Verisign
- En générant un nouveau certificat et une clé SSL sur l'appliance NetScaler

Paramètres de la politique SSL d'entreprise

Chaque entreprise a sa propre politique SSL et définit les exigences auxquelles tous les certificats SSL doivent adhérer. La sécurité a toujours été l'une des principales priorités pour tous les utilisateurs d'entreprise, et les paramètres SSL jouent donc un rôle important.

Par exemple, une société ABC exige que tous les certificats aient une force de clé minimale de 2 048 bits et plus. Les certificats doivent être autorisés par une autorité de certification (CA) ou des émetteurs de confiance. Les administrateurs doivent vérifier tous ces paramètres SSL pour s'assurer que les certificats respectent la politique de l'entreprise. Il est fastidieux de vérifier chaque certificat manuellement. Pour pallier ce problème, NetScaler Console vous aide à configurer les paramètres de la politique SSL d'entreprise et affiche tout certificat non conforme avec l'étiquette « Non recommandé ».

Vous pouvez afficher le résumé des certificats non conformes (non recommandés) sur le tableau de bord SSL.



REMARQUE

Les certificats « Non recommandé » sont classés en fonction de différents paramètres, et vous pouvez les afficher dans les composants pertinents.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fonctionnement du certificat NetScaler Console

Le tableau de bord SSL vous offre une présentation visuelle de tous les certificats SSL installés sur différentes instances NetScaler. Le tableau de bord SSL inclut les informations suivantes pour chaque certificat installé sur les instances NetScaler. Il est classé en fonction des éléments suivants :

- **Auto-signés ou signés par une CA.** La section auto-signés ou signés par une CA vous aide à séparer les certificats en certificats auto-signés et certificats signés par une CA.
- **Algorithmes de signature.** Cette section classe les certificats SSL en fonction des algorithmes de signature utilisés pour le chiffrement.
- **Utilisation.** Cette section classe vos certificats SSL en fonction des certificats utilisés et non utilisés. Les certificats non utilisés nécessitent une attention particulière car ils pourraient avoir été oubliés d'être liés aux serveurs virtuels.
- **Émetteurs.** Cette section classe les certificats SSL en fonction de l'émetteur des certificats.
- **Force de la clé.** Cette section classe les certificats SSL en fonction de la force de la clé privée.
- **Top 10 des instances.** Cette section fournit les détails des 10 principales instances NetScaler en fonction du nombre de certificats SSL installés.



Cas d'utilisation de la gestion des certificats SSL

Les cas d'utilisation suivants décrivent comment vous pouvez utiliser le certificat SSL pour gérer et surveiller les certificats sur plusieurs instances NetScaler.

Installer des certificats SSL

Imaginez que vous disposez d'un parc d'instances NetScaler sur lesquelles vous devez déployer les certificats SSL requis. NetScaler Console vous offre une console unifiée pour déployer les certificats SSL sur plusieurs instances NetScaler en une seule tentative.

Par exemple, vous pourriez vouloir installer des certificats SSL sur une ou plusieurs instances NetScaler. Avec cette approche, vous pouvez minimiser l'intervention manuelle d'installation du certificat SSL sur chaque instance NetScaler. Vous pouvez effectuer une installation en masse de certificats SSL sur une ou plusieurs instances NetScaler.

Pour obtenir un résumé des certificats SSL, connectez-vous à **NetScaler Console**, puis accédez à **Infrastructure > Tableau de bord SSL**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Paramètres de notification pour l'expiration des certificats

Dans ce cas d'utilisation, vous pourriez avoir de nombreux certificats sur plusieurs instances NetScaler, et le suivi de l'expiration de chaque certificat devient une surcharge. Il est fastidieux de suivre chaque certificat manuellement et de le mettre à jour avant son expiration. Pour éviter de tels scénarios, vous pouvez configurer NetScaler Console pour envoyer des notifications ou des alertes aux profils de messagerie, de téléavertisseur, de Slack ou de ServiceNow configurés. De cette façon, vous pouvez rester informé des dates d'expiration des certificats et les renouveler bien avant leur échéance.

Par exemple, vous pourriez oublier de suivre le certificat qui approche de son expiration. Et le certificat expire, provoquant une interruption de service, ce qui pourrait affecter de nombreuses applications pour les utilisateurs. Grâce aux paramètres de notification d'expiration de certificat de NetScaler Console, vous pouvez éviter de tels scénarios imprévus.

Vous pouvez consulter le résumé et suivre les certificats qui approchent de leur expiration sur le **tableau de bord SSL**.

Pour afficher le rapport des certificats expirant dans une durée donnée, vous pouvez cliquer sur la vignette pour obtenir les détails de tous les certificats expirant dans cette fenêtre.



Renouvellement des certificats

Vous pouvez désormais renouveler les certificats depuis NetScaler Console. Vous pouvez soit renouveler les certificats existants, soit créer des certificats basés sur les éléments suivants :

Mettre à jour le certificat existant

Dans ce cas d'utilisation, vous devez mettre à jour un certificat existant une fois que vous avez reçu un certificat renouvelé de l'autorité de certification (CA). Vous pouvez désormais mettre à jour les certificats existants depuis NetScaler Console sans vous connecter aux instances NetScaler.

Par exemple, il peut y avoir des changements ou des modifications aux certificats existants. L'autorité de certification émet des certificats renouvelés. Au lieu d'aller sur l'appliance NetScaler, vous pouvez maintenant mettre à jour le certificat SSL depuis NetScaler Console.

Pour mettre à jour un certificat, connectez-vous à NetScaler Console, puis accédez à **Infrastructure > Tableau de bord SSL**.

Sélectionnez le certificat que vous souhaitez mettre à jour, puis cliquez sur **Mettre à jour**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous avez la possibilité de mettre à jour les champs pertinents du certificat sélectionné depuis NetScaler Console.



Créer une demande de signature de certificat

Imaginez un cas d'utilisation où l'un des certificats SSL n'est pas conforme aux politiques de l'organisation. Vous souhaitez obtenir un nouveau certificat auprès de l'autorité de certification. Vous pouvez désormais générer une demande de signature de certificat (CSR) depuis NetScaler Console. Une CSR et une clé publique peuvent être envoyées à une CA pour obtenir le certificat SSL.

Pour déterminer et créer une CSR, sélectionnez le certificat souhaité et cliquez sur **Créer une CSR**.

Vous devez disposer d'une paire de valeurs de clé publique ou privée. Pour télécharger une clé, cliquez sur **Choisir un fichier** et sélectionnez dans la liste. Pour créer une clé, sélectionnez **Je n'ai pas d'option de clé** et spécifiez les paramètres pertinents.



Pour fournir plus de détails sur la clé sélectionnée, tels que le Nom commun, le Nom de l'organisation, la Ville, le Pays, l'État, l'Unité organisationnelle et l'ID de messagerie, afin de créer la CSR.



Lier et dissocier les certificats SSL

Vous pouvez lier plusieurs certificats SSL entre eux pour créer un bundle de certificats. Pour lier un certificat à un autre certificat, l'émetteur du premier certificat doit correspondre au domaine du second certificat.



Journaux d'audit

Les journaux d'audit sont une collection de fichiers journaux texte générés par la NetScaler Console. Ils affichent un historique des certificats SSL qui sont ajoutés, modifiés et changés à l'aide de NetScaler Console vers l'appliance NetScaler spécifique. Les journaux d'audit affichent également l'adresse IP de l'appliance NetScaler, le statut, l'heure de début et l'heure de fin de l'opération particulière.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, vous pourriez vouloir vérifier la modification qui a eu lieu sur une période donnée pour le certificat particulier. Et vous avez la possibilité de consulter l'historique des modifications apportées au certificat via le Device Log et le Command Log.

Pour déterminer les informations des certificats SSL, sur le **Tableau de bord SSL**, cliquez sur **Journal d'audit**. Le résumé de l'application inclut le statut des certificats SSL avec l'heure de début et l'heure de fin.

Pour déterminer les informations de l'appliance NetScaler d'un certificat SSL particulier, cochez la case du certificat pertinent de votre choix. Cliquez sur **Device Log**.

Pour afficher les informations sur le type de commande et le message, cliquez sur **Journal des commandes**.

Renouvellement automatique des certificats à l'aide du protocole ACME

NetScaler Console prend en charge l'environnement de gestion automatisée des certificats (ACME), un protocole ouvert conçu pour automatiser le renouvellement des certificats SSL/TLS.

Auparavant, les administrateurs réseau devaient suivre un processus manuel long et en plusieurs étapes pour renouveler les certificats. Le support ACME atténue ces difficultés en fournissant un cadre robuste pour le renouvellement automatisé des certificats afin d'effectuer les actions suivantes :

- Demander de nouveaux certificats auprès d'autorités de certification (CA) fiables.
- Valider la propriété du domaine à l'aide de méthodes automatisées (par exemple, défi DNS-01).
- Renouveler automatiquement les certificats avant leur expiration.

Prise en charge d'ACME dans NetScaler® Console

NetScaler Console utilise le client `acme.sh` et prend en charge les autorités de certification suivantes :

- Let's Encrypt
- DigiCert Inc
- Sectigo Limited

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Entrust, Inc
- GlobalSign
- GoDaddy.com, Inc
- ZeroSSL
- Google Trust Services
- Google Public CA
- BuyPass Go SSL
- Actalis
- SSL.com
- HashiCorp Vault
- Smallstep
- Pebble
- HARICA
- EJBCA

Les étapes suivantes expliquent comment le renouvellement automatique des certificats se déroule dans NetScaler Console :

1. Lorsque NetScaler Console initie une demande de certificat pour un domaine à l'aide du client `acme.sh`, le client se connecte à l'autorité de certification choisie (par exemple, Let's Encrypt ou DigiCert).
2. L'autorité de certification émet un défi pour prouver la propriété du domaine, qui dans ce cas est un défi DNS-01.
3. NetScaler Console, à l'aide d'informations d'identification préconfigurées, met automatiquement à jour l'enregistrement DNS TXT du domaine avec la valeur fournie par l'autorité de certification.
4. L'autorité de certification valide l'enregistrement TXT, confirmant la propriété du domaine.
5. Après une validation réussie, l'AC émet le certificat SSL/TLS à NetScaler Console.
6. NetScaler Console stocke le certificat dans le magasin respectif (magasin de certificats/ magasin Zero-touch).
7. En fonction de la fenêtre de renouvellement que vous avez fournie, NetScaler Console répète automatiquement ce processus de renouvellement avant la date d'expiration du certificat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Avec la prise en charge d'ACME dans NetScaler Console, vous pouvez effectuer les actions suivantes :

- Renouveler automatiquement les certificats avant leur expiration
- Passer d'une AC à une autre lors du renouvellement
- Générer ou télécharger un CSR et demander un nouveau certificat

Voici les principaux avantages :

- Cycle de vie entièrement automatisé sans intervention manuelle pour l'émission ou le renouvellement de certificats.
- Calendrier de renouvellement personnalisable qui répond aux besoins de l'organisation (par exemple, défini pour renouveler 7 jours avant l'expiration).
- Élimine les temps d'arrêt dus aux certificats expirés.
- Réduction des frais généraux d'exploitation grâce à l'automatisation du suivi des expirations et des renouvellements.
- Amélioration de la posture de sécurité grâce à des certificats toujours valides et conformes aux meilleures pratiques de l'AC.

Étapes de configuration pour l'intégration d'ACME

L'intégration d'ACME est un processus unique et comprend les étapes suivantes :

- Étape 1 : Configurer l'autorité de certification (CA).
- Étape 2 : Sélectionner les certificats à renouveler.
- Étape 3 : Ajouter un fournisseur DNS et mapper les domaines respectifs.

Prérequis

- Assurez-vous de disposer d'un compte valide pour votre autorité de certification (CA) et d'une licence correspondante.
- Assurez-vous de disposer des informations d'identification d'accès au fournisseur DNS.

Étape 1 : Configurer l'autorité de certification (CA)

Effectuez les étapes suivantes pour enregistrer l'autorité de certification (CA) utilisée pour les renouvellements :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Infrastructure > Tableau de bord SSL**. Si vous configurez ACME pour la première fois, vous verrez une bannière avec « Renouvellements automatiques pour les certificats SSL ». Cliquez sur **Démarrer**.

   

   ou

   Accédez à **Infrastructure > Tableau de bord SSL > Intégration tierce > Fournisseurs CA** et cliquez sur **Ajouter**.

2. Saisissez un nom et sélectionnez le fournisseur CA. Actuellement, seuls **Let's Encrypt** et **DigiCert Inc** sont pris en charge.
3. Fournissez les autres détails tels que l'adresse e-mail, l'URL du répertoire ACME.
4. Saisissez le nombre de jours avant lesquels NetScaler Console doit renouveler automatiquement les certificats.
5. Cliquez sur **Enregistrer et continuer**. NetScaler Console tente de se connecter à l'autorité de certification. Si la connectivité échoue, examinez les détails fournis, corrigez les détails de configuration, puis réessayez.

   

Étape 2 : Sélectionner les certificats à renouveler

Une fois les détails de l'autorité de certification ajoutés, NetScaler Console analyse automatiquement tous les certificats (du magasin de certificats et du magasin Zero-touch) et répertorie séparément les certificats émis par l'autorité de certification configurée. Examinez les certificats répertoriés.

1. Sélectionnez les certificats que vous souhaitez renouveler automatiquement. Par exemple, si vous configurez Let’s Encrypt comme autorité de certification et que vous avez 2 certificats de Let’s Encrypt et 2 d'un autre fournisseur, le tableau de bord affiche : `Let’s Encrypt: 2 and Other CA: 2`.

   

2. Vous pouvez cliquer sur **Ajouter** pour ajouter également des certificats émis par une autorité de certification différente ou sur **Supprimer** pour supprimer les certificats que vous ne souhaitez pas renouveler automatiquement. Si vous sélectionnez des certificats d'un fournisseur différent, une invite vous demande de confirmer le changement de fournisseur. Une fois que vous avez confirmé, ces certificats sont renouvelés via l'autorité de certification nouvellement configurée lorsque leur fenêtre de renouvellement est atteinte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Assurez-vous de ne pas avoir de certificats en double dans le magasin de certificats et le magasin de certificats Zero-touch. S'il y a des certificats en double, le processus de renouvellement se produit deux fois pour chaque magasin.

3. Cliquez sur **Enregistrer et continuer**.

REMARQUE :

Les certificats restent dans leurs magasins respectifs après le renouvellement. Par exemple, si un certificat est stocké dans le magasin de certificats, sa version renouvelée est également placée dans le magasin de certificats. Si le certificat est stocké dans le magasin Zero-touch, sa version renouvelée est également placée dans le magasin Zero-touch.

Le comportement de déploiement des certificats dépend du type de magasin.

- Si les certificats sont stockés dans le magasin de certificats, ils doivent être déployés manuellement sur NetScaler.
- Si les certificats sont stockés dans le magasin Zero-touch, les certificats sont automatiquement déployés sur NetScaler sans intervention de l'administrateur. Nous vous recommandons d'utiliser la gestion des certificats Zero-touch pour un déploiement transparent et entièrement automatisé des certificats renouvelés. Pour plus d'informations, consultez Gestion des certificats Zero-touch.

Étape 3 : Ajouter un fournisseur DNS et mapper les domaines

1. Cliquez sur **Ajouter** sur la page **Fournisseur DNS et mappage de domaine**.
2. Sélectionnez les fournisseurs DNS dans la liste déroulante **Sélectionner un fournisseur DNS**. Les fournisseurs DNS pris en charge par `acme.sh` sont répertoriés dans la liste déroulante. Si votre fournisseur DNS n'apparaît pas dans la liste, cela signifie qu'il n'est pas pris en charge.
3. Saisissez les détails du fournisseur tels que l'ID de clé d'accès, la clé d'accès secrète et cliquez sur **Enregistrer** pour sauvegarder la configuration.
4. Cliquez sur **Ajouter un domaine** sous **Mappage de domaine**.
5. Sélectionnez les domaines gérés par le fournisseur DNS configuré.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT :

Assurez-vous que chaque domaine est lié au fournisseur DNS correct. NetScaler Console utilise ces mappages pour effectuer automatiquement le défi DNS-01. Lors de l'émission ou du renouvellement, NetScaler Console crée les enregistrements TXT requis dans le fournisseur DNS mappé. Une fois la validation réussie, l'autorité de certification émet ou renouvelle le certificat. Les certificats ne sont renouvelés que lorsque tous les domaines associés sont correctement mappés à leurs fournisseurs DNS.

Par exemple, si votre organisation utilise Amazon Route53 comme fournisseur DNS. Tout d'abord, ajoutez les informations d'identification Amazon Route53 (ID de clé d'accès et clé secrète) sous Détails du fournisseur DNS. Ensuite, mappez les domaines gérés par Amazon Route53 (par exemple : example.com, app.example.com). Lorsqu'un certificat pour ces domaines est émis ou renouvelé, NetScaler Console crée automatiquement les enregistrements TXT requis dans Amazon Route53. Une fois la validation réussie, l'autorité de certification émet ou renouvelle les certificats.
Les fournisseurs DNS publics suivants sont pris en charge :

- 1984.hosting
- ACME DNS
- AcmeProxy Server API
- Active24
- Akamai.com Edge DNS
- Aliyun
- All-inkl Kas Server
- Alviy.com
- Amazon Route53
- Anexia.com CloudDNS
- ArtFiles.de
- ArvanCloud.ir
- autoDNS-InternetX
- Azure DNS
- Azion.om
- Beget.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- BookMyName.com
- Bunny.net
- CloudFlare
- ClouDNS.net
- ConoHa
- Constellix.com
- Core-Networks
- cPanel Server API
- Curanet.dk
- cyon.ch
- DDNSS.de
- deSEC.io
- DigitalOcean
- DirectAdmin
- DNS.Services
- DNSExit.com
- dns.la
- DNSMadeEasy
- DNSimple
- dnsHome.de
- DNSPod.cn
- DNSPod.com
- Domain-Offensive do.de
- DomeneShop.no
- DreamHost
- DuckDNS.org
- durabledns.com
- Dyn.com
- DynDnsFree.de
- Dynu.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DynV6.com
- easyDNS.net
- API DNS edgecenter
- EUserv.com
- Exoscale
- Fornex.com
- FreeDNS
- FreeMyIP.com
- Gandi LiveDNS
- Gcore.com
- GeoScaling.com
- GoDaddy.com
- Google Cloud DNS
- Google Domains
- Hetzner.com
- Hexonet.com
- hosting.de
- HuaweiCloud.com
- Hurricane Electric
- Hurricane Electric HE.net DDNS
- Infoblox
- Infomaniak.com
- INWX
- IONOS Cloud DNS
- IONOS.de
- InternetBS.net
- ISPConfig 3.1
- jdcloud.com
- Joker.com
- kapper.net

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- King.host
- Knot DNS
- Leaseweb.com
- Client DNS Lexicon
- lima-city.de
- Linode
- Linode.com-Old
- Loopia
- LuaDNS
- MailinaBox
- MaraDNS
- mijn.host
- Misaka.io
- MyDNS.JP
- Mythic-Beasts.com
- Name.com
- Namecheap
- NameMaster.de
- Namesilo
- Nanelo.com
- NederHost.nl
- Neodigit.net
- Netcup
- Netlify.com
- nic.ru
- Njalla
- NLnetLabs NSD
- NS1.com
- Nexcess
- one.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Online.net
- omg.lol
- OpenProvider
- OpenStack Designate API
- OPNsense
- Oracle Cloud Infrastructure-OCI
- OVH.com
- Plesk XML
- PointHQ
- Porkbun.com
- PowerDNS
- RackCorp.com
- RackSpace.com
- rage4.com
- RcodeZero
- reg.ru
- ScaleWay.com
- Schlundtech
- Selectel
- SelfHost.de
- ServerCow.de
- Simply.com
- Technitium DNS Server
- tele3.cz
- Tencent.com
- Timeweb.Cloud
- TransIP.nl
- UltraDNS
- united-domains Reselling
- unoeuro.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- variomedia.de
- Vercel.com
- veesp.com
- versio.nl AuroraDNS
- VSCALE
- vshosting.cz CloudDNS
- Vultr
- Websupport.sk
- West.cn
- World4You.com
- API DNS Yandex 360 pour les entreprises.
- Yandex Cloud DNS
- Zilore
- Zone.eu
- ZoneEdit.com
- Zonomi

Une fois les trois étapes terminées, NetScaler Console configure le serveur ACME CA. Les certificats sélectionnés sont renouvelés pour les domaines mappés. NetScaler Console vérifie périodiquement la validité des certificats et les renouvelle avant leur expiration (en fonction de la fenêtre configurée). Sans aucune intervention manuelle requise, les certificats restent toujours valides et à jour.

Émission et renouvellements

Accédez à **Infrastructure > Tableau de bord SSL > Émission et renouvellements** pour vérifier toutes les activités de renouvellement et les nouvelles demandes issues de l'émission de certificats.

Renouvellements automatiques

L'onglet **Renouvellements automatiques** répertorie les certificats inscrits pour le renouvellement automatique. Lorsque la fenêtre de renouvellement configurée est atteinte, NetScaler Console les renouvelle automatiquement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également déclencher un renouvellement à la demande avant la fenêtre de renouvellement planifiée. Pour un renouvellement à la demande, sélectionnez le certificat requis et cliquez sur **Renouveler maintenant**.

Si vous ne souhaitez pas que certains certificats soient renouvelés automatiquement, vous pouvez passer aux renouvellements manuels. Pour transférer les certificats du renouvellement automatique au renouvellement manuel, sélectionnez les certificats requis et cliquez sur **Migrer vers le renouvellement manuel**.



Renouvellements manuels

L'onglet **Renouvellements manuels** répertorie tous les certificats qui doivent être renouvelés manuellement. Ces certificats doivent être mis à jour manuellement, soit en renouvelant le certificat hors ligne et en téléchargeant le nouveau certificat dans le magasin approprié, soit en utilisant l'option **Renouveler maintenant**.

Pour renouveler un certificat, sélectionnez un certificat et cliquez sur **Renouveler maintenant**. Si le certificat est émis par une autorité de certification enregistrée et que le fournisseur DNS de son domaine est configuré, vous pouvez le renouveler à la demande en utilisant ACME sans le déplacer vers les renouvellements automatiques.

Vous pouvez également déplacer un certificat vers le renouvellement automatique. Pour transférer les certificats du renouvellement manuel au renouvellement automatique, sélectionnez les certificats requis et cliquez sur **Migrer vers le renouvellement automatique**.

REMARQUE :

Vous ne pouvez renouveler ou migrer qu'un seul certificat à la fois.



Journaux d'émission et de renouvellement

L'onglet **Journaux d'émission et de renouvellement** fournit la liste des demandes de certificat utilisant ACME, y compris les émissions et les renouvellements. Pour un événement ayant échoué, vous pouvez cliquer sur l'icône d'information pour afficher les informations détaillées sur l'erreur.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Émettre un certificat

L'intégration d'ACME dans NetScaler Console prend en charge la demande de nouveaux certificats directement à l'aide du protocole ACME. Vous pouvez soit créer un CSR au sein de NetScaler Console, soit télécharger un CSR existant pour demander de nouveaux certificats.

Accédez à **Infrastructure > Tableau de bord SSL > Émissions et renouvellement**, puis cliquez sur **Émettre un certificat** et sélectionnez l'une des options suivantes en fonction de votre scénario :

- **Je n'ai pas de CSR** : Si vous n'avez pas encore de CSR, NetScaler Console vous permet d'en générer un et d'émettre un nouveau certificat.
- **J'ai un CSR** : Si vous avez déjà un CSR généré hors ligne, vous pouvez le télécharger pour émettre un certificat.

Émettre un certificat sans CSR

Effectuez les étapes suivantes pour générer un CSR et émettre un nouveau certificat :

1. Accédez à **Infrastructure > Tableau de bord SSL > Émissions et renouvellement**, puis cliquez sur **Émettre un certificat** et sélectionnez **Je n'ai pas de CSR**.

   

2. Sur la page **Clé de certificat**, téléchargez une clé existante en sélectionnant **J'ai une clé** ou générez-en une nouvelle en sélectionnant **Je n'ai pas de clé**.

   

3. Saisissez les informations CSR requises.

   

4. Sélectionnez l'AC, le fournisseur DNS et le mode de déploiement du certificat pour la requête ACME. Choisissez **Cert Store** pour un déploiement manuel, ou **Zero Touch Store** pour un déploiement automatique sur NetScaler.
5. Sélectionnez **Renouveler automatiquement le certificat** si vous souhaitez que le certificat soit automatiquement renouvelé à l'avenir.

   

6. Cliquez sur **Enregistrer**.

Émettre un certificat avec CSR

Effectuez les étapes suivantes si vous avez déjà un CSR généré hors ligne et que vous souhaitez le télécharger pour émettre un certificat :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Infrastructure > Tableau de bord SSL > Émissions et renouvellement**, puis cliquez sur **Émettre un certificat** et sélectionnez **J'ai un CSR**.

   

2. Choisissez le fichier CSR et le fichier de clé associé depuis votre système local.

   

3. Sélectionnez l'AC, le fournisseur DNS et le mode de déploiement du certificat pour la requête ACME. Choisissez **Cert Store** pour un déploiement manuel, ou **Zero Touch Store** pour un déploiement automatique sur NetScaler.
4. Sélectionnez **Renouveler automatiquement le certificat** si vous souhaitez que le certificat soit automatiquement renouvelé à l'avenir.

   

5. Cliquez sur **Enregistrer**.

Intégration tierce

Vous pouvez ajouter et gérer plusieurs fournisseurs d'autorité de certification (CA) et de DNS.

Vous pouvez effectuer les actions suivantes à partir de la page **Intégration tierce** :

- Ajouter ou modifier un fournisseur de CA
- Modifier les paramètres de renouvellement automatique
- Ajouter ou modifier le certificat d'une autorité de certification (CA) configurée existante
- Ajouter ou modifier un fournisseur DNS
- Modifier les mappages de domaine

Ajouter ou modifier un fournisseur de CA

Vous pouvez enregistrer plusieurs fournisseurs d'autorité de certification (CA) pour gérer les certificats émis par différents fournisseurs. Vous pouvez également modifier les détails des fournisseurs d'autorité de certification (CA) existants.

1. Accédez à **Tableau de bord SSL > Intégration tierce > ACME > Fournisseurs d'autorité de certification (CA)**. Cliquez sur **Ajouter**.
2. Pour ajouter un fournisseur de CA, donnez-lui un nom et sélectionnez la CA.
3. Pour modifier les détails d'un fournisseur d'autorité de certification (CA) existant, sélectionnez le fournisseur d'autorité de certification (CA) et cliquez sur **Modifier**.
4. Ajoutez ou mettez à jour les détails requis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Cliquez sur **Enregistrer**.

Modifier les paramètres de renouvellement automatique

Pour modifier les paramètres de renouvellement automatique, procédez comme suit :

1. Accédez à **Tableau de bord SSL > Intégration tierce > ACME > Fournisseurs de CA**.
2. Sélectionnez un fournisseur de CA, et cliquez sur **Modifier**
3. Dans la fenêtre **Configurer le fournisseur d'autorité de certification**, modifiez le nombre de jours selon vos besoins dans la section **Paramètres de renouvellement automatique**.
4. Cliquez sur **Enregistrer et continuer**.
5. Terminez le workflow.

Ajouter ou modifier le certificat à partir d'une autorité de certification configurée existante

Pour ajouter ou modifier le certificat à partir d'une autorité de certification configurée existante, procédez comme suit

1. Accédez à **Tableau de bord SSL > Intégration tierce > ACME > Fournisseurs de CA**.
2. Sélectionnez un fournisseur de CA, et cliquez sur **Modifier**.
3. Accédez à **Étape 2 Sélectionner les certificats**, et ajoutez ou supprimez les certificats requis.
4. Cliquez sur **Enregistrer et continuer**.
5. Terminez le workflow.

REMARQUE :

Si le certificat n'a pas été dissocié de l'autorité de certification d'origine, il n'apparaît pas dans la liste de sélection pour la nouvelle autorité de certification.

Ajouter ou modifier un fournisseur DNS

Pour ajouter un nouveau fournisseur DNS ou modifier les mappages de domaine existants des fournisseurs DNS existants, procédez comme suit :

1. Accédez à **Tableau de bord SSL > Intégration tierce > ACME > Fournisseurs DNS**.
2. Pour ajouter un fournisseur DNS, cliquez sur **Ajouter**. Sélectionnez le fournisseur DNS, puis cliquez sur **Enregistrer**.
3. Pour modifier un fournisseur DNS existant, sélectionnez un fournisseur DNS, puis cliquez sur **Modifier**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Ajoutez ou mettez à jour les détails requis.
5. Cliquez sur **Enregistrer**.

Modifier les mappages de domaine

Pour modifier les mappages de domaine des fournisseurs DNS existants, procédez comme suit :

1. Accédez à **Tableau de bord SSL > Intégration tierce > ACME > Fournisseurs DNS**.
2. Sélectionnez un fournisseur DNS, puis cliquez sur **Modifier**.
3. Accédez à **Mappage de domaine**, puis ajoutez ou supprimez des domaines selon les besoins.
4. Cliquez sur **Enregistrer**.

IMPORTANT :

Si un domaine n'est pas mappé, son renouvellement de certificat s'arrête. Toujours remapper les domaines à un fournisseur DNS valide pour garantir la poursuite des renouvellements.

Limitations

- Le renouvellement de certificat n'a lieu que pour les fournisseurs DNS pris en charge par `acme.sh`.

Dépanner les problèmes liés au renouvellement automatique des certificats

Quelques messages d'erreur courants qui peuvent survenir et leur cause première associée sont répertoriés dans cette section :

- L'erreur **Certificate has invalid domain - ADCD** est signalée lorsque le nom de domaine dans le certificat n'est pas valide selon les exigences ACME.
- L'erreur **Invalid identifiers requested :: Cannot issue for "testdomain": Domain name needs at least one dot** est signalée lorsque le nom de domaine demandé ne contient pas de point (tel que "example" au lieu de "example.com").
- L'erreur **Could not get nonce from the CA server. Please check the CA server configuration.** est signalée lorsque le client ACME ne parvient pas à obtenir un nonce du CA, souvent en raison de problèmes de réseau ou de serveur.
- L'erreur **Cannot initialize API for the CA server. Please check the CA server configuration.** est signalée lorsque le client ACME ne peut pas initialiser la communication avec le serveur CA, éventuellement en raison d'une mauvaise configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'erreur **Invalid domain name provided. Please check the domain name and try again.** est signalée lorsque le format du nom de domaine est invalide ou non autorisé par le protocole ACME.
- L'erreur **Domains not changed. Certificate with same configuration already exists.** est signalée lorsqu'une demande de certificat est effectuée sans modification de la liste de domaines et que le certificat existe déjà.
- L'erreur **Error adding TXT record for domain validation. Please check the DNS configuration and try again.** est signalée lorsque le client ACME ne parvient pas à ajouter l'enregistrement DNS TXT requis pour la validation de domaine.
- L'erreur **Signature does not match. Please check the server time as it may not be in sync.** est signalée lorsqu'il y a une non-concordance de signature, souvent en raison de problèmes de synchronisation horaire entre le client et le serveur.
- L'erreur **Certificate is missing a DNS provider name.** est signalée lorsqu'aucun fournisseur DNS n'est spécifié pour la validation de domaine basée sur DNS.
- **Renouvellement ignoré car aucun fournisseur DNS actif n'est configuré.** est signalé lorsque le renouvellement du certificat est tenté mais qu'aucun fournisseur DNS actif n'est configuré.
- **Erreur de validation du ou des contacts :: impossible d'analyser l'adresse e-mail** est signalé lorsque l'adresse e-mail du contact fournie est invalide ou ne peut pas être analysée.
- **Impossible de traiter la demande de finalisation de commande. (Pour une URL de répertoire ACME invalide)** est signalé lorsque le client ACME ne peut pas finaliser la commande, souvent en raison d'une URL de répertoire ACME invalide ou inaccessible.
- **Fournisseur DNS - TestDNS n'existe pas ou n'est pas actif.** est signalé lorsque le fournisseur DNS spécifié est introuvable ou est inactif dans le système.
- **L'ID de configuration CA est vide/n'existe pas.** est signalé lorsque l'ID de configuration CA est manquant ou ne correspond à aucune configuration existante.

Gestion des certificats zéro-touche

Dans NetScaler Console, vous pouvez configurer la gestion des certificats zéro-touche sur les instances NetScaler gérées exécutant la version **14.1-34.x** et ultérieure. Avec la gestion des certificats zéro-touche, vous éliminez les interventions manuelles et créez un magasin de certificats zéro-touche en mémoire pour répondre aux requêtes d'application. Accédez à **Infrastructure > Tableau de bord SSL > Gestion des certificats zéro-touche** pour télécharger tous les certificats et clés sur NetScaler Console, et l'activer sur les instances NetScaler gérées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler interroge périodiquement le référentiel de certificats et fournit les certificats nécessaires selon les besoins.

Avec la gestion des certificats zéro-touche, les processus suivants sont automatiquement effectués par NetScaler® :

- Ajout, liaison et association des certificats
- Fourniture des certificats et des clés dans un ordre spécifique ou ensemble
- Installation et utilisation des certificats appropriés en fonction des requêtes
- Suppression des certificats expirés pendant le cycle d'interrogation périodique

Pour plus d'informations sur le fonctionnement du certificat zéro-touche sur les instances NetScaler, consultez Gestion des certificats zéro-touche NetScaler.

En tant qu'administrateur, vous devez vous assurer des points suivants dans NetScaler Console :

- Les instances NetScaler exécutent la version 14.1-34.x ou ultérieure et sont gérées dans NetScaler Console.
- Téléchargez les certificats (dans n'importe quel format) et les clés. Ensuite, activez la fonction zéro-touche sur les instances NetScaler gérées.
- Assurez-vous qu'un certificat CA valide est présent sur NetScaler Console. Si vous disposez d'un certificat CA de console mis à jour, téléchargez le certificat avant d'activer la fonction zéro-touche sur les instances NetScaler gérées. Le message d'erreur suivant s'affiche si aucun certificat CA n'est présent sur NetScaler Console :



Télécharger les certificats

1. Accédez à **Infrastructure > Tableau de bord SSL > Gestion des certificats zéro-touche**.
2. Cliquez sur **Démarrer**.



3. Les instances NetScaler exécutant la version 14.1-34.x ou ultérieure sont répertoriées. Vous pouvez soit cliquer sur **Configurer le zéro-touch** pour activer le zéro-touch, soit cliquer sur **Ignorer** pour passer à l'étape suivante.
4. Cliquez sur **Télécharger** pour télécharger tous les certificats (peuvent être dans n'importe quel format, tel que .pem, .cer et .crt).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Le fichier de certificat ou de clé doit être inférieur à 8192 octets.
- Si vous téléchargez plusieurs certificats ou fichiers de clés, la taille maximale prise en charge est de 50000 octets.
- Si les certificats ou les fichiers de clés sont protégés par un mot de passe, assurez-vous de fournir le mot de passe. Si le mot de passe n'est pas fourni, le certificat ou le fichier de clé n'est pas téléchargé.

Activer la gestion des certificats zéro-touch

Après avoir téléchargé les certificats, vous devez activer le zéro-touch sur les instances NetScaler gérées.

1. Depuis la page **Gestion des certificats zéro-touch**, cliquez sur **Configurer le zéro-touch**.



2. Cliquez sur **Ajouter des instances**, sélectionnez les instances, puis cliquez sur **Activer**.



NetScaler Console utilise l'intervalle d'interrogation par défaut pour interroger tous les certificats des instances NetScaler. Vous pouvez utiliser l'option **Interroger maintenant** pour interroger immédiatement.

Dans le **tableau de bord SSL**, vous pouvez également afficher l'utilisation des certificats sans contact qui présente les détails des certificats actifs et inactifs.

Vue du tableau de bord SSL(/en-us/netscaler-application-delivery-management-software/media/zero-touch-ssl-dashboard.png)

Prise en charge du mode de filtrage SSL

Une instance NetScaler récupère les métadonnées de certificats SSL et de clés privées spécifiques. Cette approche du moindre privilège garantit que les instances n'accèdent qu'aux ressources dont elles ont besoin, empêchant ainsi qu'une compromission sur une instance n'expose l'ensemble de votre infrastructure de certificats. Cette fonctionnalité est particulièrement utile pour les environnements où plusieurs administrateurs gèrent un groupe d'instances NetScaler à des fins distinctes.

Voici quelques-uns des avantages :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Segmentation de la sécurité** - Restreint l'accès aux métadonnées au niveau de chaque NetScaler afin de minimiser la surface d'attaque et de respecter les politiques de sécurité de l'organisation.
- **Expérience d'administration simplifiée** - Réduit la complexité des déploiements multi-locataires ou départementaux en n'affichant aux administrateurs que les ressources pertinentes pour leur groupe d'instances NetScaler.
- **Utilisation optimisée des ressources** - Empêche le gonflement de la mémoire système en récupérant les métadonnées uniquement des certificats SSL et des clés privées requis.

La configuration du mode de filtrage définit la manière dont les instances NetScaler et les fichiers SSL interagissent via des types de synchronisation spécifiques. Vous pouvez gérer ces paramètres via NetScaler Console pour vous assurer que seules les métadonnées nécessaires sont récupérées par chaque instance.

COMPOSANT	TYPE DE SYNCHRO	DESCRIPTION
Instance NetScaler	Synchro personnalisée	Les instances NetScaler dans ce mode récupèrent uniquement les métadonnées des certificats et des clés spécifiquement mappés à l'instance.
Instance NetScaler	Synchronisation globale	Les instances NetScaler dans ce mode récupèrent les métadonnées de tous les certificats et clés privées téléchargés.
Fichiers SSL	Fichiers personnalisés	Ces fichiers sont spécifiquement mappés aux instances NetScaler en mode Synchronisation personnalisée.
Fichiers SSL	Fichiers globaux	Les métadonnées de ces fichiers sont récupérées par toutes les instances NetScaler en mode Synchronisation globale.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer les paramètres du mode de filtrage

Pour configurer le mode de filtrage, définissez les types de synchronisation pour vos instances et fichiers. Cela garantit une distribution sécurisée et optimisée des métadonnées sensibles.

Vous pouvez télécharger des certificats et des clés privées directement en utilisant le bouton de téléchargement dans les sections **Fichiers de certificats** et **Instances NetScaler** du tableau de bord SSL.

Pour configurer à l'aide de l'interface graphique :

1. **Télécharger de nouveaux fichiers (jour zéro)** - Accédez à **Fichiers de certificats et instances NetScaler > Télécharger** pour ajouter de nouveaux actifs.

   Sélectionnez l'un des types de synchronisation suivants :

   - **GLOBAL** - Sélectionnez pour utiliser le mode de synchronisation global et terminer le téléchargement.
   - **PERSONNALISÉ** - Sélectionnez pour utiliser le mode de synchronisation personnalisé, choisissez les instances spécifiques pour le mappage, puis téléchargez les fichiers.

2. **Déplacer les fichiers existants (jour N)** - Pour déplacer les certificats et les clés du mode de synchronisation global vers le mode de synchronisation personnalisé, sélectionnez les instances NetScaler cibles et cliquez sur **Ajouter des fichiers existants**.
3. **Sélectionner les domaines** - Une fois les instances sélectionnées, choisissez les domaines pertinents pour déclencher le déplacement. NetScaler Console détecte et déplace automatiquement les certificats et les fichiers de clé privée correspondants vers le mode de synchronisation personnalisé.
4. **Afficher les actifs** - Accédez à la page de destination pour afficher tous les certificats et fichiers de clé privée mappés à chaque instance NetScaler en mode de synchronisation personnalisé.
5. **Changer de mode de synchronisation** - Pour ramener les instances en mode de synchronisation global, cliquez sur **Passer à la synchronisation globale** sur la page de destination.

Utiliser le tableau de bord SSL

Vous pouvez utiliser le tableau de bord des certificats SSL dans NetScaler Console pour afficher des graphiques qui vous aident à suivre les émetteurs de certificats, les forces de clé et les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

algorithmes de signature. Le tableau de bord des certificats SSL affiche également des graphiques qui indiquent les éléments suivants :

- Nombre de jours après lesquels les certificats expirent
- Nombre de certificats utilisés et non utilisés
- Nombre de certificats auto-signés et signés par une CA
- Nombre d'émetteurs
- Algorithmes de signature
- Protocoles SSL
- Top 10 des instances par nombre de certificats utilisés

Pour surveiller les certificats SSL

Vous pouvez utiliser le tableau de bord SSL sur NetScaler Console pour surveiller vos certificats si votre entreprise a une politique SSL où vous avez défini certaines exigences en matière de certificats SSL, telles que tous les certificats doivent avoir une force de clé minimale de 2048 bits et être autorisés par une autorité de CA de confiance.

Dans un autre exemple, vous avez peut-être téléchargé un nouveau certificat mais oublié de le lier à un serveur virtuel. Le tableau de bord SSL met en évidence les certificats SSL utilisés ou non utilisés. Dans la section **Utilisation**, vous pouvez voir le nombre de certificats qui ont été installés et le nombre de certificats utilisés. Vous pouvez ensuite cliquer sur le graphique pour voir le nom des certificats, l'instance sur laquelle il est utilisé, sa validité, son algorithme de signature, etc.

Pour surveiller les certificats SSL dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.

NetScaler Console vous permet d'interroger les certificats SSL et d'ajouter immédiatement tous les certificats SSL des instances à NetScaler Console. Pour ce faire,

1. Accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur **Interroger maintenant**.

   Sur la page **Interroger maintenant**, vous pouvez interroger toutes les instances NetScaler gérées ou sélectionner des instances spécifiques.
3. Cliquez sur **Démarrer l'interrogation**.

Dans le **Tableau de bord SSL**, vous pouvez surveiller les certificats SSL NetScaler, les serveurs virtuels SSL et les protocoles SSL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez cliquer sur les métriques du tableau de bord pour afficher les détails relatifs aux certificats SSL, aux serveurs virtuels SSL ou aux protocoles SSL.

Par exemple, lorsque vous cliquez sur le nombre sous **Auto-signés vs signés par une CA** sur le tableau de bord, l'interface graphique de NetScaler Console affiche tous les certificats SSL sur les instances NetScaler.



Le tableau de bord SSL de NetScaler Console affiche également la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels. En tant qu'administrateur, vous pouvez spécifier les protocoles que vous souhaitez surveiller via la stratégie SSL. Pour plus d'informations, consultez Configuration des stratégies SSL. Les protocoles pris en charge sont SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 et TLS 1.3. Les protocoles SSL utilisés sur les serveurs virtuels apparaissent sous forme de graphique à barres. Cliquer sur un protocole spécifique affiche une liste des serveurs virtuels utilisant ce protocole.

Un graphique en anneau apparaît après l'activation ou la désactivation des clés Diffie-Hellman (DH) ou RSA éphémères sur le tableau de bord SSL. Ces clés permettent une communication sécurisée avec les clients d'exportation même si le certificat de serveur ne prend pas en charge les clients d'exportation, comme dans le cas d'un certificat de 1024 bits. Cliquer sur le graphique approprié affiche une liste des serveurs virtuels sur lesquels les clés DH ou RSA éphémères sont activées.

Pour afficher les pistes d'audit des certificats SSL

Vous pouvez désormais afficher les détails des journaux des certificats SSL sur NetScaler Console. Les détails des journaux affichent les opérations effectuées à l'aide de certificats SSL sur NetScaler Console, telles que : l'installation de certificats SSL, la liaison et la déliaison de certificats SSL, la mise à jour de certificats SSL et la suppression de certificats SSL. Les informations de piste d'audit sont utiles lors de la surveillance des modifications de certificats SSL effectuées sur une application avec plusieurs propriétaires.

Pour afficher un journal d'audit pour une opération particulière effectuée sur NetScaler Console à l'aide de certificats SSL, accédez à **Infrastructure > Tableau de bord SSL** \> et cliquez sur **Journaux d'audit**.



Pour une opération particulière effectuée à l'aide d'un certificat SSL, vous pouvez afficher son statut, son heure de début et son heure de fin. De plus, vous pouvez afficher l'instance sur laquelle l'opération a été effectuée et les commandes exécutées sur cette instance.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour supprimer le certificat SSL sur le tableau de bord SSL

NetScaler 14.1-38.x et versions ultérieures offre la possibilité de supprimer les fichiers de certificat SSL associés de NetScaler lors de la suppression de la configuration sélectionnée d'un certificat SSL. Pour supprimer un certificat SSL :

1. Accédez à **Infrastructure > Tableau de bord SSL**.
2. Dans la section **Certificats SSL** où les détails des certificats SSL sont affichés, cliquez sur le lien de l'étiquette **Inutilisé**.
3. Une page affichant une liste de certificats inutilisés s'affiche.
4. Choisissez un ou plusieurs certificats inutilisés que vous souhaitez supprimer.

   
5. Cliquez sur **Supprimer**.
6. Une boîte de dialogue **Confirmer** apparaît, offrant les options suivantes pour supprimer également les fichiers de certificat de NetScaler® :

   - **Ne pas supprimer** : Ignore la suppression des fichiers de certificat de NetScaler.
   - **Supprimer** : Supprime les fichiers de certificat de NetScaler pour les certificats expirés et non expirés.
   - **Supprimer si expiré** : Supprime les fichiers de certificat de NetScaler uniquement pour les certificats expirés.

   REMARQUE :

   Pour les versions de NetScaler antérieures à 14.1-38.x, la suppression du ou des fichiers de certificat est ignorée pour les trois options. L'option de suppression du fichier de certificat avec la configuration n'est applicable qu'à partir de NetScaler 14.1-38.x.
7. Sélectionnez l'option appropriée en fonction de vos besoins.
8. Cliquez sur **Oui** pour supprimer le certificat ou sur **Non** pour quitter le flux de travail sans apporter de modifications.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour exclure les certificats NetScaler par défaut sur le tableau de bord SSL

NetScaler Console vous permet d'afficher ou de masquer les certificats NetScaler par défaut qui apparaissent sur les graphiques du tableau de bord SSL, selon vos préférences. Par défaut, tous les certificats sont affichés sur le tableau de bord SSL, y compris les certificats par défaut.

Pour afficher ou masquer les certificats par défaut sur le tableau de bord SSL :

1. Accédez à **Infrastructure > Tableau de bord SSL** dans l'interface graphique de NetScaler Console.
2. Sur la page **Tableau de bord SSL**, cliquez sur **Paramètres**.
3. Sur la page **Paramètres**, sélectionnez **Général**.
4. Saisissez le nombre de jours avant l'expiration du certificat pour recevoir une notification concernant l'expiration du certificat.
5. Sélectionnez la méthode de notification et créez les profils correspondants.
6. Dans la section **Filtre de certificat**, décochez la case **Afficher les certificats par défaut** et cliquez sur **Enregistrer et quitter**.



Afficher, télécharger et téléverser des fichiers SSL

Pour afficher les fichiers SSL sur NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL > Fichiers SSL sur NetScaler Console**.

Vous pouvez afficher, télécharger et téléverser les fichiers suivants sur NetScaler Console :

- Certificats SSL
- Clés SSL
- CSR SSL

Pour afficher et télécharger des fichiers SSL sur une instance NetScaler, accédez à **Infrastructure > Tableau de bord SSL > Fichiers SSL sur NetScaler**.

Vous ne pouvez accéder aux fichiers SSL qu'après la sauvegarde des instances NetScaler, soit manuellement, soit via un processus de sauvegarde planifié.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT :

Pour activer le téléchargement des fichiers SSL à partir des instances NetScaler, activez la fonctionnalité **Certificats SSL d'instance**. Pour plus d'informations, consultez Activer ou désactiver les fonctionnalités de NetScaler Console.

Afficher la chaîne de certificats SSL

Vous pouvez afficher la chaîne de certificats complète, des certificats intermédiaires jusqu'au certificat d'autorité de certification racine.

Pour afficher une chaîne de certificats :

1. Accédez à **Infrastructure > Tableau de bord SSL** et cliquez sur les certificats SSL dans n'importe quelle vignette.
2. Dans la page **Certificats SSL**, sélectionnez un certificat et cliquez sur **Détails**. La chaîne de certificats s'affiche sous **Liens**.



Configurer les notifications d'expiration des certificats SSL

En tant qu'administrateur de sécurité, vous pouvez configurer des notifications pour vous informer de l'expiration prochaine des certificats et inclure des informations sur les instances Citrix NetScaler qui utilisent ces certificats. En activant les notifications, vous pouvez renouveler vos certificats SSL à temps.

Par exemple, vous pouvez configurer une notification par e-mail à envoyer à une liste de distribution d'e-mails 30 jours avant l'expiration de votre certificat.

Pour configurer les notifications depuis NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Sur la page **Tableau de bord SSL**, cliquez sur **Paramètres**.
3. Sur la page **Paramètres SSL**, cliquez sur l'icône **Modifier** .
4. Dans la section **Paramètres de notification**, spécifiez quand vous souhaitez envoyer la notification en termes de nombre de jours avant la date d'expiration.
5. Choisissez le type de notification que vous souhaitez envoyer. Sélectionnez le type de notification et la liste de distribution dans le menu déroulant. Les types de notification sont les suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **E-mail** – Spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos certificats sont sur le point d'expirer.
- **SMS** – Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos certificats sont sur le point d'expirer.
- **Slack** - Spécifiez les détails du profil Slack.
- **Alertes PagerDuty** - Spécifiez un profil PagerDuty. En fonction des paramètres de notification configurés dans votre portail PagerDuty, une notification est envoyée lorsque vos certificats sont sur le point d'expirer.
- **ServiceNow** - Une notification est envoyée au profil ServiceNow par défaut lorsque vos certificats sont sur le point d'expirer.

  IMPORTANT

  Assurez-vous que l'adaptateur ITSM de Citrix Cloud est configuré pour ServiceNow et intégré à NetScaler Console. Pour plus d'informations, consultez (/fr-fr/netscaler-application-delivery-management-software/current-release/configure/integrate-itsm-adapter-netscaler-adm-servicenow.html).

6. Cliquez sur **Enregistrer et quitter**.

NetScaler Console envoie désormais un piège d'expiration de certificat SSL au serveur de destination de piège externe lorsque vos certificats SSL sont sur le point d'expirer. NetScaler Console envoie un piège lorsque les deux conditions suivantes sont remplies :

- Vous avez configuré le nombre de jours avant l'expiration du certificat dans la page des paramètres du tableau de bord SSL.
- Vous avez ajouté la destination du piège.

Vous pouvez définir les destinations de piège en accédant à **Paramètres > SNMP > Destinations de piège**. Saisissez l'adresse IP du serveur SNMP de destination où les pièges sont envoyés. Entrez le numéro de port et tapez « public » (sans guillemets) comme chaîne de communauté.

Mettre à jour un certificat installé

Après avoir reçu un certificat renouvelé de l'autorité de certification (CA), vous n'avez pas besoin de vous connecter aux instances NetScaler individuelles pour mettre à jour les certificats. Vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pouvez mettre à jour les certificats existants dans NetScaler Console avec des certificats du magasin de certificats.

Pour mettre à jour un certificat SSL depuis NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Dans la page **Certificats SSL**, sélectionnez un certificat et cliquez sur **Mettre à jour**. Vous pouvez également cliquer sur le certificat SSL pour afficher ses détails, puis cliquer sur **Mettre à jour** dans le coin supérieur droit de la page **Certificat SSL**.
4. Dans la page **Mettre à jour le certificat SSL**, sélectionnez **Certificat** pour afficher la page **Magasin de certificats**.

   
5. Dans la page **Magasin de certificats**, sélectionnez le fichier de certificat que vous souhaitez ajouter. Cliquez sur **Sélectionner**.

   
6. Si le nom de domaine du nouveau certificat ne correspond pas à l'ancien certificat, sélectionnez **Aucune vérification de domaine** si vous souhaitez que le serveur héberge le nouveau domaine.

   

   Cliquez sur **OK**. Tous les serveurs virtuels SSL auxquels ce certificat est lié sont automatiquement mis à jour.

   REMARQUE :

   Lorsque vous mettez à jour un certificat SSL existant avec une chaîne de certificats provenant du magasin de certificats, le certificat existant est mis à jour avec les certificats liés. Sélectionnez le certificat et cliquez sur **Détails** pour afficher la chaîne de certificats.

Installer des certificats SSL sur une instance NetScaler

Avant d'installer des certificats SSL sur les instances Citrix NetScaler, assurez-vous que les certificats sont émis par des autorités de certification (CA) fiables. Assurez-vous également que la force de clé des certificats est de 2048 bits ou plus et que les clés sont signées avec des algorithmes de signature sécurisés.

Pour installer un certificat SSL à partir d'une autre instance NetScaler :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également importer un certificat à partir d'une instance NetScaler choisie et l'appliquer à d'autres instances NetScaler ciblées depuis l'interface graphique de NetScaler Console.

1. Accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur **Installer le certificat**.
3. Sur la page **Installer le certificat SSL sur les instances NetScaler**, spécifiez les paramètres suivants :

   a. **Source du certificat** Sélectionnez l'option **Importer depuis l'instance**.

      - Choisissez l'**instance** à partir de laquelle vous souhaitez importer le certificat.
      - Choisissez le **certificat** dans la liste de tous les fichiers de certificat SSL de l'instance.

   b. **Détails du certificat**

      - **Nom du certificat**. Spécifiez un nom pour la clé de certificat.
      - **Mot de passe**. Mot de passe pour chiffrer la clé privée. Vous pouvez utiliser cette option pour télécharger des clés privées chiffrées.

4. Cliquez sur **Sélectionner les instances** pour sélectionner les instances NetScaler sur lesquelles vous souhaitez installer vos certificats.
5. Pour enregistrer la configuration pour une utilisation future, cochez la case **Enregistrer la configuration**.
6. Cliquez sur **OK**.

Pour installer un certificat SSL depuis NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur **Installer le certificat**.
3. Sur la page **Installer le certificat SSL sur les instances NetScaler**, spécifiez les paramètres suivants :

   a. **Source du certificat** Sélectionnez l'option **Importer depuis le magasin de certificats**.

      - **Fichier de certificat** - Téléchargez un fichier de certificat SSL en sélectionnant soit **Local** (votre machine locale) soit **Appliance** (le fichier de certificat doit être présent sur l'instance virtuelle NetScaler Console).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **Détails du certificat**

- **Nom du certificat** – Spécifiez un nom pour la clé de certificat.

4. Cliquez sur **Sélectionner les instances** pour sélectionner les instances NetScaler Console sur lesquelles vous souhaitez installer vos certificats.
5. Pour enregistrer la configuration pour une utilisation ultérieure, cochez la case **Enregistrer la configuration**.
6. Cliquez sur **OK**.

Créer une demande de signature de certificat (CSR)

Une demande de signature de certificat (CSR) est un bloc de texte chiffré généré sur le serveur où le certificat sera utilisé. Elle contient des informations qui seront incluses dans le certificat, telles que le nom de votre organisation, le nom commun (nom de domaine), la localité et le pays.

Pour créer une CSR à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL installés, puis sélectionnez le certificat pour lequel vous souhaitez créer une CSR et choisissez **Créer une CSR** dans la liste **Sélectionner une action**.
3. Sur la page **Créer une demande de signature de certificat (CSR)**, spécifiez un nom pour la CSR.
4. Effectuez l'une des opérations suivantes :

- **Télécharger une clé** - Sélectionnez l'option **J'ai une clé**. Pour télécharger votre fichier de clé, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de clé doit être présent sur l'instance virtuelle de NetScaler Console).
- **Créer une clé** - Sélectionnez l'option Je n'ai pas de clé, puis spécifiez les paramètres suivants :

Algorithme de chiffrement	Type de clé. Par exemple, RSA.
Nom du fichier de clé	Nom de votre fichier dans lequel la clé RSA est stockée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Taille de la clé	Taille de la clé en bits.
Valeur de l'exposant public	Choisissez **3** ou **F4** dans la liste déroulante fournie. Cette valeur fait partie de l'algorithme de chiffrement requis pour créer votre clé RSA.
Format de clé	Par défaut, PEM est sélectionné. PEM est le format de clé recommandé pour votre certificat SSL.
Algorithme d'encodage PEM	Dans la liste déroulante, sélectionnez l'algorithme (**DES** ou **DES3**) que vous souhaitez utiliser pour chiffrer la clé RSA générée. Si vous sélectionnez cet algorithme, vous devrez fournir une phrase secrète PEM.
Phrase secrète PEM	Si vous avez choisi l'algorithme d'encodage PEM, saisissez une phrase secrète.
Confirmer la phrase secrète PEM	Confirmez votre phrase secrète PEM.

5. Cliquez sur **Continuer**.
6. Sur la page suivante, fournissez plus de détails.

   La plupart des champs ont des valeurs par défaut extraites du sujet du certificat sélectionné. Le sujet contient des détails tels que le nom commun, le nom de l'organisation, l'état et le pays.

   Dans le champ **Nom alternatif du sujet**, vous pouvez spécifier plusieurs valeurs, telles que des noms de domaine et des adresses IP avec un seul certificat. Les noms alternatifs du sujet vous aident à sécuriser plusieurs domaines avec un seul certificat.

   Spécifiez les noms de domaine et les adresses IP au format suivant :

   ```
   DNS:<Domain name>, IP:<IP address>
   ```

   Créer une demande de signature dans la console(/en-us/netscaler-application-delivery-management-software/media/create-csr-with-distinguished-name-fields.png)

   Dans cet exemple, il sécurise `10.0.0.1` et `www.example.com`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vérifiez les champs et cliquez sur **Continuer**.

REMARQUE

La plupart des autorités de certification acceptent les soumissions de certificats par e-mail. L'autorité de certification renvoie un certificat valide à l'adresse e-mail à partir de laquelle vous soumettez la CSR.

Lier et délier des certificats SSL

Vous créez un bundle de certificats en liant plusieurs certificats ensemble. Pour lier un certificat à un autre certificat, l'émetteur du premier certificat doit correspondre au domaine du second certificat. Par exemple, si vous souhaitez lier le certificat A au certificat B, l'« émetteur » du certificat A doit correspondre au « domaine » du certificat B.

Pour lier un certificat SSL à un autre certificat à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Sélectionnez le certificat que vous souhaitez lier, puis sélectionnez **Lier** dans la liste déroulante **Action**.
4. Dans la liste des certificats correspondants, sélectionnez le certificat auquel vous souhaitez lier, puis cliquez sur **OK**.

REMARQUE

Si aucun certificat correspondant n'est trouvé, le message suivant s'affiche : Aucun certificat trouvé à lier.

Pour délier un certificat SSL à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Choisissez l'un des certificats liés, puis sélectionnez **Délier** dans la liste déroulante **Action**.
4. Cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si le certificat sélectionné n'est pas lié à un autre certificat, le message suivant s'affiche : Le certificat n'a pas de lien CA.

Configurer une politique d'entreprise

Vous pouvez configurer une politique d'entreprise et ajouter toutes les autorités de certification (CA) approuvées, les algorithmes de signature sécurisés, et sélectionner la force de clé recommandée pour vos clés de certificat dans NetScaler Console. Si l'un des certificats installés sur votre instance Citrix NetScaler n'a pas été ajouté à la politique d'entreprise, le tableau de bord des certificats SSL affiche l'émetteur de ces certificats comme **Non recommandé**.

De plus, si la force de la clé de certificat ne correspond pas à la force de clé recommandée dans la politique d'entreprise, le tableau de bord des certificats SSL affiche les forces de ces clés comme **Non recommandé**.

Pour configurer une politique d'entreprise sur NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure** \> **Tableau de bord SSL**, puis cliquez sur **Paramètres**.
2. Sur la page Paramètres SSL, cliquez sur l'icône **Modifier** pour ajouter toutes les autorités de certification (CA) approuvées, les algorithmes de signature sécurisés, et sélectionner la force de clé recommandée pour vos certificats et clés. Les forces de clé prises en charge sont 512, 1024, 2048, 3072 et 4096 bits.
    - **Forces de clé recommandées** - Indique la sécurité de l'algorithme et le nombre de bits dans une clé.
    - **Algorithmes de signature recommandés** - Indique les jetons signés émis pour les applications.
    - **Autorité de certification (CA) approuvée recommandée** - Indique l'entité de confiance qui émet les certificats numériques. Cliquez sur l'icône **+** pour ajouter d'autres entités.
    - **Protocoles SSL recommandés** - Indique les versions TLS/SSL.
3. Cliquez sur **Enregistrer** pour sauvegarder votre politique d'entreprise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Le tableau de bord SSL affiche uniquement les **algorithmes de signature** qui sont sélectionnés via l'option **Paramètres** et les autres sont affichés comme **Non recommandé**.

Interroger les certificats SSL des instances NetScaler

NetScaler Console interroge automatiquement les certificats SSL une fois toutes les 24 heures à l'aide des appels NITRO et du protocole Secure Copy (SCP). Vous pouvez également interroger manuellement les certificats SSL pour découvrir les certificats SSL nouvellement ajoutés sur les instances Citrix NetScaler. L'interrogation de tous les certificats SSL des instances NetScaler entraîne une charge importante sur le réseau.

Au lieu d'interroger tous les certificats SSL des instances NetScaler, vous pouvez interroger manuellement uniquement les certificats SSL d'une ou plusieurs instances sélectionnées.

Pour interroger les certificats SSL sur les instances NetScaler :

1. Dans NetScaler Console, accédez à **Infrastructure > Tableau de bord SSL**.
2. Sur la page **Tableau de bord SSL**, dans le coin supérieur droit, cliquez sur **Interroger maintenant**.

   
3. La page **Interroger maintenant** s'affiche, vous donnant la possibilité d'interroger toutes les instances NetScaler du réseau ou d'interroger les instances sélectionnées.

   a. Pour interroger les certificats SSL de toutes les instances NetScaler, sélectionnez l'onglet **Toutes les instances** et cliquez sur **Démarrer l'interrogation**.

   

   b. Pour interroger des instances spécifiques, sélectionnez l'onglet **Sélectionner Instances**, sélectionnez les instances dans la liste et cliquez sur **Interroger maintenant**.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser le magasin de certificats NetScaler Console pour gérer les certificats SSL

Le magasin de certificats NetScaler Console vous aide à stocker et à gérer vos certificats SSL en un seul endroit. Vous pouvez ensuite utiliser les certificats stockés pour configurer les paramètres NetScaler.

Le magasin de certificats vous permet d'ajouter, de mettre à jour et de supprimer des certificats SSL. Vous pouvez également utiliser le magasin de certificats pour importer un certificat à partir d'une instance NetScaler et l'appliquer à d'autres instances NetScaler ciblées.

Ajouter des certificats SSL au magasin de certificats

1. Accédez à **Infrastructure > Tableau de bord SSL** et sélectionnez **Gérer le magasin de certificats** dans la liste.

   

2. Cliquez sur **Ajouter**.
3. Sur la page **Ajouter un certificat**, saisissez les détails suivants :

   - **Nom de la clé de certificat** - Saisissez un nom pour le certificat. Le nom ne doit contenir que des caractères alphanumériques ASCII, des traits de soulignement et des tirets, et doit comporter moins de 30 caractères. Vous ne pouvez pas modifier le nom après la création du certificat.
   - **Fichier de certificat** - Parcourez votre lecteur local et téléchargez le fichier de certificat.
   - **Fichier de clé** - Téléchargez le fichier de clé depuis votre ordinateur local.
   - **Mot de passe** - Si vous avez une clé privée chiffrée au format PEM, saisissez la phrase secrète utilisée pour chiffrer la clé privée.
   - **Ajouter une chaîne de certificats** - Sélectionnez cette option pour ajouter le certificat dans une chaîne de certificats.
   - **Chaîne de certificats** - Parcourez votre lecteur local et téléchargez le fichier de certificat.
   - Cliquez sur **Créer**.

Mettre à jour les certificats SSL dans le magasin de certificats

1. Accédez à **Infrastructure > SSL Dashboard** et sélectionnez **Manage Certificate Store** dans la liste.
2. Sélectionnez le certificat que vous souhaitez mettre à jour et cliquez sur **Update**.
3. Sur la page **Update Certificate**, saisissez les détails suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Certkey Name** - Affiche le nom du certificat que vous avez sélectionné pour la mise à jour.
- **Certificate File** - Pour mettre à jour le fichier de certificat, chargez un fichier de certificat.
- **Key File** - Pour mettre à jour le fichier de clé, chargez un fichier de clé depuis votre ordinateur local.
- **Password** - Si vous avez une clé privée chiffrée au format PEM, saisissez la phrase secrète utilisée pour chiffrer la clé privée.
- **Add Certificate Chain** - Sélectionnez cette option pour ajouter le certificat dans une chaîne de certificats.
- **Certificate Chain** - Parcourez votre lecteur local et chargez le fichier de certificat.
- Cliquez sur **OK**.

Supprimer les certificats SSL du magasin de certificats

1. Accédez à **Infrastructure > SSL Dashboard** et sélectionnez **Manage Certificate Store** dans la liste.
2. Sélectionnez le certificat et cliquez sur **Delete**.
3. Lorsque vous y êtes invité, cliquez sur **Yes** pour supprimer le certificat.

Installer les certificats SSL sur les instances NetScaler®

1. Accédez à **Infrastructure > Tableau de bord SSL** et sélectionnez **Gérer le magasin de certificats** dans la liste.
2. Sélectionnez le certificat et cliquez sur **Installer**.
3. Sur la page **Installer le certificat SSL sur les instances NetScaler**, saisissez les détails suivants :

   a. **Source du certificat**

   - **Certificat** - Affiche le nom du certificat que vous avez sélectionné.

   b. **Détails du certificat**

   - **Nom du certificat** - Affiche le nom du certificat.
   - **Enregistrer la configuration** - Sélectionnez cette option pour enregistrer la configuration NetScaler. La configuration NetScaler est enregistrée après l'installation du certificat.

4. Cliquez sur **Sélectionner les instances** pour sélectionner les instances NetScaler sur lesquelles vous souhaitez installer vos certificats.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cliquez sur **OK**.

Importer des certificats depuis les instances NetScaler

1. Accédez à **Infrastructure > Tableau de bord SSL** et sélectionnez **Gérer le magasin de certificats** dans la liste.
2. Cliquez sur **Importer les certificats NetScaler**.
3. Sur la page **Importer les certificats NetScaler**, vous pouvez sélectionner l'un des onglets suivants :

   - **Importer les certificats NetScaler** - Cliquez sur **Démarrer l'interrogation** pour interroger tous les certificats SSL sur toutes les instances NetScaler.
   - **Sélectionner les instances** - Sélectionnez une instance NetScaler et cliquez sur **Importer les certificats NetScaler** pour interroger les certificats SSL uniquement sur l'instance NetScaler sélectionnée.

   Après l'interrogation, les certificats SSL et les fichiers de clés sont téléchargés et ajoutés au magasin de certificats.

   REMARQUE :

   L'opération d'importation échoue pour les certificats si des noms de certificats identiques existent dans le magasin. Cependant, l'opération d'importation continue d'interroger les certificats restants et ajoute les certificats NetScaler, si disponibles, au magasin.

Mettre à jour les certificats de serveur sans téléchargements intermédiaires

Vous pouvez renouveler les certificats sans la tâche répétitive de re-téléchargement des certificats intermédiaires. Cette amélioration réduit la charge de travail manuelle et minimise le risque d'erreurs de configuration.

Renouvellements sans effort

NetScaler Console préserve la chaîne de certificats existante par défaut lors d'une mise à jour. Cela garantit que votre chaîne reste intacte et valide, même lorsque vous ne téléchargez qu'un nouveau certificat de niveau serveur.

Améliorations clés

- **Complexité réduite** - Élimine les téléchargements intermédiaires obligatoires lors des mises à jour standard des certificats de serveur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **La sécurité avant tout** - La préservation automatique de la chaîne prévient la « rupture de chaîne », une cause fréquente d'erreurs de négociation SSL.

Pour mettre à jour les certificats de serveur sans téléchargements intermédiaires

1. Accédez à **Infrastructure > Tableau de bord SSL > Magasin de certificats**.
2. Sélectionnez le certificat que vous souhaitez mettre à jour et cliquez sur **Mettre à jour**.
3. **Écraser la chaîne de certificats existante** - Sélectionnez cette option si votre renouvellement nécessite des modifications de la chaîne intermédiaire :
    - **Avec un bundle** - Remplace la chaîne existante par le nouveau bundle téléchargé.
    - **Sans bundle** - Supprime entièrement la chaîne de certificats actuelle.
4. **Ajouter une chaîne de certificats** - Sélectionnez cette option pour télécharger et ajouter manuellement des certificats intermédiaires s'ils ne sont pas inclus dans votre fichier de certificat de serveur principal.

Exemples

La structure finale du certificat dépend de l'état de votre chaîne de certificats existante et des options que vous sélectionnez lors de la mise à jour.

SCÉNARIO A : LE CERTIFICAT EXISTANT N'A PAS DE CHAÎNE

ACTION DE MISE À JOUR	RÉSULTAT
Le nouveau certificat téléchargé n'inclut pas de chaîne	Le certificat de serveur est mis à jour. Aucune chaîne intermédiaire n'est ajoutée.
Le nouveau certificat téléchargé inclut une chaîne	Le certificat de serveur est mis à jour et la nouvelle chaîne intermédiaire est attachée.

SCÉNARIO B : LE CERTIFICAT EXISTANT A UNE CHAÎNE

ACTION DE MISE À JOUR	RÉSULTAT
Le nouveau certificat téléchargé inclut une chaîne (Remplacer la chaîne de certificats existante est activé)	Le certificat de serveur est mis à jour et la chaîne intermédiaire existante est remplacée par la nouvelle chaîne.
Le nouveau certificat téléchargé n'inclut pas de chaîne (Remplacer la chaîne de certificats existante est activé)	Le certificat de serveur est mis à jour et la chaîne intermédiaire existante est explicitement supprimée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gérer les certificats et chiffrements personnalisés de base de données dans un déploiement haute disponibilité

NetScaler Console vous permet de remplacer les certificats de base de données intégrés par défaut par vos propres certificats provenant d'une autorité de certification de confiance. Vous pouvez également configurer vos propres suites de chiffrement dans la base de données NetScaler Console. Cette fonctionnalité offre une plus grande flexibilité et sécurité pour vos besoins de gestion de certificats, et sécurise toutes les communications entre vos nœuds HA avec des certificats SSL de confiance.

Installer vos certificats de base de données sur NetScaler Console

Pour installer vos certificats dans une configuration HA :

1. Accédez à **Paramètres > Déploiement HA** et cliquez sur **Certificats de base de données**.
2. Cliquez sur l'onglet **Certificat installé** et cliquez sur **Installer un nouveau certificat**.
3. Dans la page **Installer le certificat de base de données sur Application Delivery Management**, téléchargez un certificat racine, un certificat de serveur et une clé de serveur. Vous pouvez effectuer l'une des opérations suivantes :
   - **Choisir un fichier > Local** pour télécharger un fichier de certificat ou de clé depuis votre machine locale.
   - **Choisir un fichier > Appliance** pour télécharger un fichier de certificat ou de clé présent sur NetScaler Console.
4. Cliquez sur **Installer**.

REMARQUE :

S'il existe plusieurs certificats de chaîne, vous devez les combiner en un seul fichier. Assurez-vous que l'ordre de concaténation est correct, avec les certificats intermédiaires en premier, suivis du certificat racine. Cet ordre est essentiel pour que la chaîne de certificats soit reconnue correctement.

Par exemple, la commande suivante ajoute le contenu de chaque fichier de certificat (intermediate_certificate1.crt, intermediate_certificate2.crt et root_certificate.crt) au fichier nommé combined_certs.crt :

```
cat intermediate_certificate1.crt >> combined_certs.crt
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
cat intermediate_certificate2.crt >> combined_certs.crt
cat root_certificate.crt >> combined_certs.crt
```

Gérer vos certificats de base de données installés

Pour afficher, télécharger et supprimer vos certificats installés :

1. Accédez à **Paramètres > Déploiement HA** et cliquez sur **Certificats de base de données**.
2. Cliquez sur l'onglet **Fichiers de certificat** et sélectionnez **Certificats racine, Certificats de serveur** ou **Clés de serveur** pour afficher les fichiers correspondants.
3. Pour télécharger un fichier sur votre machine locale, cliquez sur **Télécharger**.
4. Pour supprimer un fichier de certificat, sélectionnez le fichier et cliquez sur **Supprimer**. Dans la boîte de dialogue de confirmation qui apparaît, cliquez sur **OK**.

Configurer les suites de chiffrement de la base de données

Pour configurer les suites de chiffrement pour un déploiement HA :

1. Accédez à **Paramètres > Déploiement HA** et cliquez sur **Certificats de base de données**.
2. Cliquez sur l'onglet **Chiffrements**, puis sur **Configurer le chiffrement**.
3. Dans la page **Configurer les suites de chiffrement**, sélectionnez un ou plusieurs chiffrements dans la liste des chiffrements disponibles.
4. Cliquez sur **Configurer**. Dans la boîte de dialogue de confirmation qui apparaît, cliquez sur **Oui** pour modifier les paramètres de chiffrement.

REMARQUE :

La modification des paramètres de chiffrement redémarre les nœuds secondaires et de reprise après sinistre de NetScaler Console.

Événements

Lorsqu'une adresse IP d'une instance Citrix NetScaler est ajoutée à NetScaler Console, NetScaler Console envoie un appel NITRO et s'ajoute implicitement comme destination de trap pour que l'instance reçoive ses traps ou événements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les événements représentent des occurrences d'événements ou d'erreurs sur une instance NetScaler gérée. Par exemple, lorsqu'il y a une défaillance système ou un changement de configuration, un événement est généré et enregistré sur le serveur NetScaler Console. Les événements reçus dans NetScaler Console sont affichés sur la page Résumé des événements (**Infrastructure > Événements**), et tous les événements actifs sont affichés sur la page Messages d'événements (**Infrastructure > Événements > Messages d'événements**).

NetScaler Console vérifie également les événements générés sur les instances pour former des alarmes de différents niveaux de gravité. Ces alarmes sont ensuite affichées sous forme de messages, dont certains peuvent nécessiter une attention immédiate. Par exemple, une défaillance système peut être classée comme une gravité d'événement « Critique » et devrait être traitée immédiatement.

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent la surveillance des événements, qui peuvent être nombreux, générés dans votre infrastructure NetScaler.

Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en attribuant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez créer des filtres sont : la gravité, les instances NetScaler, la catégorie, les objets de défaillance, les commandes de configuration et les messages.

Vous pouvez également vous assurer que plusieurs notifications sont déclenchées pour un événement pendant un intervalle de temps spécifique, jusqu'à ce que l'événement soit effacé. En mesure supplémentaire, vous pouvez personnaliser votre e-mail avec une ligne d'objet et un message utilisateur spécifiques, et télécharger une pièce jointe.

Utiliser le tableau de bord des événements

En tant qu'administrateur réseau, vous pouvez afficher des détails tels que les modifications de configuration, les conditions de connexion, les pannes matérielles, les violations de seuil et les changements d'état d'entité sur vos instances NetScaler, ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements de NetScaler Console pour afficher les rapports générés pour les détails de gravité des événements critiques sur toutes vos instances NetScaler.

Pour afficher les détails sur le tableau de bord des événements :

Accédez à **Infrastructure > Événements > Rapports**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le graphique des 10 premiers appareils sur le tableau de bord affiche un rapport des 10 premières instances par le nombre d'événements générés sur celles-ci. Vous pouvez cliquer sur une instance dans le graphique pour afficher plus de détails sur la gravité de l'événement.



Vous pouvez afficher plus de détails en accédant au type d'instance NetScaler (**Infrastructure > Événements > Rapports** \> **NetScaler/ NetScaler SDX**) pour afficher les éléments suivants :

- Les 10 premiers appareils par panne matérielle
- Les 10 premiers appareils par modification de configuration
- Les 10 premiers appareils par échec d'authentification

  
- Les 10 premiers appareils par changements d'état d'entité

  
- Les 10 premiers appareils par violation de seuil

  

Définir l'âge de l'événement pour les événements

Vous pouvez définir l'option d'âge de l'événement pour spécifier l'intervalle de temps (en secondes). NetScaler Console surveille les appliances jusqu'à la durée définie et génère un événement uniquement si l'âge de l'événement dépasse la durée définie.

Remarque :

> La valeur minimale pour l'âge de l'événement est de 60 secondes. Si vous laissez le champ **Âge de l'événement** vide, la règle d'événement est appliquée immédiatement après que l'événement se soit produit.

Par exemple, imaginez que vous souhaitez gérer diverses appliances NetScaler et être averti par e-mail si l'un de vos serveurs virtuels tombe en panne pendant 60 secondes ou plus. Vous pouvez créer une règle d'événement avec les filtres nécessaires et définir l'âge de l'événement de la règle à 60 secondes. Ensuite, chaque fois qu'un serveur virtuel reste inactif pendant 60 secondes ou plus, vous recevez une notification par e-mail avec des détails tels que le nom de l'entité, le changement de statut et l'heure.

Pour définir l'âge de l'événement dans NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans NetScaler Console, accédez à **Infrastructure > Événements > Règles**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer une règle**, définissez les paramètres de la règle.
3. Spécifiez l'âge de l'événement en secondes.

   Assurez-vous de définir tous les pièges corrélés dans la section **Catégorie** et de définir également la gravité respective dans la section **Gravité** lorsque vous définissez l'âge de l'événement. Dans l'exemple précédent, sélectionnez les pièges `entityup`, `entitydown` et `entityofs`.

Planifier un filtre d'événements

Après avoir créé un filtre pour votre règle, si vous ne souhaitez pas que le serveur NetScaler Console envoie une notification chaque fois que l'événement généré satisfait aux critères du filtre, vous pouvez planifier le déclenchement du filtre uniquement à des intervalles de temps spécifiques, tels que quotidiennement, hebdomadairement ou mensuellement.

Par exemple, si vous avez planifié une activité de maintenance système pour différentes applications sur vos instances à des moments différents, les instances peuvent générer plusieurs alarmes.

Si vous avez configuré un filtre pour ces alarmes et activé les notifications par e-mail pour ces filtres, le serveur envoie un grand nombre de notifications par e-mail lorsque NetScaler Console reçoit ces traps. Si vous souhaitez que le serveur envoie ces notifications par e-mail uniquement pendant une période spécifique, vous pouvez le faire en planifiant un filtre.

Pour planifier un filtre à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Événements > Règles**.
2. Sélectionnez la règle pour laquelle vous souhaitez planifier un filtre, puis cliquez sur **Afficher la planification**.
3. Sur la page **Règle planifiée**, cliquez sur **Planifier** et spécifiez les paramètres suivants :

   - **Activer la règle** – Cochez cette case pour activer la règle d'événement planifiée.
   - **Récurrence** - Intervalle auquel planifier la règle. Sélectionnez un jour spécifique de la semaine ou une date spécifique du mois.
   - **Jours** : Sélectionnez le jour de la semaine pour exécuter la règle. Vous pouvez sélectionner plusieurs jours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Dates** : Saisissez les dates. Vous pouvez saisir plusieurs dates séparées par des virgules.
- **Intervalle de temps planifié (heures)** – Heures auxquelles planifier la règle (utilisez le format 24 heures).

4. Cliquez sur **Planifier**.



Définir des notifications par e-mail répétées pour les événements

Pour vous assurer que tous les événements critiques sont traités et qu'aucune notification par e-mail importante n'est manquée, vous pouvez choisir d'envoyer des notifications par e-mail répétées pour les règles d'événement qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances impliquant des pannes de disque et que vous souhaitez être averti jusqu'à ce que le problème soit résolu, vous pouvez choisir de recevoir des notifications par e-mail répétées concernant ces événements.

Ces notifications par e-mail sont envoyées de manière répétée, à des intervalles prédéfinis, jusqu'à ce que le destinataire accuse réception de la notification ou que la règle d'événement soit effacée.

REMARQUE

Les événements ne peuvent être effacés automatiquement que si un piège « clair » équivalent est défini et envoyé depuis votre instance NetScaler.

Pour effacer un événement manuellement, vous pouvez effectuer les opérations suivantes :

- Accédez à **Infrastructure > Événements > Résumé des événements**, choisissez une **Catégorie**, sélectionnez un événement dans la catégorie et cliquez sur **Effacer**.
- Ou, accédez à **Infrastructure > Événements > Messages d'événement**. Choisissez un type d'instance, puis sélectionnez un événement dans la grille ci-dessous et cliquez sur **Effacer**.

Pour définir des notifications par e-mail répétées depuis NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Événements > Règles**, puis cliquez sur **Ajouter** pour créer une règle.
2. Sur la page **Créer une règle**, définissez les paramètres de la règle.
3. Sous Actions de la **règle d'événement**, cliquez sur **Ajouter une action**. Ensuite, sélectionnez **Action d'envoi d'e-mail** dans la liste déroulante **Type d'action** et sélectionnez une **Liste de distribution d'e-mails**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Vous pouvez également ajouter une ligne d'objet et un message utilisateur personnalisés, et télécharger une pièce jointe à votre e-mail lorsqu'un événement entrant correspond à la règle configurée.
5. Cochez la case **Répéter la notification par e-mail jusqu'à ce que l'événement soit effacé**.



Supprimer les événements

Lorsque vous choisissez l'action d'événement **Supprimer l'action**, vous pouvez configurer une période, en minutes, pendant laquelle un événement est supprimé ou ignoré. Vous pouvez supprimer l'événement pendant un minimum d'une minute.

Remarque :

> Vous pouvez également configurer le temps de suppression à 0 minute, ce qui signifie un temps infini. Si vous ne spécifiez aucune durée, NetScaler Console considère le temps de suppression comme nul et il n'expire jamais.

Pour supprimer des événements à l'aide de NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Événements > Règles**. Cliquez sur **Ajouter**.
2. Spécifiez tous les paramètres requis pour créer une règle.
3. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** pour attribuer des actions de notification à l'événement.
4. Sur la page **Ajouter une action d'événement**, sélectionnez **Supprimer l'action** dans la liste déroulante **Type d'action** et spécifiez la période, en minutes, pendant laquelle un événement doit être supprimé.
5. Cliquez sur **OK**.



Créer des règles d'événement

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent la surveillance d'un grand nombre d'événements générés dans votre infrastructure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en attribuant des actions à ces règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez créer des filtres sont : la gravité, les instances Citrix Application Delivery Controller (NetScaler), la catégorie, les objets de défaillance, les commandes de configuration et les messages.

Vous pouvez attribuer les actions suivantes aux événements :

- **Action d'envoi d'e-mail** : Envoyer un e-mail pour les événements qui correspondent aux critères de filtre.
- **Action d'envoi de trap** : Envoyer ou transférer des traps SNMP vers une destination de trap externe
- **Action d'exécution de commande** : Exécuter une commande lorsqu'un événement entrant répond à la règle configurée.
- **Action d'exécution de tâche** : Exécuter une tâche pour les événements qui correspondent aux critères de filtre que vous avez spécifiés.
- **Action de suppression** : Supprime un événement pendant une période spécifique.
- **Envoyer des notifications Slack** : Envoyer des notifications sur le canal Slack configuré pour les événements qui correspondent aux critères de filtre.
- **Envoyer des notifications PagerDuty** : Envoyer des notifications d'événement basées sur les configurations PagerDuty pour les événements qui correspondent aux critères de filtre.
- **Envoyer des notifications ServiceNow** : Générer automatiquement des incidents ServiceNow pour un événement qui correspond aux critères de filtre.

Pour plus d'informations, consultez Ajouter des actions de règle d'événement

Vous pouvez également faire renvoyer les notifications à un intervalle spécifié jusqu'à ce qu'un événement soit effacé. Et vous pouvez personnaliser l'e-mail avec une ligne d'objet spécifique, un message utilisateur et une pièce jointe.



Par exemple, en tant qu'administrateur, vous pourriez vouloir surveiller les événements de « forte utilisation du CPU » pour des instances NetScaler spécifiques si ces événements peuvent entraîner une panne de vos instances NetScaler. Vous pouvez :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Créer une règle pour surveiller les instances et spécifier une action qui vous envoie une notification par e-mail lorsqu'un événement de la catégorie « forte utilisation du CPU » se produit.
- Planifier l'exécution de la règle à un moment précis, par exemple entre 11 h et 23 h, afin de ne pas être averti à chaque fois qu'un événement est généré.

La configuration d'une règle d'événement implique les tâches suivantes :

1. Définir la règle
2. Choisir la gravité de l'événement que la règle détecte
3. Spécifier la catégorie de l'événement
4. Spécifier les instances NetScaler auxquelles la règle s'applique
5. Sélectionner les objets de défaillance
6. Spécifier les filtres avancés
7. Spécifier les actions à entreprendre lorsque la règle détecte un événement

Étape 1 - Définir une règle d'événement

Accédez à **Infrastructure > Événements > Règles**, puis cliquez sur **Ajouter**. Si vous souhaitez activer votre règle, cochez la case **Activer la règle**.

Vous pouvez définir l'option **Ancienneté de l'événement** pour spécifier l'intervalle de temps (en secondes) après lequel NetScaler Console actualise une règle d'événement.

Remarque :

> La valeur minimale pour l'âge de l'événement est de 60 secondes. Si vous laissez le champ **Âge de l'événement** vide, la règle d'événement est appliquée immédiatement après que l'événement se soit produit.

D'après l'exemple ci-dessus, vous souhaiterez peut-être être averti par e-mail chaque fois que votre instance NetScaler rencontre un événement « utilisation élevée du processeur » pendant 60 secondes ou plus. Vous pouvez définir l'âge de l'événement à 60 secondes, de sorte que chaque fois que votre instance NetScaler rencontre un événement « utilisation élevée du processeur » pendant 60 secondes ou plus, vous recevez une notification par e-mail avec les détails de l'événement.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également filtrer les règles d'événement par **Famille d'instances** pour suivre l'instance NetScaler à partir de laquelle NetScaler Console reçoit un événement.

Si vous souhaitez inclure une expression régulière autre que la correspondance de modèle par astérisque (*), sélectionnez **Activer le filtre avancé avec correspondance d'expressions régulières**.

Étape 2 - Choisir la gravité de l'événement

Vous pouvez créer des règles d'événement qui utilisent les paramètres de gravité par défaut. La gravité spécifie la gravité actuelle des événements pour lesquels vous souhaitez ajouter la règle d'événement.

Vous pouvez définir les niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement, Clair et Information.



REMARQUE

Vous pouvez configurer la gravité pour les événements génériques et spécifiques aux événements avancés. Pour modifier la gravité des événements pour les instances NetScaler gérées sur NetScaler Console, accédez à **Infrastructure > Événements > Paramètres d'événement**. Choisissez la **Catégorie** pour laquelle vous souhaitez configurer la gravité de l'événement et cliquez sur **Configurer la gravité**. Attribuez un nouveau niveau de gravité et cliquez sur **OK**.

Étape 3 - Spécifier la catégorie d'événement

Vous pouvez spécifier la ou les catégories d'événements générés par vos instances NetScaler. Toutes les catégories sont créées sur les instances NetScaler. Ces catégories sont ensuite mappées avec NetScaler Console, qui peut être utilisée pour définir des règles d'événement. Sélectionnez la catégorie que vous souhaitez prendre en compte et déplacez-la du tableau **Disponible** vers le tableau **Configuré**.

Dans l'exemple ci-dessus, vous devez choisir « cpuUsageHigh » comme catégorie d'événement dans le tableau affiché.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 4 - Spécifier les instances NetScaler

Sélectionnez les adresses IP des instances NetScaler pour lesquelles vous souhaitez définir la règle d'événement. Dans la section **Instances**, cliquez sur **Sélectionner les instances**. Dans la page **Sélectionner les instances**, choisissez vos instances, puis cliquez sur **Sélectionner**.



Étape 5 - Sélectionner les objets de défaillance

Vous pouvez soit sélectionner un objet de défaillance dans la liste fournie, soit ajouter un objet de défaillance pour lequel un événement a été généré. Vous pouvez également spécifier une expression régulière pour ajouter des objets de défaillance. Selon l'expression régulière spécifiée, les objets de défaillance sont automatiquement ajoutés à la liste. Les objets de défaillance sont des instances d'entité ou des compteurs pour lesquels un événement a été généré.

IMPORTANT

Pour lister les objets de défaillance à l'aide d'une expression régulière, sélectionnez **Activer le filtre avancé avec correspondance Regex** à l'Étape 1.

L'objet de défaillance affecte la manière dont un événement est traité et garantit qu'il reflète le problème exact tel que notifié. Avec ce filtre, vous pouvez suivre rapidement les problèmes sur les objets de défaillance et identifier la cause d'un problème. Par exemple, si un utilisateur rencontre des problèmes de connexion, l'objet de défaillance est ici le nom d'utilisateur ou le mot de passe, tel que `nsroot`.

Cette liste peut contenir des noms de compteurs pour tous les événements liés aux seuils, des noms d'entités pour tous les événements liés aux entités, des noms de certificats pour les événements liés aux certificats, et ainsi de suite.



Étape 6 - Spécifier les filtres avancés

Vous pouvez affiner le filtrage d'une règle d'événement par :

- **Commandes de configuration** - Vous pouvez spécifier la commande de configuration complète ou spécifier une expression régulière pour filtrer les événements.

  Vous pouvez affiner le filtrage de la règle d'événement par l'état d'authentification de la commande et/ou son état d'exécution. Par exemple, pour un `NetscalerConfigChange event`, tapez `[.]*bind system global policy_name[.]*`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Messages** - Vous pouvez spécifier la description complète du message, ou spécifier une expression régulière pour filtrer les événements.Par exemple, pour un événement `NetscalerConfigChange`, tapez `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :\^([.]*10.122.132.142[.]*)`.

Étape 7 - Ajouter des actions de règle d'événement

Vous pouvez ajouter des actions de règle d'événement pour attribuer des actions de notification à un événement. Ces notifications sont envoyées ou exécutées lorsqu'un événement répond aux critères de filtre définis ci-dessus. Vous pouvez ajouter les actions d'événement suivantes :

- Action d'envoi d'e-mail
- Action d'envoi de trap
- Action d'exécution de commande
- Action d'exécution de tâche
- Action de suppression
- Envoyer des notifications Slack
- Envoyer des notifications PagerDuty
- Envoyer des notifications ServiceNow

Pour définir l'action de règle d'événement par e-mail

Lorsque vous choisissez le type d'action d'événement « Action d'envoi d'e-mail », un e-mail est déclenché lorsque les événements répondent aux critères de filtre définis. Vous devez soit créer une liste de distribution d'e-mails en fournissant les détails du serveur de messagerie ou du profil de messagerie, soit sélectionner une liste de distribution d'e-mails que vous avez précédemment créée.

En raison du grand nombre de serveurs virtuels configurés dans NetScaler Console, vous pourriez recevoir un nombre élevé d'e-mails chaque jour. Les e-mails ont une ligne d'objet par défaut qui fournit des informations sur la gravité de l'événement, la catégorie de l'événement et l'objet de l'échec. Mais la ligne d'objet ne contient aucune information sur le nom du serveur virtuel d'où proviennent ces événements. Vous avez maintenant la possibilité d'inclure des informations supplémentaires telles que le nom de l'entité affectée, le nom de l'objet de l'échec.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également ajouter une ligne d'objet personnalisée et un message utilisateur, et télécharger une pièce jointe à votre e-mail lorsqu'un événement entrant correspond à la règle configurée.

Lors de l'envoi d'e-mails pour les notifications d'événements, vous pouvez souhaiter envoyer un e-mail de test pour vérifier les paramètres configurés. Le bouton « Test » vous permet désormais d'envoyer un e-mail de test après avoir configuré un serveur de messagerie, les listes de distribution associées et d'autres paramètres. Cette fonctionnalité garantit que les paramètres fonctionnent correctement.

Vous pouvez également vous assurer que tous les événements critiques sont traités et qu'aucune notification par e-mail importante n'est manquée, en cochant la case **Répéter la notification par e-mail jusqu'à ce que l'événement soit effacé** pour envoyer des notifications par e-mail répétées pour les règles d'événement qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances impliquant des pannes de disque et que vous souhaitez être informé jusqu'à ce que le problème soit résolu, vous pouvez choisir de recevoir des notifications par e-mail répétées concernant ces événements.



Pour définir l'action de règle d'événement de trap

Lorsque vous choisissez le type d'action d'événement **Envoyer l'action de trap**, les traps SNMP sont envoyés ou transférés vers une destination de trap externe. En définissant une liste de distribution de traps (ou une destination de trap et les détails du profil de trap), les messages de trap sont envoyés à des écouteurs de traps spécifiques lorsque les événements répondent aux critères de filtre définis.

Pour définir l'action Exécuter la commande

Lorsque vous choisissez l'action d'événement **Exécuter la commande**, vous pouvez créer une commande ou un script qui peut être exécuté sur NetScaler Console pour les événements correspondant à un critère de filtre particulier.

Vous pouvez également définir les paramètres suivants pour le script **Exécuter la commande** :

Paramètre	Description
Source	Ce paramètre correspond à l'adresse IP source de l'événement reçu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Catégorie	Ce paramètre correspond au type de traps défini sous la catégorie du filtre
$entité	Ce paramètre correspond aux instances d'entité ou aux compteurs pour lesquels un événement a été généré. Il peut inclure les noms de compteurs pour tous les événements liés aux seuils, les noms d'entités pour tous les événements liés aux entités et les noms de certificats pour tous les événements liés aux certificats.
$gravité	Ce paramètre correspond à la gravité de l'événement.
$objet de défaillance	L'objet d'échec affecte la manière dont un événement est traité et garantit que l'objet d'échec reflète le problème exact tel qu'il a été notifié. Cela peut être utilisé pour identifier rapidement les problèmes et la raison de l'échec, au lieu de simplement signaler des événements bruts.

REMARQUE

Lors de l'exécution de la commande, ces paramètres sont remplacés par des valeurs réelles.

Par exemple, imaginez que vous souhaitiez définir une action d'exécution de commande lorsque le statut d'un serveur virtuel d'équilibrage de charge est **Hors service**. En tant qu'administrateur, vous pourriez envisager de fournir une solution rapide en ajoutant un autre serveur virtuel. Dans NetScaler Console, vous pouvez :

- Écrire un fichier de script (.sh).

  Voici un exemple de fichier de script (.sh) :

```
#!/bin/sh

source=$1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
failureobj=$2

payload='{"params":{"warning":"YES"},"lbvserver":
{"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"
80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog
":"ENABLED","

bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":""}}'

url="http://$source/nitro/v1/config/lbvserver"

curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/
json" -X POST -d $payload $url
```

- Enregistrez le fichier .sh dans un emplacement persistant sur l'agent NetScaler. Par exemple, `/var`.
- Indiquez l'emplacement du fichier .sh dans NetScaler Console pour l'exécuter lorsque les critères de la règle sont remplis.

Pour définir l'action **Exécuter la commande** pour la création d'un nouveau serveur virtuel :

1. Définir la règle
2. Sélectionnez la gravité de l'événement
3. Sélectionnez la catégorie d'événement **entitydown**
4. Sélectionnez l'instance sur laquelle le serveur virtuel est configuré
5. Sélectionnez ou créez un objet d'échec pour le serveur virtuel
6. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** et sélectionnez **Exécuter l'action de commande** dans la liste **Type d'action**.
7. Sous **Liste d'exécution des commandes**, cliquez sur **Ajouter**.

   La page Créer une liste de distribution de commandes s'affiche.

   a. Dans **Nom du profil**, spécifiez un nom de votre choix

   b. Dans **Exécuter la commande**, spécifiez l'emplacement de l'agent NetScaler où le script doit être exécuté. Par exemple : `/sh/var/demo.sh $source $failureobj`.

   c. Sélectionnez **Ajouter la sortie** et **Ajouter les erreurs**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous pouvez activer les options **Ajouter la sortie** et **Ajouter les erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur NetScaler Console. Si vous n'activez pas ces options, NetScaler Console ignore toutes les sorties et erreurs générées lors de l'exécution du script de commande.

d. Cliquez sur **Créer**.

8. Dans la page **Ajouter une action d'événement**, cliquez sur **OK**.



REMARQUE

Vous pouvez activer les options **Ajouter la sortie** et **Ajouter les erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lors de l’exécution d’un script de commande dans les fichiers journaux du serveur NetScaler Console. Si vous n’activez pas ces options, NetScaler Console ignore toutes les sorties et erreurs générées lors de l’exécution du script de commande.

Pour définir l'action de tâche `Execute`

En créant un profil avec des tâches de configuration, une tâche est exécutée en tant que tâche intégrée ou tâche personnalisée pour les instances NetScaler et NetScaler SDX, pour les événements et les alarmes qui correspondent aux critères de filtre que vous avez spécifiés.

1. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** et sélectionnez **Exécuter l'action de tâche** dans la liste déroulante **Type d'action**.
2. Créez un profil avec une tâche que vous souhaitez exécuter lorsque les événements répondent aux critères de filtre définis.
3. Lors de la création d'une tâche, spécifiez un nom de profil, le type d'instance, le modèle de configuration et l'action que vous souhaitez effectuer si les commandes de la tâche échouent.
4. En fonction du type d'instance sélectionné et du modèle de configuration choisi, spécifiez les valeurs de vos variables et cliquez sur **Terminer** pour créer la tâche.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour définir l'action de suppression

Lorsque vous choisissez l'action d'événement **Action de suppression**, vous pouvez configurer une période, en minutes, pendant laquelle un événement est supprimé ou ignoré. Vous pouvez supprimer l'événement pendant un minimum d'une minute.



Pour définir les notifications Slack depuis NetScaler Console

Configurez le canal Slack requis en fournissant le nom du profil et l'URL du webhook dans l'interface graphique de NetScaler Console. Les notifications d'événements sont ensuite envoyées à ce canal. Vous pouvez configurer plusieurs canaux Slack pour recevoir ces notifications.

1. Dans NetScaler Console, accédez à **Infrastructure > Événements > Règles**, puis cliquez sur **Ajouter** pour créer une règle.
2. Sur la page **Créer une règle**, définissez les paramètres de la règle tels que la gravité et la catégorie. Sélectionnez les instances ainsi que les objets de défaillance qui doivent être surveillés.
3. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action**. Ensuite, sélectionnez **Envoyer des notifications Slack** dans la liste **Type d'action** et sélectionnez **Liste de profils Slack.**
4. Vous pouvez également ajouter une liste de profils Slack en cliquant sur **Ajouter** à côté du champ **Liste de profils Slack**.
5. Saisissez les paramètres suivants pour créer une liste de profils :
    a. **Nom du profil**. Saisissez un nom pour la liste de profils à configurer sur NetScaler Console
    b. **Nom du canal**. Saisissez le nom du canal Slack auquel les notifications d'événement doivent être envoyées.
    c. **URL du webhook**. Saisissez l'URL du webhook du canal que vous avez saisi précédemment. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom du canal et toutes les notifications d'événement sont envoyées à cette URL pour être publiées sur le canal Slack désigné. Voici un exemple de webhook : `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`
6. Cliquez sur **Créer** et cliquez sur **OK** dans la fenêtre **Ajouter une action d'événement**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous pouvez également ajouter les profils Slack en accédant à **Système** \> **Notifications** \> **Profils Slack**. Cliquez sur **Ajouter** et créez le profil comme décrit dans la section précédente.

Vous pouvez afficher l'état des profils Slack que vous avez créés.

Votre règle d'événement est maintenant créée avec des filtres appropriés et des actions de règle d'événement bien définies.

Pour définir les notifications PagerDuty à partir de NetScaler Console

Vous pouvez ajouter un profil PagerDuty comme option dans NetScaler Console pour surveiller les notifications d'incident en fonction de vos configurations PagerDuty. PagerDuty vous permet de configurer des notifications par e-mail, SMS, notification push et appel téléphonique sur un numéro enregistré.

Avant d'ajouter un profil PagerDuty dans NetScaler Console, assurez-vous d'avoir effectué les configurations requises dans PagerDuty. Pour plus d'informations, consultez la documentation PagerDuty.

Vous pouvez sélectionner votre profil PagerDuty comme l'une des options pour recevoir des notifications pour les fonctionnalités suivantes :

- **Événements** – Liste des événements générés pour les instances NetScaler.
- **Licences** – Liste des licences actuellement actives, sur le point d'expirer, etc.
- **Certificats SSL** – Liste des certificats SSL ajoutés aux instances NetScaler.

Pour ajouter un profil PagerDuty dans NetScaler Console :

1. Connectez-vous à NetScaler Console à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Paramètres > Notifications > Profils PagerDuty**.
3. Cliquez sur **Ajouter** pour créer un nouveau profil.
4. Dans la page Créer un profil PagerDuty :
    a. Indiquez un nom de profil de votre choix.
    b. Saisissez la **clé d'intégration**.

        Vous pouvez obtenir la clé d'intégration depuis votre portail PagerDuty.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Cliquez sur **Créer**.

Cas d'utilisation :

Considérez un scénario dans lequel vous :

- voulez envoyer des notifications à votre profil PagerDuty.
- avez configuré l'appel téléphonique comme option dans PagerDuty pour recevoir des notifications.
- voulez recevoir des alertes par appel téléphonique pour les événements NetScaler.

Pour configurer :

a. Accédez à **Événements** > **Règles**

b. Sur la page **Créer une règle**, configurez tous les autres paramètres pour créer une règle.

c. Sous **Actions de création de règle**, cliquez sur **Ajouter une action**.

La page **Ajouter une action d'événement** s'affiche.

i. Sous **Type d'action**, sélectionnez **Envoyer des notifications PagerDuty**.

ii. Sélectionnez votre profil PagerDuty et cliquez sur **OK**.

Une fois la configuration terminée, chaque fois qu'un nouvel événement est généré pour l'instance NetScaler, vous recevrez un appel téléphonique. À partir de cet appel, vous pouvez décider de :

- Accuser réception de l'événement
- Le marquer comme résolu
- Escalader à un autre membre de l'équipe

Pour générer automatiquement des incidents ServiceNow à partir de NetScaler Console

Vous pouvez générer automatiquement des incidents ServiceNow pour les événements NetScaler Console en sélectionnant le profil ServiceNow sur l'interface graphique de NetScaler Console. Vous devez choisir le profil ServiceNow dans NetScaler Console pour configurer une règle d'événement.

Avant de configurer une règle d'événement pour générer automatiquement des incidents ServiceNow, intégrez NetScaler Console à une instance ServiceNow. Pour plus d'informations, consultez Configurer l'adaptateur ITSM pour ServiceNow.

Pour configurer une règle d'événement, accédez à **Événements** > **Règles**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Sur la page **Créer une règle**, configurez tous les autres paramètres pour créer une règle.
2. Sous **Créer des actions de règle**, cliquez sur **Ajouter une action**.

   La page **Ajouter une action d'événement** s'affiche.

   a. Dans **Type d'action**, sélectionnez **Envoyer des notifications ServiceNow**.
   b. Dans **Profil ServiceNow**, sélectionnez le profil **Citrix_Workspace_SN** dans la liste.
   c. Cliquez sur **OK**.

Modifier la gravité signalée des événements qui se produisent sur les instances NetScaler

Vous pouvez gérer le signalement des événements générés sur tous vos appareils, afin de pouvoir afficher les détails d'un événement particulier sur une instance particulière et consulter des rapports basés sur la gravité des événements. Vous pouvez créer des règles d'événement qui utilisent les paramètres de gravité par défaut, et vous pouvez modifier ces paramètres de gravité. Vous pouvez configurer la gravité pour les événements génériques et spécifiques à l'entreprise.

Vous pouvez définir les niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement et Clair.

Pour modifier la gravité d'un événement :

1. Accédez à **Infrastructure > Événements > Paramètres d'événement**.
2. Cliquez sur l'onglet correspondant au type d'instance NetScaler que vous souhaitez modifier. Ensuite, sélectionnez la catégorie dans la liste et cliquez sur **Configurer la gravité**.
3. Dans **Configurer la gravité de l'événement**, sélectionnez le niveau de gravité dans la liste déroulante.
4. Cliquez sur **OK**.

Afficher le résumé des événements

Vous pouvez maintenant afficher une page de résumé des événements pour surveiller les événements et les traps reçus sur votre serveur NetScaler Console. Accédez à **Infrastructure > Événements**. La page de résumé des événements affiche les informations suivantes sous forme de tableau :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Résumé de tous les événements reçus par NetScaler Console**. Les événements sont classés par catégorie, et les différentes gravités sont affichées dans différentes colonnes : Critique, Majeur, Mineur, Avertissement, Clair et Information. Par exemple, un événement Critique se produirait lorsqu'une instance NetScaler tombe en panne et cesse d'envoyer des informations au serveur NetScaler Console. Pendant l'événement, une notification est envoyée à un administrateur, expliquant la raison pour laquelle l'instance est en panne, la durée pendant laquelle elle a été en panne, et ainsi de suite. L'événement est ensuite enregistré sur la page de résumé des événements, sur laquelle vous pouvez afficher un résumé et accéder aux détails de l'événement.

  

- **Nombre de traps reçus pour chaque catégorie**. Le nombre de traps reçus, classés par gravité. Par défaut, chaque trap envoyé des instances NetScaler à NetScaler Console a une gravité attribuée, mais en tant qu'administrateur réseau, vous pouvez spécifier sa gravité dans l'interface graphique de NetScaler Console.

Si vous cliquez sur un type de catégorie ou un trap, vous êtes redirigé vers la page **Événements**, sur laquelle des filtres tels que la Catégorie et la Gravité sont présélectionnés. Cette page affiche plus d'informations sur l'événement, telles que l'adresse IP et le nom d'hôte de l'instance NetScaler, la date de réception du trap, la catégorie, les objets de défaillance, la commande de configuration exécutée et la notification de message.



Afficher les messages d'événement

Tous les événements actifs reçus dans NetScaler® Console sont affichés sur la page **Infrastructure > Événements > Messages d'événement**.

Sur la page **Messages d'événement**, vous pouvez afficher la liste des instances et les détails des événements, tels que la gravité, la catégorie, la date de l'événement et l'objet de l'échec.

Vous pouvez filtrer les événements en fonction de l'heure à laquelle ils se sont produits, par exemple, au cours des 30 dernières minutes, 1 heure, 1 jour. Vous pouvez également sélectionner une heure personnalisée en fonction de vos préférences.

NetScaler Console prend en charge les traps SNMP personnalisés, qui sont étiquetés comme **personnalisés** sous **Messages d'événement**. L'étiquette **personnalisé** vous aide à les distinguer des alertes SNMP par défaut.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les niveaux de gravité des événements et les détails des traps SNMP

Lorsque vous créez un événement et ses paramètres dans NetScaler Console, vous pouvez le consulter immédiatement sur la page Résumé des événements. De même, vous pouvez afficher et surveiller en détail l'état de santé, la disponibilité, les modèles et les versions de toutes les instances Citrix NetScaler ajoutées à votre serveur NetScaler Console sur le tableau de bord de l'infrastructure.

Sur le tableau de bord de l'infrastructure, vous pouvez désormais masquer les valeurs non pertinentes afin de visualiser et de surveiller plus facilement des informations telles que les événements par gravité, l'état de santé, la disponibilité, les modèles et la version des instances NetScaler en détail.

Par exemple, les événements de niveau de gravité **Critique** peuvent être rares. Cependant, lorsque ces événements critiques se produisent sur votre réseau, vous pouvez souhaiter approfondir l'enquête, dépanner et surveiller où et quand l'événement s'est produit. Si vous sélectionnez tous les niveaux de gravité sauf Critique, le graphique n'affiche que les occurrences d'événements critiques. De plus, en cliquant sur le graphique, vous êtes redirigé vers la page **Événements basés sur la gravité**, où vous pouvez voir tous les détails concernant le moment où un événement critique s'est produit pour la durée que vous avez sélectionnée : la source de l'instance, la date, la catégorie et la notification de message envoyée lorsque l'événement critique s'est produit.

De même, vous pouvez afficher l'état de santé d'une instance NetScaler VPX sur le tableau de bord. Vous pouvez masquer la période pendant laquelle l'instance était opérationnelle et n'afficher que les périodes où l'instance était hors service. En cliquant sur le graphique, vous êtes redirigé vers la page de cette instance, où le filtre *hors service* est déjà appliqué, et vous pouvez voir des détails tels que le nom d'hôte, le nombre de requêtes HTTP reçues par seconde, l'utilisation du CPU, etc. Vous pouvez également sélectionner l'instance et consulter le tableau de bord de l'instance Citrix spécifique pour plus de détails.

Pour sélectionner des événements spécifiques par gravité dans NetScaler Console :

1. Connectez-vous à NetScaler Console à l'aide de vos identifiants d'administrateur.
2. Accédez à **Infrastructure > Tableau de bord**.

   Ou,

   Accédez à **Infrastructure > Événements > Rapports**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Dans le menu situé dans le coin supérieur droit de la page, sélectionnez la durée pour laquelle vous souhaitez afficher les événements par gravité.



4. Le graphique en anneau **Événements par gravité** affiche une représentation visuelle de tous les événements par leur gravité. Différents types d'événements sont représentés par des sections de couleurs différentes, et la longueur de chaque section correspond au nombre total d'événements de ce type de gravité.
5. Vous pouvez cliquer sur chaque section du graphique en anneau pour afficher la page correspondante **Événements basés sur la gravité**, qui présente les détails suivants pour la gravité sélectionnée et la durée sélectionnée :

   - Source de l'instance
   - Données de l'événement
   - Catégorie des événements générés par l'instance NetScaler
   - Notification de message envoyée

   REMARQUE

   Sous le graphique en anneau, vous pouvez voir une liste des gravités représentées dans le graphique. Par défaut, un graphique en anneau affiche tous les événements de tous les types de gravité, et par conséquent, tous les types de gravité de la liste sont mis en surbrillance. Vous pouvez basculer les types de gravité pour afficher et surveiller plus facilement la gravité choisie.



Pour afficher les détails des traps SNMP NetScaler sur NetScaler Console :

Vous pouvez désormais afficher les détails de chaque trap SNMP reçu de ses instances NetScaler gérées sur le serveur NetScaler Console, sur la page **Paramètres d'événement**. Accédez à **Infrastructure > Événements > Paramètres d'événement**. Pour un trap spécifique reçu de votre instance, vous pouvez afficher les détails suivants sous forme de tableau :

- **Catégorie** - Spécifie la catégorie de l'instance à laquelle l'événement appartient.
- **Gravité** - La gravité de l'événement est indiquée par des couleurs et son type de gravité.
- **Description** - Spécifie les messages associés à l'événement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Par exemple, pour un événement avec la catégorie de trap **monRespTimeoutBelowThresh**, la description du trap s'affiche comme suit : « Ce trap est envoyé lorsque le délai d'expiration de la réponse pour une sonde de moniteur redevient normal, inférieur au seuil défini. »

Afficher et exporter les messages syslog NetScaler

Depuis votre NetScaler Console, vous pouvez surveiller les événements syslog générés sur vos instances Citrix NetScaler. Pour cela, vous devez configurer NetScaler Console comme serveur syslog pour vos instances NetScaler. Une fois NetScaler Console configurée, tous les messages syslog sont redirigés des instances NetScaler vers NetScaler Console.

Configurer NetScaler Console comme serveur syslog

Suivez ces étapes pour configurer NetScaler Console comme serveur syslog :

1. Depuis l'interface graphique de NetScaler Console, accédez à **Infrastructure > Instances**.
2. Sélectionnez l'instance NetScaler à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans NetScaler Console.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Syslog**.
4. Cliquez sur **Activer**.
5. Dans la liste déroulante **Fonctionnalité**, sélectionnez une fonctionnalité locale ou de niveau utilisateur.
6. Sélectionnez le niveau de journalisation requis pour les messages syslog.
7. Cliquez sur **OK**.

Ces étapes configurent toutes les commandes syslog dans l'instance NetScaler, et NetScaler Console commence à recevoir les messages syslog.

Afficher et rechercher les messages syslog

Vous pouvez afficher tous vos messages syslog générés sur vos instances NetScaler gérées. Les messages syslog sont stockés de manière centralisée dans la base de données et sont disponibles sous **Infrastructure > Événements > Messages Syslog** à des fins d'audit. Vous pouvez combiner ces informations de journalisation et en déduire des rapports pour l'analyse à partir des données collectées.

De plus, vous pouvez utiliser des filtres pour affiner les résultats de recherche des messages syslog et trouver exactement ce que vous cherchez en temps réel. Cliquez sur **Besoin d'aide ?** pour ouvrir l'aide à la recherche intégrée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.




Ensuite, ajoutez le terme de recherche. Pour certaines catégories, une liste préremplie de termes de recherche s'affiche. Par défaut, la durée de recherche est de 1 jour. Vous pouvez modifier la plage horaire et la date en cliquant sur la flèche vers le bas. Vous pouvez affiner davantage votre recherche en sélectionnant des options dans le volet **Résumé Syslog**.



Exporter et planifier les messages syslog

Vous pouvez afficher les messages syslog sans vous connecter à NetScaler Console, en planifiant une exportation de tous les messages syslog reçus sur le serveur. Vous pouvez exporter les messages syslog générés sur vos instances NetScaler aux formats PDF, CSV, PNG et JPEG. Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail ou un compte Slack spécifiés à divers intervalles.

Pour exporter et planifier les messages de journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.



- Pour exporter les messages de journal, cliquez sur **Exporter les rapports > Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.
- Pour planifier l'exportation des messages syslog, cliquez sur **Exporter les rapports > Planifier le rapport**, et définissez les paramètres requis. Vous pouvez recevoir le rapport par e-mail ou Slack.



Supprimer les messages syslog

Lorsqu'elle est configurée en tant que serveur syslog, NetScaler Console reçoit tous les messages syslog qui lui sont envoyés par les instances NetScaler configurées. Il peut y avoir un grand nombre de messages que vous ne souhaitez pas voir. Par exemple, vous pourriez ne pas être intéressé par tous les messages de niveau informationnel. Vous pouvez désormais ignorer certains messages syslog qui ne vous intéressent pas. Vous pouvez supprimer certains des messages syslog arrivant dans NetScaler Console en configurant des filtres. NetScaler Console supprime tous les messages qui correspondent aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique de NetScaler Console et ne sont pas non plus stockés dans la base de données NetScaler Console du client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez supprimer certains des messages syslog enregistrés arrivant dans NetScaler Console en configurant des filtres. Les deux filtres qui peuvent être utilisés pour supprimer les messages syslog sont la gravité et la facilité. Vous pouvez également supprimer les messages provenant d'une instance NetScaler particulière ou de plusieurs instances. Vous pouvez également fournir un modèle de texte pour que NetScaler Console recherche et supprime les messages. NetScaler Console supprime tous les messages qui correspondent aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique de NetScaler Console et ne sont pas non plus stockés dans la base de données client. Par conséquent, une bonne quantité d'espace est économisée sur le serveur de stockage.

Voici quelques cas d'utilisation pour la suppression des messages syslog :

- Si vous souhaitez ignorer tous les messages de niveau information, supprimez le niveau 6 (informationnel)
- Si vous souhaitez uniquement enregistrer les conditions d'erreur du pare-feu, supprimez tous les niveaux autres que le niveau 3 (erreurs)

Suppression des messages syslog en créant des filtres

1. Dans NetScaler Console, accédez à **Infrastructure > Événements > Messages Syslog** \> **Filtre de suppression**.
2. Sur la page **Créer un filtre de suppression**, mettez à jour les informations suivantes :

   a. **Nom** - saisissez un nom pour le filtre.

   REMARQUE

   Si différents utilisateurs ont des accès différents à plusieurs instances NetScaler, des filtres différents doivent être créés pour différentes instances, car les utilisateurs ne peuvent voir que les filtres pour lesquels ils ont accès à toutes les instances.

   b. **Gravité** - Sélectionnez et ajoutez les niveaux de journalisation pour lesquels vous devez supprimer les messages. Par exemple, si vous ne souhaitez pas afficher les messages d'information entrants, vous pouvez sélectionner Informationnel pour supprimer ces messages.

   c. **Instances** - Sélectionnez les instances NetScaler sur lesquelles les messages syslog ont été configurés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. **Fonctionnalités** - Sélectionnez la fonctionnalité pour supprimer les messages en fonction de la source qui les génère.

e. **Modèle de message** - Vous pouvez également saisir un modèle de texte entouré d'astérisques (*) pour supprimer les messages. Les messages sont recherchés en fonction de la chaîne du modèle de texte, et ceux qui contiennent ce modèle sont supprimés.



Désactivation du filtre

Pour permettre l'affichage des messages sur NetScaler Console, vous devez désactiver le filtre.

1. Accédez à **Infrastructure > Événements > Messages Syslog** \> **Filtre de suppression**, et sur la page **Filtre de suppression**, sélectionnez le filtre et cliquez sur **Modifier**.
2. Sur la page **Configurer le filtre de suppression**, décochez la case **Activer le filtre** pour désactiver le filtre.

Configurer les paramètres de purge pour les événements d'instance

Les instances Citrix NetScaler gérées par votre serveur NetScaler Console envoient en continu des données de messages d'événement à stocker sur NetScaler Console. Vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapports réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont purgées toutes les 24 heures (à 00h00).

REMARQUE

La valeur que vous pouvez spécifier ne peut pas dépasser 40 jours ni être inférieure à 1 jour.

Pour configurer les paramètres de purge pour les événements d'instance :

1. Accédez à **Système** \> **Administration système**.
2. Sous **Paramètres de purge**, cliquez sur **Instance Paramètres de purge des événements**.
3. Entrez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler Console, puis cliquez sur **OK**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fonctions réseau

Grâce à la fonctionnalité Fonctions réseau, vous pouvez surveiller l'état des entités configurées sur vos instances Citrix NetScaler gérées. Vous pouvez afficher des statistiques telles que les détails des transactions, les détails des connexions et le débit d'un serveur virtuel d'équilibrage de charge. Vous pouvez également activer ou désactiver les entités lorsque vous planifiez une maintenance.

Le tableau de bord Fonctions réseau vous fournit les graphiques suivants :

- Les 5 principaux serveurs virtuels avec le plus grand nombre de connexions client
- Les 5 principaux serveurs virtuels avec le plus grand nombre de connexions serveur
- Les 5 principaux serveurs virtuels avec le débit maximal (Mo/s)
- Les 5 serveurs virtuels avec le débit le plus faible (Mo/s)
- Les 5 principales instances avec le plus grand nombre de serveurs virtuels
- État des serveurs virtuels
- État de santé des serveurs virtuels d'équilibrage de charge
- Protocoles

Générer des rapports pour les entités d'équilibrage de charge

NetScaler Console vous permet de consulter les rapports des entités d'instance Citrix NetScaler à tous les niveaux. Il existe deux types de rapports que vous pouvez télécharger dans NetScaler Console \> Fonctions réseau - rapports consolidés et rapports individuels.

Rapports consolidés : Vous pouvez télécharger et consulter un rapport consolidé ou un rapport récapitulatif pour toutes les entités gérées sur les instances NetScaler.

Ce rapport vous permet d'avoir une vue d'ensemble de la correspondance entre les instances NetScaler, les partitions et les entités d'équilibrage de charge correspondantes (serveurs virtuels, groupes de services et services) qui sont présentes dans le réseau.

L'image suivante montre un exemple de rapport récapitulatif.



Le rapport consolidé est au format CSV. Les entrées de chaque colonne sont décrites comme suit :

- **Adresse IP NetScaler** : L'adresse IP de l'instance NetScaler est affichée dans le rapport
- **Nom d'hôte NetScaler®** : Le nom d'hôte est affiché dans le rapport.
- **Partition** : L'adresse IP de la partition administrative est affichée

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Serveur virtuel** : \<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **Services** : \<name_of_the_service\>#service-IP_address:port_number
- **Groupes de services** : \<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

REMARQUE

- S'il n'y a pas de nom d'hôte disponible, l'adresse IP correspondante est affichée.
- Les colonnes vides indiquent que les entités respectives ne sont pas configurées pour cette instance NetScaler.

Rapports individuels : Vous pouvez également télécharger et afficher des rapports indépendants de toutes les instances et entités. Par exemple, vous pouvez télécharger un rapport pour uniquement les serveurs virtuels d'équilibrage de charge, les services d'équilibrage de charge ou les groupes de services d'équilibrage de charge.

NetScaler Console vous permet de télécharger le rapport instantanément. Vous pouvez également planifier la génération du rapport à une heure fixe, une fois par jour, une fois par semaine ou une fois par mois.

Générer un rapport d'équilibrage de charge combiné

1. Dans NetScaler Console, accédez à **Infrasturcture > Fonctions réseau > Équilibrage de charge.**
2. Sur la page **Équilibrage de charge**, cliquez sur
   
   .
3. Sur la page **Exporter** qui s'ouvre, vous avez deux options pour afficher le rapport :

   a. Sélectionnez l'onglet **Exporter maintenant** et cliquez sur **OK**.

   Le rapport consolidé est téléchargé sur votre système.

   b. Sélectionnez l'onglet **Planifier le rapport** pour planifier la génération et l'exportation du rapport à intervalles réguliers. Spécifiez les paramètres de récurrence de la génération du rapport et créez un profil de messagerie vers lequel le rapport est exporté.

      i. **Récurrence** - sélectionnez **Quotidien**, **Hebdomadaire** ou **Mensuel** dans la liste déroulante.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ii. **Heure de récurrence** - Saisissez l'heure au format Heure:Minute (format 24 heures).

iii. **Profil de messagerie** - Sélectionnez un profil dans la liste déroulante, ou cliquez sur **+** pour créer un profil de messagerie.

REMARQUE

Si vous sélectionnez une récurrence **Hebdomadaire**, assurez-vous de sélectionner les jours de la semaine où vous souhaitez que le rapport soit planifié.

REMARQUE

Si vous sélectionnez la récurrence **Mensuelle**, assurez-vous de saisir tous les jours où vous souhaitez que le rapport soit planifié, séparés par des virgules.

Générer un rapport d'entité d'équilibrage de charge individuel

Vous pouvez générer et exporter un rapport individuel pour un type particulier d'entité associé aux instances. Par exemple, considérez un scénario où vous souhaitez voir une liste de tous les services d'équilibrage de charge dans le réseau.

1. Dans NetScaler Console, accédez à **Infrasturcture > Network Funtions > Load Balancing > Services.**
2. Sur la page **Services**, cliquez sur le bouton **Exporter** dans le coin supérieur droit.
   a. Sélectionnez l'onglet **Exporter maintenant** si vous souhaitez générer et afficher le rapport à cet instant.
   b. Sélectionnez **Planifier l'exportation** pour planifier la génération et l'exportation du rapport à intervalles réguliers.

REMARQUE

Vous pouvez uniquement télécharger les rapports ou les exporter en tant que pièces jointes. Vous ne pouvez pas afficher les rapports sur l'interface graphique de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exporter ou planifier l'exportation des rapports de fonctions réseau

Vous pouvez générer un rapport complet pour les fonctions réseau sélectionnées telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, l'équilibrage de charge global des serveurs (GSLB), l'authentification et NetScaler Gateway dans NetScaler Console. Ce rapport vous permet d'avoir une vue d'ensemble de la correspondance entre les instances NetScaler, les partitions et les entités liées correspondantes (serveurs virtuels, groupes de services et services) présentes dans le réseau. Vous pouvez exporter ces rapports au format de fichier .csv.

Le rapport affiche les données de serveur virtuel suivantes :

- Adresse IP NetScaler®
- Nom d'hôte
- Données de partition
- Nom du serveur virtuel
- Type de serveur virtuel
- Serveur virtuel
- Serveur virtuel LB cible

REMARQUE

Pour les serveurs virtuels de commutation de contenu et de redirection de cache, la colonne Serveur virtuel LB cible répertorie tous les serveurs LB, c'est-à-dire les serveurs par défaut et les serveurs basés sur des stratégies.

- Nom du service
- Nom du groupe de services

Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à différents intervalles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Pour les serveurs virtuels GSLB, le rapport des fonctions réseau affiche uniquement les serveurs virtuels GSLB et les services associés.
- Pour les serveurs virtuels de commutation de contenu et de redirection de cache, le rapport affiche uniquement les liaisons aux serveurs LB associés.
- Les serveurs virtuels SSL ne sont pas répertoriés dans ce rapport car une liste distincte de serveurs virtuels SSL n'est pas gérée sur NetScaler Console.
- Lorsqu'un nouveau rapport est généré, les rapports plus anciens sont automatiquement purgés de votre compte.
- Vous ne pouvez pas générer de rapport de fonctions réseau pour HAProxy.

Pour exporter et planifier des rapports de fonctions réseau :

1. Accédez à **Infrastructure > Fonctions réseau**.
2. Sur la page **Fonctions réseau**, dans le volet de droite, cliquez sur **Générer un rapport** dans le coin supérieur droit de la page.
3. Sur la page **Générer un rapport**, vous disposez des 2 options suivantes :

   a. Sélectionnez l'onglet **Exporter maintenant** et cliquez sur **OK**. Le rapport est téléchargé sur votre système.

   L'image suivante montre un exemple de rapport de fonctions réseau.

   

   b. Sélectionnez l'onglet **Planifier un rapport** pour planifier la génération et l'exportation du rapport à intervalles réguliers. Spécifiez les paramètres de récurrence de génération du rapport et créez un profil de messagerie vers lequel le rapport est exporté.

      i. **Récurrence** - sélectionnez **Quotidien**, **Hebdomadaire** ou **Mensuel** dans la liste déroulante.

      ii. **Heure de récurrence** - Saisissez l'heure au format 24 heures (Heure:Minute).

      iii. **Profil de messagerie** - Sélectionnez un profil dans la liste déroulante ou cliquez sur **+** pour créer un profil de messagerie.

Cliquez sur **Activer la planification** pour planifier votre rapport, puis cliquez sur **OK**. En cochant la case **Activer la planification**, vous pouvez générer les rapports sélectionnés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rapports réseau

Vous pouvez optimiser l'utilisation des ressources en surveillant vos rapports réseau sur NetScaler Application Delivery Management (NetScaler Console). Vous pouvez avoir un déploiement distribué avec de nombreuses applications déployées à plusieurs emplacements. Pour garantir des performances optimales de vos applications, vous avez également déployé plusieurs instances Citrix Application Delivery Controller (NetScaler) pour équilibrer la charge, commuter le contenu ou compresser le trafic. Les performances réseau peuvent avoir un impact sur les performances des applications. Pour continuer à maintenir les performances de vos applications, vous devez surveiller régulièrement les performances de votre réseau et vous assurer que toutes les ressources sont utilisées de manière optimale.

NetScaler Console vous permet désormais de générer des rapports non seulement pour les instances au niveau global, mais aussi pour des entités telles que les serveurs virtuels et les interfaces réseau. La famille d'instances comprend les instances NetScaler. Les serveurs virtuels pour lesquels vous pouvez générer des rapports sont les suivants :

- Serveurs, services et groupes de services d'équilibrage de charge
- Serveurs de commutation de contenu
- Serveurs de redirection de cache
- Équilibrage de charge de service global (GSLB)
- Authentification
- NetScaler Gateway

Le tableau de bord de rapports réseau dans NetScaler Console est hautement personnalisable. Vous pouvez désormais créer plusieurs tableaux de bord pour diverses instances, serveurs virtuels et autres entités.

Tableau de bord des rapports réseau

L'image suivante met en évidence les différentes fonctionnalités du tableau de bord :



- Le panneau latéral gauche répertorie tous les tableaux de bord personnalisés créés dans NetScaler Console. Vous pouvez cliquer sur l'un d'eux pour afficher les différents rapports qui composent le tableau de bord. Par exemple, un tableau de bord TCP et SSL contient divers rapports liés aux protocoles TCP et SSL.
- Vous pouvez personnaliser chaque tableau de bord avec plusieurs widgets pour afficher divers rapports. Un widget représente un rapport sur le tableau de bord, c'est-à-dire une collection de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rapports plus liés. Par exemple, un rapport d'utilisation des octets TCP de compression contient des rapports sur les octets TCP compressés transférés et reçus par seconde.

- Vous pouvez afficher des rapports pour une heure, un jour, une semaine ou un mois. De plus, vous pouvez désormais utiliser l'option de curseur de chronologie pour personnaliser la durée des rapports générés sur la console NetScaler.
- Vous pouvez supprimer un rapport en cliquant sur « X ». Vous pouvez également exporter le rapport au format .pdf, .jpeg, .png ou .csv vers votre système. Vous pouvez également planifier l'heure et la récurrence de la génération du rapport. Vous pouvez également configurer une liste de distribution de courrier électronique à laquelle les rapports doivent être envoyés.
- La section Instances en haut du tableau de bord répertorie les adresses IP de toutes les instances pour lesquelles le rapport est généré.
- Vous pouvez soit supprimer des instances en cliquant sur « X », soit ajouter d'autres instances aux rapports. Mais, actuellement, NetScaler Console vous permet d'afficher des rapports pour 10 instances.
- Vous pouvez également exporter l'intégralité du tableau de bord au format .pdf, .jpeg, .png ou .csv vers votre système. Toutes les modifications apportées au tableau de bord doivent être enregistrées. Cliquez sur Enregistrer pour enregistrer les modifications.

La section suivante explique en détail les tâches de création d'un tableau de bord, de génération de rapports et d'exportation de rapports.

Pour afficher ou créer un tableau de bord :

1. Dans NetScaler Console, accédez à **Infrastructure > Rapports réseau**.

   

2. Pour afficher les tableaux de bord existants, cliquez sur **Afficher le tableau de bord**. La page **Tableau de bord** des rapports réseau s'ouvre, où vous pouvez afficher tous vos tableaux de bord et widgets de rapport.
3. Pour créer un tableau de bord, cliquez sur **Nouveau tableau de bord**. La page Créer un tableau de bord s'ouvre.

   

4. Dans l'onglet Paramètres de base, saisissez les détails suivants :

   a. **Nom**. Saisissez le nom du tableau de bord.

   b. **Famille d'instances**. Sélectionnez le type d'instance - NetScaler ou NetScaler SDX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **Type**. Sélectionnez le type d'entité pour lequel vous souhaitez générer des rapports. Dans cet exemple, sélectionnez les serveurs virtuels d'équilibrage de charge.

d. **Description**. Saisissez une description significative pour le tableau de bord.

5. Cliquez sur **Suivant**. Tous les rapports pris en charge pour l'instance et l'entité spécifique apparaissent.
6. Dans l'onglet **Sélectionner les rapports**, sélectionnez les rapports requis. Dans cet exemple, vous pouvez sélectionner les transactions, les connexions et le débit. Cliquez sur **Suivant**.

Sélectionner les rapports réseau(/en-us/netscaler-application-delivery-management-software/media/nw-dash-rprt.png)

1. Dans l'onglet **Sélectionner les entités**, cliquez sur **Ajouter**.

   Une fenêtre apparaît avec la liste des entités en fonction du type d'entité sélectionné dans l'onglet **Paramètres de base**. Dans cet exemple, la fenêtre **Choisir les serveurs virtuels LB** apparaît.
2. Sélectionnez les entités que vous souhaitez surveiller.

   Sélectionner les entités réseau(/en-us/netscaler-application-delivery-management-software/media/nw-dash-entities.png)
3. Cliquez sur **Créer**.

Le tableau de bord est créé et affiche tous les rapports que vous avez sélectionnés.

REMARQUE

Actuellement, les modifications apportées aux légendes ou aux filtres ne peuvent pas être enregistrées.

Exportation des rapports réseau

Bien que vous puissiez exporter les rapports de widgets aux formats .pdf, .png, .jpeg ou .csv, vous ne pouvez exporter les tableaux de bord entiers qu'aux formats .pdf, .jpeg ou .png.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous ne pouvez pas exporter de rapports dans NetScaler Console si vous disposez de permissions en lecture seule. Vous avez besoin d'une permission de modification pour pouvoir créer un fichier dans NetScaler Console et pour pouvoir exporter le fichier.

Pour exporter les rapports de tableau de bord :

1. Accédez à **Infrastructure > Network Reporting**
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez sur **Tableau de bord 1**.
4. Cliquez sur le bouton d'exportation en haut à droite de la page.
5. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.

   Sur la page **Exporter**, vous pouvez effectuer l'une des opérations suivantes :
6. Sélectionnez l'onglet **Exporter maintenant**. Pour afficher et enregistrer le rapport au format PDF, JPEG, PNG ou CSV.
7. Sélectionnez l'onglet **Planifier l'exportation**. Pour planifier le rapport quotidiennement, hebdomadairement ou mensuellement et l'envoyer par e-mail ou message Slack.

   Vous pouvez planifier l'exportation de la page du tableau de bord **Network Reporting** de manière récurrente. Par exemple, vous pouvez définir une option pour générer un rapport de tableau de bord chaque semaine pour l'heure précédente à un moment précis. Le rapport est ensuite généré chaque semaine et affiche l'état du tableau de bord. Le rapport remplace l'horodatage, s'il est défini par l'utilisateur.

REMARQUE

- si vous sélectionnez une récurrence hebdomadaire, assurez-vous de sélectionner les jours de la semaine où vous souhaitez que le rapport soit planifié.
- Si vous sélectionnez une récurrence mensuelle, assurez-vous de saisir tous les jours où vous souhaitez que le rapport soit planifié, séparés par des virgules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lors de la planification des rapports réseau, vous pouvez personnaliser l'en-tête du rapport en saisissant une chaîne de texte dans le champ **Objet**. Le rapport créé à l'heure planifiée portera cette chaîne comme nom.

Par exemple, pour les rapports réseau provenant d'un serveur virtuel particulier, vous pouvez taper l'objet comme "authentication-reports-10.106.118.120", où 10.106.118.120 est l'adresse IP du serveur virtuel surveillé.

REMARQUE

Actuellement, cette option n'est disponible que lorsque vous planifiez l'exportation des rapports. Vous ne pouvez pas ajouter d'en-tête au rapport lorsque vous l'exportez instantanément.

Afficher les données de rapport réseau en appliquant des agrégations

Vous pouvez appliquer des agrégations aux données de performance réseau et afficher les performances des applications sur le tableau de bord. Vous pouvez également exporter les résultats en fonction de vos besoins. En utilisant ces agrégations appliquées aux données, vous pouvez analyser et vous assurer que toutes les ressources sont utilisées de manière optimale. Accédez à **Réseau > Rapports réseau** et sélectionnez une durée d'un jour ou plus pour obtenir l'option **Afficher par**.

Dans les données moyennes existantes, vous pouvez appliquer des agrégations en sélectionnant l'option dans la liste **Afficher par**. Lorsque vous appliquez une agrégation, les données sont mises à jour pour chaque métrique du tableau de bord. Cliquez sur **Paramètres** et sélectionnez **Filtres d'agrégation**.



Voici les agrégations que vous pouvez ajouter :

- Nombre
- Max
- Min
- Somme
- Écart type
- Variance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Mode
- Médiane
- 25e centile
- 75e centile
- 95e centile
- 99e centile
- Premier
- Dernier

Vous pouvez ajouter jusqu'à 4 options d'agrégation au tableau de bord. Après avoir ajouté les options d'agrégation, NetScaler Console prend environ 1 heure pour générer des rapports pour les options d'agrégation sélectionnées.

Pour exporter les rapports de widget :

1. Accédez à **Infrastructure > Rapports réseau**.
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez également sur **Skype for Business**.
4. Sélectionnez un widget. Par exemple, sélectionnez **Transactions de serveur virtuel d'équilibrage de charge**.
5. Cliquez sur le bouton d'exportation en haut à droite de la page
6. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.



Comment gérer les seuils pour les rapports réseau sur NetScaler Console

Pour surveiller l'état d'une instance NetScaler, vous pouvez définir des seuils sur les compteurs et recevoir des notifications lorsqu'un seuil est dépassé. Sur NetScaler Console, vous pouvez configurer des seuils, les afficher, les modifier et les supprimer.

Par exemple, vous pouvez recevoir une notification par e-mail lorsque le compteur de connexions pour un serveur virtuel de commutation de contenu atteint une valeur spécifiée. Vous pouvez

© 1997–2026 Citrix Systems, Inc. All rights reserved.

définir un seuil pour un type d'instance spécifique. Vous pouvez également choisir les rapports que vous souhaitez générer pour des métriques de compteur spécifiques à partir de l'instance choisie.

Lorsque la valeur d'un compteur dépasse ou tombe en dessous (tel que spécifié par la règle) de la valeur de seuil, un événement de la gravité spécifiée est généré pour signaler un problème lié aux performances. Lorsque la valeur du compteur revient à une valeur que vous considérez normale, l'événement est effacé. Ces événements peuvent être consultés en accédant à **Infrastructure > Événements > Rapports**. Sur la page Rapports, vous pouvez cliquer sur le graphique en anneau **Événements par gravité** pour afficher les événements par leur gravité.

Vous pouvez également associer une action à un seuil, telle que l'envoi d'un e-mail ou d'un message SMS, lorsque le seuil est dépassé.

Pour créer un seuil :

1. Dans NetScaler Console, accédez à **Infrastructure > Rapports réseau > Seuils**. Sous **Seuils**, cliquez sur **Ajouter**.
2. Sur la page **Créer un seuil**, spécifiez les détails suivants :
   - **Nom**. Nom du seuil.
   - **Type d'instance**. Choisissez NetScaler.
   - **Nom du rapport**. Nom du rapport de performances qui fournit des informations sur ce seuil.
3. Vous pouvez également définir des règles pour spécifier quand un événement doit être généré ou effacé. Vous pouvez spécifier les détails suivants dans la section **Configurer la règle** :
   - **Métrique**. Sélectionnez la métrique pour laquelle vous souhaitez définir un seuil.
   - **Comparateur**. Sélectionnez un comparateur pour vérifier si la valeur surveillée est supérieure ou égale, ou inférieure ou égale à la valeur de seuil.
   - **Valeur de seuil**. Saisissez la valeur pour laquelle la gravité de l'événement est calculée. Par exemple, vous pouvez générer un événement avec une gravité critique si la valeur surveillée pour les Connexions client actuelles atteint 80 pour cent. Dans ce cas, saisissez 80 comme valeur de seuil. Vous pouvez afficher les événements de « gravité critique » en accédant à **Infrastructure > Événements > Rapports**. Sur la page Rapports, vous pouvez cliquer sur le graphique en anneau **Événements par gravité** pour afficher les événements par leur gravité.
   - **Valeur de réinitialisation**. Saisissez la valeur qui indique quand réinitialiser la valeur. Par exemple, vous pouvez vouloir réinitialiser le seuil des Connexions client actuelles lorsque la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

valeur surveillée atteint 50 pour cent. Dans ce cas, saisissez 50 comme valeur de réinitialisation.

- **Gravité de l'événement**. Sélectionnez le niveau de sécurité que vous souhaitez définir pour la valeur de seuil.

4. Vous pouvez choisir les instances et les entités à définir avec la valeur de seuil. Dans la section **Instances**, choisissez l'une des options suivantes :

   - **Toutes les instances**. Le seuil est défini pour toutes les instances.
   - **Instances spécifiques**. Le seuil est défini pour des instances spécifiques. Utilisez la flèche droite pour déplacer les instances de la liste **Disponible** vers la liste **Configurée**. Le seuil est défini pour les instances de la liste **Configurée**.
   - **Entités spécifiques**. Le seuil est défini pour des entités spécifiques.

     Cliquez sur **Ajouter** pour sélectionner les entités.

     Une fenêtre apparaît avec la liste des entités en fonction du type de rapport sélectionné dans le champ **Nom du rapport**. Dans cet exemple, la fenêtre **Choisir les serveurs virtuels LB** apparaît.

     

     Sélectionnez les entités pour lesquelles vous souhaitez définir un seuil. Cliquez sur **Sélectionner**. Les entités sélectionnées apparaissent dans la section **Instances**.

     REMARQUE

     L'option **Entités spécifiques** apparaît uniquement si vous sélectionnez des rapports basés sur les serveurs virtuels dans **Nom du rapport**. Par exemple, si vous sélectionnez **Statistiques de service LB**

5. Vous pouvez également ajouter un **Message d'événement**. Saisissez un message que vous souhaitez voir apparaître lorsque le seuil est atteint. NetScaler Console ajoute la valeur surveillée et la valeur de seuil à ce message.
6. Sélectionnez **Activer** pour activer le seuil afin de générer des alertes.
7. En option, vous pouvez configurer des **Actions** telles que des notifications par e-mail ou Slack, ou les deux.
8. Cliquez sur **Créer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Définir l'intervalle d'interrogation des performances pour les rapports réseau

Par défaut, toutes les 5 minutes, les appels NITRO collectent des données de performance pour les rapports réseau. NetScaler Console récupère les statistiques d'instance, telles que les informations de compteur, et les agrège par minute, par heure, par jour ou par semaine. Vous pouvez consulter ces données agrégées dans des rapports prédéfinis.

Pour définir l'intervalle d'interrogation des performances, accédez à **Infrastructure > Rapports réseau** et cliquez sur **Configurer l'intervalle d'interrogation**. Votre intervalle d'interrogation ne peut pas être inférieur à 5 minutes ni supérieur à 60 minutes.



Configuration des paramètres d'élagage des rapports réseau

Vous pouvez configurer l'intervalle de purge des données de rapports réseau dans NetScaler Console. Ce paramètre limite la quantité de données de rapports réseau stockées dans la base de données du serveur NetScaler Console. Par défaut, l'élagage des données historiques des rapports réseau a lieu toutes les 24 heures (à 01h00).

REMARQUE

La valeur que vous pouvez spécifier ne peut pas dépasser 30 jours ni être inférieure à 1 jour.

Tâches de configuration

Le processus de gestion de la configuration de NetScaler Application Delivery Management (NetScaler Console) assure la réplication correcte des modifications de configuration, des mises à niveau du système et d'autres activités de maintenance sur plusieurs instances Citrix NetScaler du réseau.

NetScaler Console vous permet de créer des tâches de configuration qui vous aident à effectuer toutes ces activités facilement sur plusieurs appareils en une seule tâche. Les tâches et les modèles de configuration simplifient les tâches administratives les plus répétitives en une seule tâche sur NetScaler Console. Une tâche de configuration contient un ensemble de commandes de configuration que vous pouvez exécuter sur un ou plusieurs appareils gérés.

Les tâches de configuration peuvent utiliser des commandes SSH pour exécuter des commandes de configuration ou utiliser SCP pour copier des fichiers localement ou vers un autre appareil. Par exemple, nous pouvons planifier un basculement HA ou une mise à niveau HA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Bien que vous puissiez sélectionner n'importe quel nombre d'instances NetScaler pour la mise à niveau, NetScaler Console sur site prend en charge un maximum de 40 threads de mise à niveau simultanés. Cela signifie que seules 40 instances peuvent être mises à niveau simultanément.

Vous pouvez créer une tâche de configuration en utilisant l'une des quatre options suivantes dans NetScaler Console. Utilisez l'une d'entre elles pour créer une source réutilisable de commandes et d'instructions pour le système afin d'exécuter une tâche de configuration.

1. Modèle de configuration
2. Instance
3. Fichier
4. Enregistrer et lire

Modèle de configuration

Vous pouvez créer des modèles de configuration lors de la création d'une tâche et enregistrer un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page Créer des tâches, ils sont automatiquement affichés sur la page Créer un modèle.

Remarque L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Cependant, vous pouvez renommer les modèles de configuration personnalisés.

Vous pouvez utiliser l'un des modèles suivants :

Éditeur de configuration : Vous pouvez utiliser l'éditeur de configuration pour saisir des commandes CLI, enregistrer la configuration en tant que modèle et l'utiliser pour configurer des tâches.

Modèle intégré : Vous pouvez choisir parmi une liste de modèles de configuration. Ces modèles fournissent les syntaxes des commandes CLI et vous permettent de spécifier des valeurs pour les variables. Les modèles intégrés sont répertoriés, avec leurs descriptions dans le tableau ci-dessous. Vous pouvez planifier une tâche en utilisant l'option de modèle intégré. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégré pour planifier une

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tâche de configuration de serveurs syslog. Vous pouvez également choisir d'exécuter la tâche immédiatement ou de la planifier pour une exécution ultérieure.

Instance

Vous pouvez effectuer une mise à niveau à bundle unique de vos instances NetScaler SDX exécutant NetScaler version 11.0 et ultérieure. Pour effectuer une mise à niveau à bundle unique, vous utilisez une tâche intégrée dans NetScaler Console. Vous pouvez également mettre à niveau une instance NetScaler en extrayant la configuration en cours d'exécution ou une configuration enregistrée et en exécutant les commandes sur une autre instance NetScaler du même type. Cela vous permet de répliquer la configuration d'une instance sur l'autre.

Fichier

Vous pouvez télécharger un fichier de configuration depuis votre machine locale et créer des tâches.

Avantages de l'utilisation d'un fichier

- Vous pouvez utiliser n'importe quel fichier texte pour créer une source réutilisable de commandes de configuration.
- Aucun formatage n'est requis.
- Le fichier peut être enregistré sur votre machine locale.

Vous pouvez soit créer et enregistrer un nouveau fichier, soit importer un fichier existant, et exécuter les commandes.

Enregistrer et lire

En utilisant Créer une tâche, vous pouvez soit saisir vos propres commandes CLI, soit utiliser le bouton d'enregistrement et de lecture pour obtenir des commandes à partir d'une session NetScaler. Lorsque vous exécutez la tâche, les modifications apportées au fichier ns.conf sur l'instance sélectionnée sont enregistrées et copiées dans NetScaler Console.

Articles connexes

- Comment utiliser la commande SCP (put) dans les tâches de configuration
- Comment utiliser les variables dans les tâches de configuration
- Comment créer des tâches de configuration à partir de commandes correctives
- Comment utiliser les modèles de configuration pour créer des modèles d'audit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Comment utiliser l'enregistrement et la lecture pour créer des tâches de configuration
- Comment utiliser le modèle de configuration principal sur NetScaler Console

Créer une tâche de configuration

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une ou plusieurs instances gérées. Vous pouvez créer des tâches pour apporter des modifications de configuration à travers les instances, répliquer les configurations sur plusieurs instances sur votre réseau, et enregistrer et rejouer les tâches de configuration à l'aide de l'interface graphique de NetScaler Console et les convertir en commandes CLI.

Vous pouvez utiliser la fonctionnalité Tâches de configuration de NetScaler Console pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

Pour créer une tâche de configuration sur NetScaler Console :

1. Accédez à **Infrastructure > Configuration > Tâches de configuration**.
2. Cliquez sur **Créer une tâche**.
3. Sur la page **Créer une tâche**, sous l'onglet **Sélectionner la configuration**, spécifiez le nom de la tâche et sélectionnez le **Type d'instance** dans la liste.
4. Dans la liste **Source de configuration**, sélectionnez le modèle de tâche de configuration que vous souhaitez créer. Ajoutez les commandes pour le modèle sélectionné.

    - Vous pouvez soit saisir les commandes, soit importer les commandes existantes à partir des modèles de configuration enregistrés.
    - Vous pouvez également ajouter plusieurs modèles de différents types dans l'éditeur de configuration lors de la création d'une tâche dans les Tâches de configuration.
    - Dans la liste **Source de configuration**, sélectionnez les différents modèles, puis faites glisser les modèles dans l'éditeur de configuration. Les types de modèles peuvent être **Modèle de configuration**, **Modèle intégré**, **Configuration principale**, **Enregistrer et rejouer**, **Instance** et **Fichier**.

REMARQUE

Si vous ajoutez le modèle `Deploy Master Configuration Job` pour la première fois, ajoutez un modèle de type différent, alors l'ensemble du modèle de tâche devient de type `Master Configuration`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également réorganiser et réordonner les commandes dans l'éditeur de configuration. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser et déposer la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en modifiant simplement le numéro de ligne de commande dans la zone de texte. Vous pouvez également réorganiser et réordonner la ligne de commande lors de la modification de la tâche de configuration.

Vous pouvez définir des variables qui vous permettent d'attribuer différentes valeurs à ces paramètres ou d'exécuter une tâche sur plusieurs instances. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'une tâche de configuration dans une vue consolidée unique. Cliquez sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définies lors de la création ou de la modification d'une tâche de configuration.

Vous pouvez personnaliser les commandes de restauration pour chaque commande dans l'éditeur de configuration. Pour spécifier vos commandes personnalisées, activez l'option de restauration personnalisée.

IMPORTANT

Pour que la restauration personnalisée prenne effet, complétez l'assistant **Créer une tâche**. Et dans l'onglet **Exécuter**, sélectionnez l'option **Restaurer les commandes réussies** dans la liste **En cas d'échec de la commande**.

5. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration.

   a. Dans une paire haute disponibilité NetScaler, vous pouvez exécuter une tâche de configuration locale sur un nœud principal ou secondaire. Sélectionnez le nœud sur lequel vous souhaitez exécuter la tâche.

      - **Exécuter sur les nœuds principaux** - Sélectionnez cette option pour exécuter la tâche uniquement sur les nœuds principaux.
      - **Exécuter sur les nœuds secondaires** - Sélectionnez cette option pour exécuter la tâche uniquement sur les nœuds secondaires.

      Vous pouvez également choisir les nœuds principal et secondaire pour exécuter la même tâche de configuration. Si vous ne sélectionnez ni le nœud principal ni le nœud secondaire, la tâche de configuration s'exécute automatiquement sur le nœud principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Dans l'onglet **Spécifier les valeurs des variables**, vous avez deux options :

    a. Téléchargez le fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur NetScaler Console.

    b. Saisissez des valeurs communes pour les variables que vous avez définies pour toutes les instances

    c. Cliquez sur **Suivant**.

Pour envoyer une notification par e-mail et Slack pour une tâche :

Une notification par e-mail et Slack est désormais envoyée chaque fois qu'une tâche est exécutée ou planifiée. La notification comprend des détails tels que le succès ou l'échec de la tâche, ainsi que les informations pertinentes.

1. Accédez à **Infrastructure > Configuration > Tâches de configuration**.
2. Sélectionnez la tâche pour laquelle vous souhaitez activer la notification par e-mail et Slack, puis cliquez sur **Modifier**.
3. Dans l'onglet **Exécuter**, accédez au volet **Recevoir le rapport d'exécution via** :

    - Cochez la case **E-mail** et choisissez la liste de distribution d'e-mails à laquelle vous souhaitez envoyer le rapport d'exécution.

      Si vous souhaitez ajouter une liste de distribution d'e-mails, cliquez sur **Ajouter** et spécifiez les détails du serveur de messagerie.
    - Cochez la case **Slack** et choisissez le canal Slack auquel vous souhaitez envoyer le rapport d'exécution.

      Si vous souhaitez ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **Nom du profil**, le **Nom du canal** et le **Jeton** du canal Slack requis.

      Profil Slack(/en-us/netscaler-application-delivery-management-software/media/configjobemail-slack-added.png)

4. Cliquez sur **Terminer**.

Pour envoyer une notification par e-mail et Slack pour une tâche :

Une notification par e-mail et Slack est désormais envoyée chaque fois qu'une tâche est exécutée ou planifiée. La notification comprend des détails tels que la réussite ou l'échec de la tâche, ainsi que les informations pertinentes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Infrastructure > Configuration > Tâches de configuration**.
2. Sélectionnez la tâche pour laquelle vous souhaitez activer la notification par e-mail et Slack, puis cliquez sur **Modifier**.
3. Dans l'onglet **Exécuter**, accédez au volet **Recevoir le rapport d'exécution via** :
   - Cochez la case **E-mail** et choisissez la liste de distribution d'e-mails à laquelle vous souhaitez envoyer le rapport d'exécution.

     Si vous souhaitez ajouter une liste de distribution d'e-mails, cliquez sur **Ajouter** et spécifiez les détails du serveur de messagerie.
   - Cochez la case **Slack** et choisissez le canal Slack vers lequel vous souhaitez envoyer le rapport d'exécution.

     Si vous souhaitez ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **Nom du profil**, le **Nom du canal** et le **Jeton** du canal Slack requis.
4. Cliquez sur **Terminer**.

Pour afficher les détails du résumé d'exécution :

1. Accédez à **Infrastructure > Configuration > Tâches de configuration**.
2. Sélectionnez la tâche dont vous souhaitez afficher le résumé d'exécution et cliquez sur **Détails**.
3. Cliquez sur **Résumé d'exécution** pour voir :
   - L'état de l'instance sur laquelle la tâche est exécutée
   - Les commandes exécutées sur la tâche
   - L'heure de début et de fin de la tâche, et
   - Le nom de l'utilisateur de l'instance

Utiliser l'enregistrement et la lecture pour créer des tâches de configuration

Si vous êtes habitué à utiliser l'interface graphique NetScaler pour configurer une instance NetScaler, il peut parfois être difficile de se souvenir des commandes CLI exactes pour créer une tâche de configuration et l'exécuter sur plusieurs instances NetScaler.

NetScaler Console vous permet d'enregistrer les tâches de configuration effectuées à l'aide de l'interface graphique d'une instance NetScaler et de les convertir en commandes CLI. Vous pouvez ensuite créer une tâche de configuration à partir de ces commandes CLI et l'exécuter sur plusieurs instances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour enregistrer la configuration de l'interface graphique et la convertir en tâche de configuration

1. Accédez à **Infrastructure > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Spécifiez le nom de la tâche et le type d'instance.
3. Dans la liste **Source de configuration**, sélectionnez **Enregistrer et lire**, puis sélectionnez l'instance source à partir de laquelle vous souhaitez enregistrer la configuration. Cliquez sur **Enregistrer**.

   
4. L'**interface graphique NetScaler** s'ouvre. Configurez les fonctionnalités et les paramètres que vous souhaitez inclure dans la tâche de configuration. Ensuite, fermez la fenêtre de l'interface graphique NetScaler et cliquez sur **Arrêter** dans l'**Éditeur de configuration**. Les commandes apparaissent sous forme de lien dans le volet gauche. Faites glisser les commandes vers le volet droit, puis cliquez sur **Suivant**.

   Vous pouvez ensuite réorganiser et réordonner les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser et déposer la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en modifiant simplement le numéro de ligne de commande dans la zone de texte.
5. Vous pouvez examiner toutes les variables que vous avez définies lors de la création ou de la modification d'une tâche de configuration dans une vue consolidée unique.
6. Effectuez l'une des opérations suivantes pour afficher toutes les variables dans une vue consolidée unique :

   - Lors de la création d'une tâche de configuration, accédez à **Infrastructure > Tâches de configuration**, sélectionnez **Créer une tâche**. Sur la page **Créer une tâche**, vous pouvez examiner toutes les variables que vous avez ajoutées lors de la création de la tâche de configuration.
   - Lors de la modification d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, sélectionnez le Nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez examiner toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définies lors de la création ou de la modification d'une tâche de configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables tels que le nom, le nom d'affichage, le type et la valeur par défaut dans un format tabulaire. Vous pouvez également modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.

   

9. Cliquez sur **Ajouter des instances** et sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche de configuration. Cliquez sur **OK**, puis sur **Suivant**.

   

10. Si vous avez spécifié des variables dans les commandes, sous l'onglet **Spécifier les valeurs des variables**, sélectionnez l'une des options suivantes pour spécifier les variables de vos instances :

    - **Télécharger le fichier d'entrée pour les valeurs des variables :** Cliquez sur **Télécharger le fichier de clé d'entrée** pour télécharger un fichier d'entrée. Dans le fichier d'entrée, saisissez les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur NetScaler Console.
    - **Valeurs de variables communes pour toutes les instances** : Saisissez les valeurs des variables. Les variables varient en fonction du modèle sélectionné.

    Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et téléchargés précédemment lors de la création ou de la modification des tâches de configuration.

    Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, puis cliquez sur **Créer une tâche**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

    Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nom de fichier).10. Sous l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11. Sous l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
12. Sous l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de la planifier pour une exécution ultérieure. Vous pouvez également choisir l'action que NetScaler Console doit entreprendre si la commande échoue.

    Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées, et vous pouvez choisir d'envoyer ou non une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.

    
13. Sur la page **Tâches**, vous pouvez ensuite afficher la progression de l'exécution de votre tâche de configuration sur toutes les instances.

Utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances

Vous pouvez utiliser la fonctionnalité Tâches de configuration de NetScaler Console pour extraire une configuration particulière d'une instance NetScaler et la répliquer sur plusieurs instances.

Par exemple, vous avez peut-être configuré à la fois l'équilibrage de charge et l'optimisation front-end (FEO) sur une instance NetScaler pour votre déploiement. Cependant, vous souhaitez maintenant répliquer uniquement la configuration FEO sur d'autres instances NetScaler.

Pour récupérer et répliquer la configuration d'une instance vers d'autres instances NetScaler :

1. Accédez à **Infrastructure > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Spécifiez le nom de la tâche et le type d'instance.
3. Sélectionnez **Instance** comme **Source de configuration** et sélectionnez l'instance source dont vous souhaitez répliquer la configuration. Sélectionnez le type de configuration que vous souhaitez extraire. Si vous sélectionnez « Configuration par durée », définissez la période pendant laquelle vous avez exécuté cette configuration, puis cliquez sur **Extraire**.

   Le nombre de commandes exécutées sur cette instance pendant la durée que vous avez sélectionnée s'affiche à l'écran, comme mis en évidence dans l'image suivante.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Faites glisser les commandes vers le champ **Commandes** dans le volet de droite.

   

   Conservez uniquement les commandes liées à FEO et supprimez manuellement les commandes liées à l'équilibrage de charge, ou les commandes liées à toute autre configuration, puis cliquez sur **Suivant**.
5. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer la configuration FEO. Cliquez sur **OK**, puis cliquez sur **Suivant**.
6. Si vous avez spécifié des variables dans les commandes, sous l'onglet Spécifier les valeurs des variables, cliquez sur **Télécharger le fichier de clé d'entrée**. Dans le fichier téléchargé, spécifiez les valeurs des variables, puis téléchargez le fichier vers NetScaler Console.
7. Sous l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
8. Dans l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter la tâche sur les instances NetScaler sélectionnées.

Utiliser des variables dans les tâches de configuration

Une tâche de configuration est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Lorsque vous exécutez la même configuration sur plusieurs instances, vous pouvez souhaiter utiliser des valeurs différentes pour les paramètres utilisés dans votre configuration. Vous pouvez définir des variables qui vous permettent d'attribuer des valeurs différentes à ces paramètres ou d'exécuter une tâche sur plusieurs instances.

Par exemple, considérons une configuration d'équilibrage de charge de base où vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel. Maintenant, vous pourriez vouloir avoir la même configuration sur deux instances mais avec des valeurs différentes pour les noms et adresses IP du serveur virtuel et des services. Vous pouvez utiliser la fonctionnalité des tâches de configuration pour y parvenir en utilisant des variables pour définir les noms et adresses IP du serveur virtuel et des services.

Dans cet exemple, les commandes et variables suivantes sont utilisées :

```
add lb vserver <servername> HTTP <ipaddress> <portnumber>
```

```
add service <servicename1> <ipaddress1> HTTP 80
```

```
add service <servicename2> <ipaddress2> HTTP 80
```

```
bind lb vserver <servername> <servicename1>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind lb vserver <servername> <servicename2>
```

Pour créer une tâche de configuration en définissant des variables dans NetScaler Console :

1. Accédez à **Infrastructure > Tâches de configuration**.
2. Cliquez sur **Créer une tâche**.
3. Sur la page **Créer une tâche**, sélectionnez les paramètres de tâche personnalisés tels que le nom de la tâche, le type d'instance et le type de configuration.
4. Dans l'éditeur de configuration, saisissez les commandes pour ajouter un serveur virtuel d'équilibrage de charge, deux services, et lier les services au serveur virtuel. Double-cliquez pour sélectionner les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge `*ipaddress*`, et cliquez sur **Convertir en variable**.
5. Une fois que vous voyez des signes dollar encadrer la valeur de la variable, cliquez sur la variable pour spécifier davantage les détails de la variable tels que le nom, le nom d'affichage et le type. Vous pouvez également cliquer sur l'option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable. Cliquez sur **Enregistrer**, puis sur **Suivant**.

   Saisissez le reste de vos commandes et définissez toutes les variables.
6. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'une tâche de configuration dans une vue consolidée unique.
7. Effectuez l'une des opérations suivantes pour afficher toutes les variables dans une vue consolidée unique :

   - Lors de la création d'une tâche de configuration, accédez à **Infrastructure > Tâches de configuration**, sélectionnez **Créer une tâche**. Sur la page **Créer une tâche**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création de la tâche de configuration.
   - Lors de la modification d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
8. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définies lors de la création ou de la modification d'une tâche de configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables tels que le nom, le nom d'affichage, le type et la valeur par défaut dans un format tabulaire. Vous pouvez également modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.

   

10. Vous pouvez ensuite réorganiser et réordonner les commandes dans l'éditeur de configuration, le cas échéant. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser et déposer la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en modifiant simplement le numéro de ligne de commande dans la zone de texte.
11. Sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche de configuration.
12. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Télécharger le fichier d'entrée pour les valeurs des variables**, puis cliquez sur **Télécharger le fichier de clés d'entrée**. Dans notre exemple, vous devrez spécifier le nom du serveur sur chaque instance, les adresses IP du serveur et des services, les numéros de port et les noms des services. Enregistrez le fichier et téléchargez-le. Si vos valeurs ne sont pas définies avec précision, le système peut générer une erreur.
13. Le fichier de clés d'entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs des variables pour chaque instance NetScaler que vous avez sélectionnée précédemment, puis cliquez sur **Télécharger** pour télécharger le fichier de clés d'entrée vers NetScaler Console. Cliquez sur **Suivant**. Le fichier de clés d'entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs des variables pour chaque instance NetScaler que vous avez sélectionnée précédemment.

REMARQUE

Dans le fichier de clés d'entrée, les variables sont définies à trois niveaux :

- Niveau global
- Niveau groupe d'instances
- Niveau de l'instance

Les variables globales sont des valeurs de variable qui sont appliquées à toutes les instances. Les valeurs de variable au niveau du groupe d'instances sont appliquées à toutes les instances

© 1997–2026 Citrix Systems, Inc. All rights reserved.

définies dans un groupe. Les valeurs de variable au niveau de l'instance sont appliquées uniquement à une instance spécifique.

NetScaler Console donne la priorité aux valeurs au niveau de l'instance. S'il n'y a pas de valeurs fournies aux variables pour les instances individuelles, NetScaler Console utilise la valeur fournie au niveau du groupe. S'il n'y a pas de valeurs fournies au niveau du groupe, NetScaler Console utilise la valeur de variable fournie au niveau global. Si vous fournissez une entrée pour une variable aux trois niveaux, NetScaler Console utilise la valeur au niveau de l'instance comme valeur par défaut.

14. Cliquez sur **Télécharger** pour télécharger le fichier de clé d'entrée vers NetScaler Console. Cliquez sur **Suivant**.

    IMPORTANT

    Lorsque vous téléchargez un fichier CSV depuis un Mac, le Mac stocke le fichier CSV avec des points-virgules au lieu de virgules. Cela entraînera l'échec de la configuration lorsque vous téléchargerez le fichier d'entrée et exécuterez la tâche. Si vous utilisez un Mac, utilisez un éditeur de texte pour apporter les modifications nécessaires, puis téléchargez le fichier.

15. Vous pouvez également attribuer des valeurs de variable communes à toutes les instances et cliquer sur **Télécharger** pour télécharger le fichier de clé d'entrée vers NetScaler Console.

    Les fichiers de clé d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et téléchargés précédemment lors de la création ou de la modification des tâches de configuration.

    Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, puis cliquez sur **Créer une tâche**. Sur la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs de variable communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

    Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs de variable communes pour toutes les**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

instances pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

16. Sous l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
17. Sous l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de la planifier pour une exécution ultérieure. Vous pouvez également choisir l'action que NetScaler Console doit entreprendre en cas d'échec de la commande et si vous souhaitez envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.

Après avoir configuré et exécuté vos tâches, vous pouvez consulter les détails de la tâche en accédant à **Infrastructure > Tâches de configuration** et en sélectionnant la tâche que vous venez de configurer. Cliquez sur **Détails**, puis sur **Détails des variables** pour afficher la liste des variables ajoutées à votre tâche.

REMARQUE

Les valeurs que vous avez fournies pour les variables à l'**ÉTAPE 5** sont conservées par NetScaler Console lorsque vous enregistrez la tâche et quittez, ou lorsque vous planifiez l'exécution d'une tâche ultérieurement.

Créer des tâches de configuration à partir de commandes correctives

Vous pouvez utiliser la fonctionnalité de modèle d'audit dans NetScaler Console pour surveiller les modifications de configuration sur les instances NetScaler gérées et résoudre les erreurs de configuration.

Le flux de travail typique pour l'audit des modifications de configuration à l'aide de modèles d'audit comprend les étapes suivantes

1. Créez un modèle d'audit avec un ensemble de commandes NetScaler valides/attendues pour l'audit des configurations d'instance.
2. Sélectionnez les instances NetScaler sur lesquelles vous souhaitez exécuter le modèle d'audit pour vérifier les différences entre la configuration en cours d'exécution et les configurations attendues.
3. Comprenez les commandes différentielles/correctives et utilisez la fonctionnalité « Créer une tâche » pour amener les configurations de l'instance à l'état souhaité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Considérez un scénario où plusieurs administrateurs gèrent cinq instances NetScaler. Tous ces administrateurs mettent à jour la configuration d'instance existante chaque fois que des modifications sont nécessaires. Le super administrateur veut s'assurer qu'un certain ensemble de configurations importantes reste inchangé, quelles que soient les modifications apportées par les autres administrateurs. Pour ce cas d'utilisation, le super administrateur crée un modèle de la configuration qui est censée être présente sur les instances NetScaler et l'exécute sur les instances. NetScaler Console compare la configuration du modèle d'audit avec la configuration en cours d'exécution et signale toute non-concordance sur le tableau de bord **Audit de configuration**.

Si vous remarquez une modification dans la configuration de certaines instances, vous pouvez utiliser la fonctionnalité de commandes correctives de NetScaler Console pour créer une tâche de configuration avec les commandes de configuration modifiées et corrigées pour des instances NetScaler spécifiques.

S'il existe une différence entre la configuration du modèle d'audit et la configuration en cours d'exécution, un message d'état **Différence existante** apparaît sur la page **Rapport d'audit**. Cliquer sur le lien **Différence existante** vous amène à la page **Différence de configuration**, où vous pouvez afficher la commande corrective. Vous pouvez également utiliser ces commandes correctives pour créer une tâche de configuration et l'exécuter sur les instances NetScaler spécifiques afin de les ramener à la configuration souhaitée.

Pour créer une tâche de configuration à partir de commandes correctives sur NetScaler Console

1. Accédez à **Infrastructure > Audit de configuration**.
2. Sur la page **Audit de configuration**, cliquez à l'intérieur de l'un des deux graphiques en anneau pour accéder à la page **Rapports d'audit**.
3. Cliquez sur le lien **Différence existante** (sous la colonne **Différence enregistrée vs en cours d'exécution** dans le tableau) pour l'instance pour laquelle vous souhaitez corriger les commandes de configuration. La page **Différence de configuration** apparaît, listant les différences entre la configuration enregistrée, la configuration en cours d'exécution et la configuration de correction pour cette instance.

   
4. Cliquez sur **Créer une tâche** pour accéder à la page **Créer une tâche**, sur laquelle les commandes correctives sont pré-remplies. Pour savoir comment créer une tâche de configuration, consultez Comment créer une tâche de configuration sur NetScaler Console.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Répliquer la configuration en cours d'exécution et enregistrée d'une instance NetScaler à une autre

May 24, 2018

Vous pouvez désormais répliquer la configuration d'une instance NetScaler sur d'autres instances. Lorsque vous configurez une tâche dans NetScaler Console, sélectionnez une instance comme source de configuration et choisissez la configuration en cours d'exécution ou enregistrée de l'instance sélectionnée.

Par exemple, lorsque vous sélectionnez **Configuration en cours d'exécution** et cliquez sur **Extraire**, NetScaler Console envoie une requête à l'instance NetScaler sélectionnée pour localiser la configuration en cours d'exécution, et l'affiche sous forme de modèle. Vous pouvez faire glisser le modèle dans le champ **Commandes** du volet droit. Vous pouvez modifier les commandes, les paramètres et les instances.

Pour répliquer les commandes de configuration en cours d'exécution et enregistrées d'une instance vers une autre instance sur NetScaler Console :

1. Accédez à **Infrastructure > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Spécifiez le nom de la tâche et le type d'instance. Par exemple, spécifiez *NetScaler Running Config1* comme nom de votre tâche et *NetScaler* comme type d'instance.
3. Sélectionnez **Instance** comme **Source de configuration**, puis sélectionnez l'instance source dont vous souhaitez répliquer la configuration sur d'autres instances.
4. Vous voyez les trois options suivantes :
    - Configuration en cours d'exécution
    - Configuration enregistrée
    - Configuration par durée
5. Choisissez **Configuration en cours d'exécution**, puis cliquez sur **Extraire**. Le nombre de commandes de configuration en cours d'exécution sur cette instance s'affiche.

    
6. Faites glisser les commandes dans le champ **Commandes** du volet droit.
7. Vous pouvez modifier les commandes dans le champ Commandes. Par exemple, si les commandes extraites sont destinées à configurer une instance NetScaler. Cela peut inclure l'ajout de partitions, la configuration de l'équilibrage de charge, la liaison du serveur d'équilibrage de charge aux services, et ainsi de suite. Vous pourriez vouloir modifier vos

© 1997–2026 Citrix Systems, Inc. All rights reserved.

commandes pour configurer vos nouvelles instances NetScaler sans partitions. Ainsi, pour supprimer les partitions, supprimez manuellement les commandes liées à la création de partitions et cliquez sur **Suivant**.

8. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer les commandes de configuration en cours d'exécution. Cliquez sur **OK**, puis sur **Suivant**.
9. Si vous avez spécifié des variables dans les commandes, sous l'onglet **Spécifier les valeurs des variables**, cliquez sur **Télécharger le fichier de clé d'entrée**. Dans le fichier téléchargé, spécifiez les valeurs des variables, puis téléchargez le fichier vers NetScaler Console.
10. Sous l'onglet **Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11\. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de la planifier pour une exécution ultérieure. Vous pouvez également choisir l'action que NetScaler Console doit entreprendre si la commande échoue et si vous souhaitez envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.

Réutiliser les tâches de configuration exécutées

Les tâches de configuration vous permettent de créer un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Vous pouvez également exécuter le même ensemble de tâches de configuration enregistrées après avoir modifié les commandes, les paramètres, la source de configuration et les instances de la tâche. Ceci est utile lorsque les mêmes ensembles de commandes doivent être exécutés sur une instance différente, ou lorsque la tâche rencontre une erreur et arrête son exécution.

NetScaler Console fournit une fonction pour exécuter à nouveau les tâches terminées. Grâce à cette fonction, les tâches entièrement exécutées peuvent être exécutées à nouveau sans modifier le nom de la tâche.

REMARQUE

Vous ne pouvez réexécuter que les tâches qui sont exécutées lorsque le mode d'exécution est « Maintenant ».

Pour modifier les tâches terminées :

1. Depuis la page d'accueil de NetScaler Console, accédez à **Infrastructure > Tâches de configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sur la page **Tâches**, sélectionnez une tâche dont le résumé d'exécution indique « Terminé », puis cliquez sur **Modifier**. Vous pouvez également modifier une tâche de configuration planifiée.
3. Sur la page **Configurer la tâche**, vous pouvez voir que le nom de la tâche et le type d'instance ne sont pas modifiables. Vous pouvez modifier d'autres champs tels que la source de configuration, ajouter des instances, modifier les valeurs des variables et définir les paramètres d'exécution.
4. Cliquez sur **Terminer** pour exécuter à nouveau la tâche de configuration.

REMARQUE

Vous pouvez également sélectionner la tâche et cliquer à nouveau sur **Exécuter** pour exécuter la tâche sans modifier la source, l'instance et les commandes. Ceci est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, la tâche peut rencontrer une erreur transitoire côté serveur, et vous devrez peut-être exécuter la tâche à nouveau.



Utiliser la commande SCP (put) dans les tâches de configuration

Vous pouvez utiliser la fonctionnalité Tâches de configuration de NetScaler Console pour créer des tâches de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées. Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une seule instance gérée ou sur plusieurs instances gérées. Par exemple, vous pouvez utiliser des tâches de configuration pour les mises à niveau d'appareils.

Les tâches de configuration dans NetScaler Console utilisent des commandes Secure Shell (SSH) pour configurer les instances, et vous pouvez configurer une tâche de configuration pour utiliser la copie sécurisée (SCP) afin de transférer des fichiers en toute sécurité. SCP est basé sur le protocole SSH. L'une des commandes **SCP** que vous pouvez inclure dans une tâche de configuration est la commande « put ». Vous pouvez utiliser la commande « put » dans les tâches de configuration pour télécharger ou transférer un ou plusieurs fichiers stockés dans un répertoire local de votre système vers NetScaler Console, puis vers un répertoire sur l'instance ou les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Le fichier est téléchargé vers NetScaler Console et est ensuite copié (put) vers les instances NetScaler sélectionnées. Le fichier téléchargé est stocké dans NetScaler Console et n'est supprimé que lorsque la tâche est supprimée. Ceci est nécessaire pour les tâches planifiées pour une exécution ultérieure.

La commande a la syntaxe suivante :

```
put <local_filename> <remote_path/remote_filename>
```

Où,

\<local_filename\> est le nom du fichier local à télécharger.

\<remote_path / remote_filename\> est le chemin d'accès à un répertoire distant et le nom à attribuer au fichier lorsqu'il est copié dans ce répertoire.

REMARQUE :

Si le répertoire distant contient un fichier portant le même nom que le fichier local, la commande put écrase le fichier distant.

Lors de la création de la tâche de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'affecter différents fichiers à ces paramètres pour le même ensemble d'instances NetScaler chaque fois que vous exécutez la tâche. De plus, lorsque vous utilisez un fichier à plusieurs endroits dans une tâche et que vous souhaitez renommer le fichier, vous pouvez redéfinir la variable au lieu de modifier le nom du fichier à tous les endroits.

Pour utiliser la commande put afin de télécharger des fichiers dans une tâche de configuration :

1. Accédez à **Infrastructure > Tâches de configuration**.
2. Sur la page **Tâches**, cliquez sur **Créer une tâche**.
3. Sur la page **Créer une tâche**, entrez le nom de la tâche dans le champ Nom de la tâche, et dans le volet **Éditeur de configuration**, entrez la commande « put ».

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Par exemple, si vous souhaitez créer une tâche de configuration qui copie un fichier de certificat SSL enregistré sur votre système local vers plusieurs instances NetScaler, vous pouvez ajouter une commande « put » qui utilise une variable au lieu du nom d'un fichier particulier, et définir le type de variable comme « fichier ».

```
put scp-file /nsconfig/scp-file
```

Dans cet exemple,

- `scp-file` - Il s'agit du nom du fichier qui doit être téléchargé dans l'instance NetScaler.
- `/nsconfig/scp-file` - Il s'agit du dossier de destination sur l'instance où le `scp-file` sera placé après l'exécution de la tâche.

4. Dans la commande que vous avez saisie, sélectionnez le nom de fichier que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**, comme illustré dans la figure suivante.



5. Vérifiez que le nom du fichier est entouré de signes dollar (indiquant qu'il s'agit maintenant d'une variable), puis cliquez sur la variable.
6. Spécifiez les détails de la variable, tels que le nom, le nom d'affichage et le type.
7. Dans la liste déroulante **Type**, sélectionnez **Fichier**. Cliquez sur **Enregistrer**. La déclaration de la variable en tant que type « Fichier » vous permet de télécharger des fichiers vers NetScaler Console.



8. Cliquez sur **Suivant** et sélectionnez les instances NetScaler vers lesquelles copier les fichiers.
9. Sous l'onglet **Spécifier les valeurs de variable**, dans la section **Valeurs de variables communes pour toutes les instances**, sélectionnez le fichier depuis le stockage local de votre système, cliquez sur **Télécharger** pour télécharger le fichier vers NetScaler Console, puis cliquez sur **Suivant**.



10. Dans l'onglet **Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
11. Dans l'onglet **Exécuter**, vous pouvez exécuter le travail maintenant ou le planifier pour une exécution ultérieure. Vous pouvez également choisir l'action que NetScaler Console doit entreprendre si la commande échoue. Vous pouvez également créer une notification par e-mail

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pour recevoir des informations sur la réussite ou l'échec du travail, ainsi que d'autres détails. Cliquez sur **Terminer**.

12. Vous pouvez consulter les détails du travail en accédant à **Infrastructure > Travaux de configuration**, puis en sélectionnant le travail que vous avez configuré. Cliquez sur **Détails**, puis sur **Détails des variables** pour afficher la liste des variables ajoutées à votre travail.

Utiliser des modèles de configuration

Les modèles de configuration vous permettent d'enregistrer et de réutiliser un ensemble de commandes de configuration afin que vous puissiez appliquer des configurations cohérentes sur toutes vos instances NetScaler. Les rubriques suivantes vous aident à créer et à gérer des modèles de configuration :

- Utiliser le modèle de configuration principal
- Planifier des tâches créées à l'aide de modèles intégrés
- Planifier une tâche pour configurer l'exportation de métriques de NetScaler vers Prometheus
- Utiliser des modèles de configuration pour créer des modèles d'audit
- Replannifier des tâches configurées à l'aide de modèles intégrés
- Réutiliser les modèles d'audit de configuration dans les tâches de configuration
- Importer et exporter des modèles de configuration

Utiliser le modèle de configuration maître

L'utilisation d'un modèle de configuration principal est une option flexible pour créer et déployer une configuration maître sur plusieurs instances NetScaler.

En tant qu'administrateur, vous pouvez souhaiter apporter des modifications de configuration et enregistrer des licences, des certificats et d'autres fichiers sur l'instance NetScaler. Vous pouvez enregistrer la nouvelle configuration en tant que modèle de configuration maître (fichier .conf).

Pour enregistrer votre modèle de configuration maître à partir d'une instance NetScaler, vous pouvez effectuer l'une des opérations suivantes :

- À l'invite de commande, entrez **save ns config**. La configuration est enregistrée dans la mémoire FLASH de l'instance, dans le fichier /nsconfig/ns.conf.
- Depuis l'interface graphique de l'instance, accédez à **Diagnostics** \> **View Configuration**. Choisissez le type de configuration que vous souhaitez enregistrer. Par exemple, si vous souhaitez enregistrer la configuration sauvegardée de votre instance, sélectionnez **Saved**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

configuration. Cliquez sur le lien **Save text to a file** pour enregistrer le fichier 'ns.conf' sur votre machine locale.

Lorsque vous déployez le modèle de configuration maître en utilisant le modèle de configuration 'DeployMasterConfiguration' lors de la création d'une tâche, vous pouvez le personnaliser davantage pour chaque instance NetScaler spécifique en ajoutant d'autres commandes, en modifiant les commandes existantes et en fournissant différentes valeurs de variables dans le fichier d'entrée.

Par exemple, en tant qu'administrateur, vous pouvez souhaiter télécharger des clés de certificat vers vos instances NetScaler en plus du fichier ns.conf et y déployer également la configuration maître.

IMPORTANT

Vous ne pouvez pas exécuter une tâche de configuration à l'aide du modèle DeployMasterConfiguration sur les instances NetScaler CPX, les instances configurées dans un cluster ou sur les instances NetScaler partitionnées.

Pour créer une tâche de configuration à l'aide du modèle de configuration maître sur NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Configuration Jobs**, puis cliquez sur **Create Job**.
2. Sur la page **Create Job**, sous l'onglet **Select Configuration**, spécifiez le **Job Name** et sélectionnez le **Instance Type** dans la liste déroulante.
3. Sélectionnez **Master Configuration** dans la liste déroulante **Configuration Source**. Faites glisser les commandes du modèle DeployMasterConfiguration vers le volet droit. Vous pouvez également ajouter, modifier ou supprimer des commandes dans le volet droit. Cliquez sur **Next**.

   REMARQUE

   Vous pouvez ajouter des commandes ***put*** pour ajouter des fichiers d'entrée à votre modèle. Dans notre exemple, nous devons télécharger des fichiers de certificat et de clé en plus du fichier de modèle de configuration et des fichiers d'entrée de variables.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'une tâche de configuration dans une vue consolidée unique.
5. Effectuez l'une des opérations suivantes pour afficher toutes les variables dans une vue consolidée unique :

    - Lors de la création d'une tâche de configuration, accédez à **Infrastructure > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer une tâche**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création de la tâche de configuration.
    - Lors de la modification d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.

6. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définies lors de la création ou de la modification d'une tâche de configuration.

    

7. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables tels que le nom, le nom d'affichage, le type et la valeur par défaut dans un format tabulaire. Vous pouvez également modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.

    

8. Sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche de configuration, puis cliquez sur **Suivant**.
9. Dans l'onglet **Spécifier les valeurs des variables**, chargez les éléments suivants :

    - **Fichier de modèle de configuration (.conf)** - Chargez le fichier .conf que vous avez extrait d'une instance NetScaler.
    - **Charger le fichier d'entrée (.xml/csv)** - Chargez le fichier d'entrée avec les valeurs des variables que vous avez définies dans vos commandes.

    Un exemple de fichier xml est fourni ici pour votre utilisation. Assurez-vous que les fichiers xml contiennent les détails correspondant aux instances NetScaler que vous utilisez.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
parameters and values.

If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence over the
instance group. The instance group specific parameters value will take
precedence over global parameters in the execution.

-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters and
value.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence in the
execution.



-  name. This attribute represents the IP Address of the instance. Host
name is not supported for the attibute.



HA pair should be represented as <primaryip>-<secondaryip>. Example
10.102.2.1-10.102.2.2



In the template file, the parameter name must be specified within the
dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters names are
case sensitive.

-->



<global>



</global>

<devicegroup name="BLR_DEVS">

</devicegroup>

<device name="10.106.101.209">

<param name="IP" value="10.106.101.209"/>

</device>



<!-- HA PAIR-->
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<!--<device name="10.102.43.154-10.102.43.155">

<param name="NSIP" value="10.102.43.154"/>

<param name="HostName" value="NS43HA"/>

<param name="LBSERVER" value="haserver43http"/>

<param name="SNMPTrapDest" value="10.102.43.130"/>

</device>-->

</properties>
```

10. Cliquez sur **Suivant**.



Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et téléchargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, puis cliquez sur **Créer une tâche**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs de variable communes à toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau \> Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs de variable communes à toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

1. Sous l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances, puis cliquez sur **Suivant**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sous l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de la planifier pour une exécution ultérieure. Vous pouvez également choisir l'action que NetScaler Console doit entreprendre si la commande échoue.

   Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées, et vous pouvez choisir d'envoyer ou non une notification par e-mail concernant la réussite ou l'échec de la tâche, ainsi que d'autres détails.

   

Après avoir exécuté votre tâche, vous pouvez consulter les détails de la tâche en accédant à **Infrastructure > Tâches de configuration** et en sélectionnant la tâche que vous avez configurée. Cliquez sur **Détails**, puis sur **Résumé de l'exécution** pour afficher les détails de votre tâche. Cliquez sur l'instance pour afficher les **Journaux de commandes** afin de voir les commandes exécutées sur la tâche.



Planifier des tâches créées à l'aide de modèles intégrés

Vous pouvez planifier une tâche en utilisant l'option de modèle intégré. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, utilisez l'option de modèle intégré pour planifier une tâche de configuration de serveurs syslog. Vous pouvez également choisir d'exécuter la tâche immédiatement ou de la planifier pour qu'elle soit exécutée ultérieurement.

Pour planifier une tâche à l'aide de modèles intégrés dans NetScaler Console

1. Dans NetScaler Console, accédez à **Infrastructure > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Sur la page **Créer une tâche**, dans l'onglet **Sélectionner la configuration**, spécifiez le **Nom de la tâche** et sélectionnez le **Type d'instance** dans la liste déroulante.
3. Sélectionnez **Modèle intégré** dans la liste déroulante **Source de configuration**. Faites glisser la commande ***NSConfigureSyslogServer** vers le volet de droite, puis cliquez sur **Suivant**.

   

4. Dans l'onglet **Sélectionner les instances**, cliquez sur **Ajouter des instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche, puis cliquez sur **OK**.
5. Cliquez sur **Suivant**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'une des options suivantes pour spécifier les variables de vos instances :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Valeurs de variable à partir d'un fichier d'entrée** - Téléchargez un fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes. Ensuite, téléchargez le fichier sur le serveur NetScaler Console.
- **Valeurs de variable communes à toutes les instances** – Spécifiez l'adresse IP et le port du serveur syslog.

6. Dans l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
7. Cliquez sur **Suivant**.
8. Dans l'onglet **Exécuter**, définissez les conditions suivantes :

   - **En cas d'échec de la commande** - Si une commande échoue, vous pouvez choisir d'ignorer les erreurs et de continuer à exécuter la tâche, ou d'arrêter l'exécution ultérieure de la tâche. Choisissez l'action que vous souhaitez exécuter dans la liste déroulante.
   - **Mode d'exécution** - Vous pouvez exécuter la tâche immédiatement ou la planifier pour une exécution ultérieure. Si vous souhaitez planifier la tâche ultérieurement, vous devez spécifier les paramètres de fréquence d'exécution pour cette tâche. Choisissez le calendrier que vous souhaitez que la tâche suive dans la liste déroulante.

9. Vous pouvez également exécuter une tâche sur un ensemble d'instances séquentiellement ou en parallèle en sélectionnant la méthode requise sous **Paramètres d'exécution**. Si l'exécution d'une tâche échoue sur une instance, elle ne se poursuit pas sur les instances restantes.

   Vous pouvez choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées. Une notification par e-mail peut également être envoyée concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.

10. Cliquez sur **Terminer**.

Planifier une tâche pour configurer l'exportation de métriques de NetScaler vers Prometheus

À l'aide du modèle `NSConfigurePrometheusAnalyticsProfile`, vous pouvez utiliser le schéma par défaut ou un schéma personnalisé avec des paramètres modifiés, et exécuter la tâche sur toutes les instances gérées.

Prérequis

Assurez-vous que les NetScalers gérés sont en version **13.1 build 39-27 ou ultérieure**.

Pour planifier une tâche :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans NetScaler Console, accédez à **Infrastructure > Configuration > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Sur la page **Créer une tâche**, spécifiez un nom pour la tâche et sélectionnez **NetScaler** dans la liste **Type d'instance**.
3. Sélectionnez **Modèle intégré** dans la liste **Source de configuration**. Faites glisser la commande *NSConfigurePrometheusAnalyticsProfile* vers le volet droit, puis cliquez sur **Suivant**. Vous pouvez également cliquer sur **+** pour ajouter le modèle.

   
4. Si vous souhaitez utiliser le schéma par défaut :
   a. Supprimez l'étape 3 (`put $Schema_file /var/metrics.conf/$schema_filename$`). Placez le pointeur de la souris à l'étape 3 et :
      - Sous Windows, utilisez Ctrl + A et Suppr.
      - Sous Mac, utilisez Commande + A et Suppr.
   b. Après la suppression, cliquez sur **Suivant**.
   c. Sous l'onglet **Sélectionner les instances**, cliquez sur **Ajouter des instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche, puis cliquez sur **Suivant**.
   d. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez **Valeurs de variables communes pour toutes les instances**.
      - **Nom du profil de série chronologique d'analyse** - Spécifiez le nom du profil d'analyse. Pour plus d'informations, consultez `https://docs.netscaler.com/fr-fr/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`.
      - **Nom du fichier de schéma à télécharger sur NetScaler** - Conservez ce nom de fichier tel quel `schema.json`, car c'est le fichier par défaut.

        
   e. Passez à l'étape 6.
5. Si vous souhaitez utiliser un compteur de schéma personnalisé :
   a. Sélectionnez **Modèle intégré** dans la liste **Source de configuration**. Faites glisser la commande `NSConfigurePrometheusAnalyticsProfile` vers le volet de droite et cliquez sur **Suivant**. Vous pouvez également cliquer sur + pour ajouter le modèle.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Dans l'onglet **Sélectionner les instances**, cliquez sur **Ajouter des instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche, puis cliquez sur **Suivant**.

c. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez **Valeurs de variables communes pour toutes les instances**.

- **Fichier de schéma de compteur NetScaler (.json)** - Sélectionnez le fichier de schéma que vous avez modifié avec les paramètres. Dans NetScaler, un fichier de référence `reference_schema.json` avec tous les compteurs pris en charge est disponible sous le chemin `/var/metrics_conf/`.

  Vous pouvez utiliser un client FTP pour copier le fichier en local, modifier les paramètres requis, l'enregistrer, puis le télécharger.

- **Nom du fichier de schéma à télécharger sur NetScaler** - Spécifiez le nom du fichier de schéma que vous souhaitez télécharger sur NetScaler.
- **Nom du profil de série chronologique d'analyse** - Spécifiez le nom du profil d'analyse. Pour plus d'informations, consultez `https://docs.netscaler.com/fr-fr/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`.

6. Sous l'onglet **Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
7. Cliquez sur **Suivant**.
8. Sous l'onglet **Exécuter**, définissez les conditions suivantes :

   - **En cas d'échec de la commande** - Si une commande échoue, vous pouvez choisir d'ignorer les erreurs et de continuer à exécuter la tâche ou d'arrêter l'exécution ultérieure de la tâche. Choisissez l'action que vous souhaitez exécuter dans la liste déroulante.
   - **Mode d'exécution** - Vous pouvez exécuter la tâche maintenant ou planifier son exécution ultérieurement. Si vous souhaitez planifier la tâche ultérieurement, vous devez spécifier les paramètres de fréquence d'exécution pour cette tâche. Choisissez le calendrier que vous souhaitez que la tâche suive dans la liste déroulante.

9. Vous pouvez également exécuter une tâche sur un ensemble d'instances séquentiellement ou en parallèle en sélectionnant la méthode requise sous **Paramètres d'exécution**. Si l'exécution d'une tâche échoue sur une instance, elle ne se poursuit pas sur les instances restantes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées, et vous pouvez choisir d'envoyer ou non des notifications concernant la réussite ou l'échec de la tâche, ainsi que d'autres détails.

10. Cliquez sur **Terminer**.



Utiliser des modèles de configuration pour créer des modèles d'audit

Vous pouvez maintenant utiliser les commandes de configuration précédemment enregistrées en tant que modèles de configuration pour créer des Modèles d'audit qui peuvent être appliqués à des instances NetScaler spécifiques. Lors de la création d'un modèle d'audit, vous pouvez faire glisser les modèles de configuration précédemment enregistrés dans le champ Commandes et modifier le modèle pour l'adapter à vos besoins. Vous pouvez ensuite appliquer le modèle d'audit à des instances NetScaler spécifiques. NetScaler Console compare ces instances avec le modèle d'audit et signale toute non-concordance. Ce processus vous aide à identifier les erreurs et à les corriger en temps opportun.

Vous pouvez créer des modèles de configuration lors de la création d'une tâche et en enregistrant un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page **Créer des tâches**, ils sont automatiquement affichés sur la page **Créer un modèle**.

Par exemple, considérez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

```
add lb vserver >servername> HTTP <ipaddress portnumber>
```

```
add service <servicename1 ipaddress1> HTTP 80
```

```
add service <servicename2 ipaddress2> HTTP 80
```

```
bind lb vserver <servername servicename1>
```

```
bind lb vserver <servername servicename2>
```

Pour enregistrer un modèle de configuration dans NetScaler Console :

1. Accédez à **Infrastructure > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Sur la page **Créer une tâche**, spécifiez le nom de la tâche et le type d'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Choisissez **Modèle de configuration** comme source de configuration et, dans le champ **Commandes**, entrez des commandes telles que celles de l'exemple ci-dessus.
4. Cochez la case **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour votre modèle. Vous pouvez choisir d'écraser d'autres modèles existants portant le même nom.
5. Cliquez sur **Enregistrer**.



Pour utiliser un modèle de configuration afin de créer un modèle d'audit dans NetScaler Console :

1. Accédez à **Infrastructure > Audit de configuration > Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer un modèle**, spécifiez un nom pour le modèle et saisissez une description.
3. Dans la liste **Source de configuration**, sélectionnez **Modèle de configuration**, puis faites glisser le modèle dans le champ Commandes du volet droit. Vous pouvez également modifier la configuration et enregistrer le modèle sous un nom différent. Cliquez sur **Suivant**.
4. Dans l'onglet **Sélectionner les instances**, cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez exécuter la configuration. Cliquez sur **OK**.
5. Cliquez sur **Terminer**.



Le modèle d'audit apparaît dans la liste des modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées.

Reprogrammer les jobs configurés à l'aide de modèles intégrés

Vous pouvez reprogrammer un job que vous avez planifié à l'aide de modèles intégrés dans NetScaler Console. Par exemple, vous pouvez modifier l'action que NetScaler Console doit effectuer si une commande échoue. Si vous aviez précédemment choisi d'ignorer une erreur et de continuer, vous pouvez modifier cela pour annuler toutes les commandes réussies si une commande échoue.

Pour reprogrammer un job qui a été configuré à l'aide de modèles intégrés dans NetScaler Console

1. Dans NetScaler Console, accédez à **Infrastructure > Configuration Jobs**.
2. Sélectionnez le job que vous souhaitez modifier, ajouter ou supprimer des instances, spécifier des valeurs de variables, puis modifier les actions et les paramètres d'exécution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur **Terminer** pour reprogrammer le job.

REMARQUE

Vous pouvez également sélectionner le job et cliquer sur **Exécuter à nouveau** pour l'exécuter sans modifier la source, l'instance et les commandes. Cette fonctionnalité est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le job peut rencontrer une erreur transitoire côté serveur, et vous devrez peut-être l'exécuter à nouveau.

Réutiliser les modèles d'audit de configuration dans les tâches de configuration

En tant qu'administrateur, vous pouvez désormais enregistrer les commandes de configuration sous forme d'un ensemble de modèles de configuration réutilisables lorsque vous créez une tâche et exécutez un audit de configuration. Le modèle de configuration créé et enregistré dans les tâches de configuration est disponible dans l'audit de configuration pour créer un modèle d'audit qui peut être appliqué à des instances NetScaler spécifiques. De même, le modèle d'audit créé dans le module d'audit de configuration est disponible dans les tâches de configuration afin que vous puissiez exécuter le modèle en tant que tâche de configuration. Toute modification apportée au modèle est désormais visible dans les modules Tâches de configuration et Audit de configuration.

Auparavant, les modèles de tâche de configuration et d'audit de configuration devaient être créés séparément pour la même configuration et enregistrés sous différents fichiers. Cela entraînait une duplication des efforts de création et de maintenance des modèles.

NetScaler Console vous permet d'enregistrer ce modèle dans le système afin que le modèle d'audit soit également disponible dans les tâches de configuration. Désormais, les modèles d'audit peuvent être utilisés pour créer des tâches de configuration. De cette façon, les modèles peuvent être utilisés de manière interchangeable entre les tâches de configuration et les audits de configuration.

Par exemple, considérez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add lb vserver servername HTTP ipaddress portnumber


add service servicename1 ipaddress1 HTTP 80


add service servicename2 ipaddress2 HTTP 80


bind lb vserver servername servicename1


bind lb vserver servername servicename2
```

Création d'un modèle dans les audits de configuration et sa réutilisation dans les tâches de configuration

Effectuez la tâche suivante pour créer un modèle dans le module d'audit de configuration et le réutiliser dans le module de tâches de configuration.

Pour créer un modèle d'audit :

1. Dans NetScaler Console, accédez à **Infrastructure > Audit de configuration > Modèle d'audit**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer un modèle**, spécifiez le nom du modèle. Vous pouvez également ajouter plus d'informations sur le modèle dans le champ **Description**.
3. Dans le volet **Commandes**, entrez les commandes de l'exemple.
4. Cochez la case **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour votre modèle, par exemple, vous pouvez nommer ce modèle « LBVariablesTemplate ». Vous pouvez choisir d'écraser d'autres modèles existant avec le même nom.

   REMARQUE

   Le nom du modèle d'audit peut être identique au nom du modèle de configuration.

5. Cliquez sur **Enregistrer**, puis sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Cliquez sur **Suivant**.
7. Dans l'onglet **Sélectionner les instances**, sélectionnez les **instances NetScaler** sur lesquelles vous souhaitez exécuter ces commandes de configuration, puis cliquez sur **Terminer**. Le nouveau modèle est maintenant visible dans la liste des modèles d'audit.

   
8. Lorsque vous souhaitez exécuter ces commandes de configuration, accédez à **Infrastructure > Tâches de configuration**, puis cliquez sur **Créer une tâche**. Le modèle d'audit que vous avez créé précédemment est répertorié comme modèle de configuration.

Pour réutiliser le modèle d'audit dans les tâches de configuration :

1. Saisissez un nom pour la tâche, sélectionnez le type d'instance et faites glisser le modèle vers le volet des commandes.

   Lors de la création de la tâche de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'affecter différents fichiers à ces paramètres pour le même ensemble d'instances NetScaler chaque fois que vous exécutez la tâche.
2. Dans la commande que vous avez saisie, sélectionnez le nom de fichier que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**.
3. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter ces commandes.
4. Si vous avez spécifié des variables dans les commandes, dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'une des options suivantes pour spécifier les variables de vos instances :

   - Valeurs de variable à partir d'un fichier d'entrée - Téléchargez un fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur NetScaler Console.
   - Valeurs de variable communes pour toutes les instances – Spécifiez l'adresse IP et le port du serveur syslog.
5. Dans l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances, puis cliquer sur **Suivant**.
6. Dans l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter la tâche de configuration. Si vous souhaitez maintenant ajouter un autre service à ce serveur d'équilibrage de charge et lier le

© 1997–2026 Citrix Systems, Inc. All rights reserved.

service au serveur, vous pouvez modifier les commandes dans la page de commande et les enregistrer.

7. Accédez à **Modèles d'audit** et cliquez sur **Ajouter**.
8. Faites glisser le modèle « LBVariablesTemplate » vers le volet des commandes. Vous pouvez voir que le modèle a été mis à jour avec les nouvelles commandes.

Le modèle d'audit apparaît dans la liste des modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées. Vous pouvez maintenant créer des modèles et les réutiliser entre les tâches de configuration et les modules d'audit de configuration.

Importer et exporter des modèles de configuration

Vous pouvez exporter les modèles de configuration depuis n'importe quelle NetScaler Console. Vous pouvez également importer le fichier vers la même NetScaler Console ou une autre à tout moment. Les données des modèles de configuration (telles que les commandes de configuration, les définitions de variables et les paramètres) ne sont pas perdues.

Vous pouvez exporter les modèles de configuration vers un fichier au format **.json** et l'enregistrer dans le dossier local. Vous pouvez importer des fichiers **.json** de modèles de configuration dans NetScaler Console. Ce fichier peut être nouveau ou celui que vous avez exporté depuis la même NetScaler Console ou une autre.

Pour exporter les modèles de configuration :

1. Accédez à **Infrastructure > Tâches de configuration > Modèles de configuration**.
2. Cliquez sur le bouton **Ajouter** pour créer le modèle de configuration.
3. Sur la page **Créer un modèle de configuration**, spécifiez le nom du modèle de configuration et choisissez le type d'instance. Sous **Éditeur de configuration**, sélectionnez la source de configuration comme Modèle de configuration dans le menu déroulant. Vous pouvez faire glisser les modèles de configuration existants vers l'éditeur de configuration. Cliquez sur **Créer**.

   
4. Accédez à **Infrastructure > Tâches de configuration > Modèles de configuration** pour afficher les modèles créés dans la liste des modèles de configuration.

   
5. Sélectionnez le modèle de configuration nouvellement créé et cliquez sur le bouton **Exporter**.

Le modèle de configuration correspondant est téléchargé sur votre système local au format **.json**.

Pour importer les modèles de configuration :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Infrastructure > Tâches de configuration > Modèles de configuration** et cliquez sur le bouton **Importer**. Sélectionnez le chemin où se trouvent les fichiers **.json** du modèle de configuration et téléchargez les fichiers **.json**. Il est recommandé de télécharger les fichiers **.json** que vous avez déjà exportés.
2. Vous pouvez également importer le modèle de configuration à l'aide de l'option **Fichier** dans l'Éditeur de configuration.
3. Sélectionnez **Fichier** dans le menu déroulant de l'**Éditeur de configuration**.
4. Sélectionnez **Choisir un fichier** (fichiers **.json**) depuis votre système local et téléchargez les fichiers **.json** du modèle de configuration.

REMARQUE

- Chaque nouveau modèle importé est stocké avec une nouvelle chaîne d'ID.
- Vous pouvez importer les modèles de configuration uniquement si le fichier est enregistré au format **.json**. Si vous importez des modèles de configuration autres que des fichiers **.json** depuis votre système local, une erreur s'affiche et l'importation des fichiers échoue.

Audit de configuration

Ce document inclut des sujets sur la façon de :

- Afficher les rapports d'audit
- Auditer les modifications de configuration sur les instances
- Obtenir des conseils de configuration sur la configuration réseau
- Interroger l'audit de configuration des instances NetScaler
- Générer la différence d'audit de configuration pour les traps SNMP ConfigChange

Afficher les rapports d'audit

(NetScaler Console) vous permet d'afficher et de télécharger le rapport de différences d'audit de configuration dans la section d'audit de configuration. La section d'audit de configuration vous permet d'exporter :

- Rapport récapitulatif pour toutes les instances par instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Rapport différentiel (diff) granulaire pour chaque paire instance-modèle

Les modèles d'audit dans **Modèles d'audit** s'exécutent à l'heure prévue par rapport aux configurations des instances spécifiées. Le graphique **Dérive de configuration NetScaler** sur le tableau de bord **Audit de configuration** affiche des détails de haut niveau sur les modifications de configuration entre les configurations enregistrées et non enregistrées. Lorsque vous cliquez sur le graphique **Dérive de configuration NetScaler**, la page **Rapports d'audit** qui s'affiche présente une liste d'instances affichant à la fois « Différence existante » et « Aucune différence ». Vous pouvez télécharger les rapports de différences affichés par NetScaler Console.

NetScaler Console offre également une option pour planifier l'exportation automatique d'un rapport de différences en tant que pièce jointe à un e-mail.

Pour exporter les rapports d'audit de configuration :

1. Dans NetScaler Console, accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Sur la page **Audit de configuration**, cliquez à l'intérieur du graphique **Dérive de configuration NetScaler®**.
3. La page **Rapports d'audit** répertorie les instances qui présentent une différence. La page affiche également une liste d'instances qui ne présentent aucune différence dans leurs configurations en cours d'exécution.



Dans l'image, vous pouvez voir que pour certaines instances, une différence est présente uniquement dans **Différence enregistrée vs en cours d'exécution** et pour certaines instances, une différence est présente uniquement dans **Modèle vs Différence en cours d'exécution**. Pour certaines instances, des différences existent à la fois dans **Différence enregistrée vs en cours d'exécution** et **Modèle vs Différence en cours d'exécution**.

Différence enregistrée vs en cours d'exécution

Vous pouvez afficher un rapport de la différence entre la configuration enregistrée sur l'instance et la configuration actuellement en cours d'exécution sur l'instance.

1. Cliquez sur **Différence existante** pour une instance sous **Différence enregistrée vs en cours d'exécution**.

   

   Vous pouvez afficher le rapport de la différence entre la configuration enregistrée et la configuration en cours d'exécution pour cette instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur **Exporter le rapport de différences** pour télécharger un fichier .csv du rapport de différences. Vous pouvez également cliquer sur **Exporter les commandes correctives** pour exporter les commandes vers un fichier .txt. Vous pouvez ensuite exécuter les commandes sur l'instance NetScaler Console associée à partir des tâches de configuration pour corriger la configuration de cette instance.



Différence entre le modèle et l'exécution

La section **Différence entre le modèle et l'exécution** inclut tous les modèles autres que **Différence entre la configuration enregistrée et la configuration en cours d'exécution**, qui est le modèle par défaut. Vous pouvez afficher la différence qui existe entre le modèle et la configuration en cours d'exécution.

1. Cliquez sur **Différence existante** pour l'une des instances sous **Différence entre le modèle et l'exécution**.



2. Les modèles révèlent les différences lorsque l'instance NetScaler Console s'écarte de la configuration spécifiée par le modèle.



3. Cliquez à nouveau sur **Différence existante**. L'image suivante montre la configuration recherchée par le modèle, les configurations en cours d'exécution et les configurations de correction ou les commandes à exécuter pour corriger la configuration. Si la **Configuration en cours d'exécution** est vide, cela signifie que les commandes ne sont pas configurées ou ont été supprimées.



4. Cliquez sur **Exporter le rapport de différences** pour télécharger un fichier .csv du rapport de différences. Vous pouvez également cliquer sur **Exporter les commandes correctives** pour exporter les commandes vers un fichier .txt. Vous pouvez ensuite exécuter les commandes dans l'interface de ligne de commande pour corriger la configuration de l'instance.



Vous pouvez également utiliser le paramètre de dérive Modèle vs Exécution et Exécution vs modèle pour comparer la configuration des deux manières :

- Compare la configuration du modèle d'audit avec la configuration en cours d'exécution sur l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Compare la configuration en cours d'exécution sur l'instance avec le modèle d'audit.

Par défaut, le paramètre de dérive Modèle vs. Exécution est sélectionné. Pour modifier le paramètre de dérive, sélectionnez **Paramètres** dans la page **Audit de configuration**.



Afficher les rapports d'audit de l'état des fichiers

Utilisez le graphique **État des fichiers NetScaler** pour surveiller si des fichiers sont ajoutés, modifiés ou supprimés du dossier `nsconfig`. Par exemple, si le fichier de licence est mis à jour sur une instance NetScaler, vous pouvez vérifier la date de la dernière mise à jour de ce fichier et prendre les mesures nécessaires.

1. Accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez sur le graphique **État des fichiers de configuration NetScaler**.

   La page **Rapports d'audit** répertorie les instances avec l'état Diff.

   L'**état Diff** est calculé pour l'intervalle entre l'**heure de sondage précédente** et l'**heure de sondage la plus récente**. L'**état Diff** peut être l'un des suivants :

   - **Différence existante** - Cet état indique que les fichiers ont été modifiés dans le dossier `nsconfig` d'une instance depuis l'**heure de sondage précédente**. Pour afficher ce qui a changé sur le fichier, cliquez sur **Différence existante**.

     

   - **Pas de différence** - Cet état indique que les fichiers du dossier `nsconfig` n'ont pas changé depuis l'heure de sondage précédente.
   - **N/A** - Cet état indique que la surveillance de l'état des fichiers n'est pas applicable. Cet état apparaît lorsque la console NetScaler ne sonde pas l'instance. Par exemple, lorsqu'une instance est nouvellement ajoutée ou qu'un état d'instance est inactif, le sondage de l'instance ne se produit pas.

Exclure des fichiers de l'audit de configuration

Vous pouvez exclure des fichiers spécifiques de l'audit de configuration (Config Audit) afin qu'ils ne soient pas surveillés pour les changements. Utilisez les exclusions pour les fichiers générés par le système ou fréquemment mis à jour (par exemple, les fichiers qui changent quotidiennement) afin de réduire le bruit et d'éviter les faux positifs dans les résultats d'audit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemples de noms de fichiers (ou de chemins relatifs) à exclure de la comparaison de fichiers de l'audit de configuration :

- Nom de fichier valide (ou chemin relatif)
  - `ns.conf`, `ssl/ns.cert`
- Nom de fichier non valide (ou chemin relatif)
  - `/ns.txt`, `\nsconfig\ns.conf` (Le nom de fichier exclu doit être un chemin relatif)
  - `ñs.conf` (Le nom de fichier exclu ne doit contenir que des caractères ASCII)
  - `C:/nsconfig/ns.conf` (Le nom de fichier exclu ne doit pas utiliser de chemins avec des lettres de lecteur)
  - `ssl/../../ns.conf` (Le nom de fichier exclu ne doit pas contenir de traversée de répertoire parent `..`)

Pour exclure des fichiers de l'audit de configuration, suivez les étapes suivantes :

1. Accédez à **Infrastructure > Configuration > Configuration Audit**.
2. Sélectionnez **Paramètres**.
3. Sous **Paramètres du fichier de configuration NetScaler**, ajoutez les chemins de fichiers que vous souhaitez exclure de l'audit.
4. Cliquez sur **Enregistrer**.

Auditer les modifications de configuration sur les instances

Vous voulez vous assurer que certaines configurations s'exécutent sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances NetScaler gérées, résoudre les erreurs de configuration et récupérer les configurations non enregistrées après un arrêt soudain du système.

Vous pouvez créer des modèles d'audit avec des configurations spécifiques à auditer sur certaines instances. NetScaler Console compare ces instances avec le modèle d'audit et signale toute non-concordance dans la configuration. Le rapport de différences de configuration vous permet de résoudre et de corriger les modifications de configuration indésirables.

Vous pouvez automatiser l'exécution du modèle d'audit en :

- Planifiant l'heure à laquelle le modèle doit être exécuté.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Définissant la fréquence à laquelle NetScaler Console doit exécuter le modèle. Vous pouvez exécuter le modèle quotidiennement, un jour spécifique de la semaine ou une date spécifique du mois.

Vous avez également la possibilité d'envoyer le rapport de différences généré par NetScaler Console aux adresses e-mail spécifiées que vous pouvez configurer. Avec cette option, les utilisateurs peuvent recevoir le rapport en tant que pièce jointe ou notification Slack. Ils n'ont pas besoin de se connecter à NetScaler Console pour exporter les rapports manuellement.

REMARQUE :

L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Cependant, vous pouvez renommer les modèles de configuration personnalisés.

Pour créer des modèles d'audit :

1. Accédez à **Infrastructure > Configuration > Audit de configuration > Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle**, et dans l'onglet **Commandes d'audit**, spécifiez le nom du modèle et sa description.
3. Dans la page **Éditeur de configuration**, saisissez vos commandes et enregistrez-les en tant que modèle de configuration. Vous pouvez également faire glisser un modèle existant du volet gauche vers l'éditeur.
4. Sélectionnez les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge « ipaddress1 », puis cliquez sur **Convertir en variable**. La variable est maintenant encadrée par « $ ».

   Dans la fenêtre **Définir la variable**, définissez les propriétés de cette variable : nom, nom d'affichage et type de variable. Cliquez sur l'option **Avancé** si vous souhaitez spécifier davantage une valeur par défaut pour votre variable.

   Vous pouvez également enregistrer les commandes en tant que modèle de configuration.

5. Cliquez sur **Enregistrer**, puis sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration, puis cliquez sur **Suivant**.



7. Dans l'onglet **Spécifier les valeurs des variables**, vous avez deux options :

   a. Téléchargez le fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes. Après avoir saisi les variables, téléchargez le fichier sur le serveur NetScaler Console.



   a. Saisissez des valeurs communes pour les variables que vous avez définies pour toutes les instances.



REMARQUE :

Si vous souhaitez auditer chaque instance avec des valeurs différentes, vous devez créer des variables distinctes dans le fichier d'entrée pour chaque instance.

8. Cliquez sur **Suivant**.
9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.



10. Dans l'onglet **Planifier le modèle**, vous disposez des options suivantes pour planifier l'exécution du modèle et configurer l'adresse e-mail à laquelle envoyer le rapport de différences.

    - **Utiliser l'intervalle d'interrogation global**. Sélectionnez cette option pour exécuter le modèle sur les instances à un moment configuré globalement sur NetScaler Console.
    - **Personnaliser la planification du modèle**. Utilisez cette option pour configurer l'heure et la fréquence d'exécution des modèles.
        - Spécifiez la fréquence et le moment d'exécution des modèles d'audit.
    - **Activer l'exportation des rapports**. Utilisez cette option pour :
        - **Envoyer le rapport de différences uniquement si des différences sont trouvées**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Envoyer le rapport de différences par e-mail**. Configurez le profil de messagerie auquel le rapport de différences doit être envoyé en pièce jointe.
- **Envoyer le rapport de différences via Slack**. Configurez le canal Slack auquel le rapport de différences doit être envoyé en tant que notification.

11. Cliquez sur **Terminer**.

Le modèle d'audit apparaît dans la liste **Modèles d'audit** et est exécuté à l'heure prévue par rapport aux configurations des instances spécifiées.

Afficher les modifications de configuration

Vous pouvez également utiliser le tableau de bord **Audit de configuration** pour afficher des détails de haut niveau sur les modifications de configuration, tels que :

- Les 10 instances principales par modification de configuration
- Le nombre de configurations enregistrées et non enregistrées
- Le fichier ajouté, supprimé ou modifié dans le dossier `nsconfig`

NetScaler Console vous permet également d'interroger manuellement les audits de configuration et ajoute immédiatement tous les audits de configuration des instances à NetScaler Console. Pour ce faire, accédez à **Infrastructure > Configuration > Audit de configuration**, cliquez sur **Interroger maintenant**. La page contextuelle **Interroger maintenant** vous offre la possibilité d'interroger toutes les instances NetScaler du réseau, ou d'interroger les instances sélectionnées.

Vous pouvez également forcer un audit sur une instance. Pour ce faire, cliquez sur l'un des graphiques suivants :

- **État de la configuration NetScaler enregistrée**
- **Dérive de la configuration NetScaler**

Sur la page **Rapports d'audit**, sélectionnez l'instance et, dans la liste **Action**, sélectionnez **Interroger maintenant**.

Le graphique **État du fichier de configuration NetScaler** vous indique l'état des fichiers NetScaler présents dans le dossier `nsconfig`. NetScaler Console enregistre et compare les modifications apportées aux fichiers dans le dossier `nsconfig` et affiche les différences. Voir, Afficher les rapports d'audit de l'état des fichiers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Définir les notifications d'audit de configuration

1. Accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez sur **Paramètres**.
3. Dans la page **Paramètres de notification**, cliquez sur l'icône **Modifier** pour activer les paramètres de notification.
4. Cochez la case **Activé**. Choisissez une liste de distribution de courriels dans la liste déroulante. Vous pouvez également créer une liste de distribution de courriels en cliquant sur l'icône **+** et en spécifiant les détails du serveur de messagerie.

Obtenir des conseils de configuration sur la configuration réseau

Vous configurez vos instances NetScaler avec des configurations optimales afin d'obtenir des performances optimales sur vos applications. Cependant, certaines configurations peuvent ne pas être des configurations standard, ce qui pourrait affecter les performances de vos applications.

Pour vous aider à optimiser les performances de vos applications, NetScaler Console analyse la configuration de l'instance NetScaler et vous fournit des recommandations. Vous pouvez appliquer les configurations recommandées depuis NetScaler Console.

Pour analyser l'instance NetScaler :

1. Accédez à **Infrastructure > Configuration > Audit de configuration > Conseils de configuration**.
2. Effectuez l'une des opérations suivantes :

   - Cliquez sur **Télécharger le fichier de configuration** et téléchargez le fichier de configuration de votre instance réseau.

   - Cliquez sur **Sélectionner un appareil** et sélectionnez l'instance NetScaler que vous souhaitez analyser.

NetScaler Console analyse la configuration de votre instance et fournit une liste de recommandations de configuration, comme illustré dans l'image suivante. Cochez la case à côté d'un conseil de configuration pour afficher les commandes correctives.



Si vous souhaitez mettre à jour votre configuration, spécifiez les valeurs des variables dans les commandes correctives et cliquez sur **Appliquer maintenant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Les commandes listées ici ne sont que des recommandations. Un utilisateur disposant d'un accès en lecture et écriture peut modifier n'importe quelle commande à l'aide de cette fonctionnalité. Assurez-vous d'accorder un accès privilégié limité aux utilisateurs qui, selon vous, ne doivent pas modifier les commandes.

Lorsque la commande est exécutée avec succès sur l'instance réseau, la case à cocher à côté du conseil disparaît.



Si vous souhaitez afficher les détails des commandes exécutées sur votre instance réseau, accédez à **Infrastructure > Instances >** `<Instance\_Type\>`, sélectionnez l'adresse IP de l'instance, puis cliquez sur **Afficher les événements** dans la liste déroulante **Actions**.

Sur la page **Événements**, affichez les détails de la modification de configuration.

Interroger l'audit de configuration des instances NetScaler®

NetScaler Console interroge automatiquement les audits de configuration toutes les 10 heures afin de rechercher les modifications de configuration qui se produisent sur les instances NetScaler. Vous pouvez également interroger manuellement les audits de configuration pour découvrir les modifications récentes, mais l'interrogation de la configuration de toutes les instances NetScaler impose une charge importante sur le réseau.

Au lieu d'interroger l'audit de configuration de l'instance NetScaler entière, vous pouvez interroger manuellement uniquement les audits de configuration d'une ou de plusieurs instances sélectionnées.

Pour interroger les audits de configuration des instances NetScaler :

1. Dans NetScaler Console, accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Dans **Audit de configuration**, cliquez sur **Interroger maintenant**.

   
3. La page **Interroger maintenant** s'affiche, vous donnant la possibilité d'interroger toutes les instances NetScaler du réseau ou d'interroger des instances sélectionnées.

   a. Pour interroger toutes les instances NetScaler, sélectionnez l'onglet **Toutes les instances** et cliquez sur **Démarrer l'interrogation**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Pour interroger des instances spécifiques, sélectionnez l'onglet **Sélectionner Instances**, sélectionnez les instances dans la liste, et cliquez sur **Interroger maintenant**.

Générer un diff d'audit de configuration pour les traps SNMP ConfigChange

Chaque fois qu'il y a une modification de configuration dans une instance NetScaler du réseau, le fichier de configuration est mis à jour. L'instance envoie un trap SNMP ConfigChange à NetScaler Console. Vous pouvez activer NetScaler Console pour effectuer un audit de configuration sur cette instance lorsque celle-ci envoie un trap SNMP ConfigChange.

S'il existe une différence entre la configuration du modèle d'audit et la configuration en cours d'exécution, un message d'état « Différence existante » apparaît sur la page **Rapport d'audit**. Cliquez sur le lien **Différence existante** pour accéder à la page **Différence de configuration**, où vous pouvez afficher la commande corrective. Vous pouvez utiliser ces commandes correctives pour créer une tâche de configuration et l'exécuter sur les instances NetScaler spécifiques. Lorsque vous exécutez la tâche de configuration, les instances sont ramenées à la configuration souhaitée.

Pour plus d'informations sur la création de tâches de configuration à partir de commandes correctives, consultez Comment créer des tâches de configuration à partir de commandes correctives sur NetScaler Console.

Pour exécuter des modèles d'audit de configuration lors de la réception d'un trap SNMP ConfigChange :

NetScaler Console vous permet d'activer l'option d'exécution du modèle d'audit de configuration dans NetScaler Console.

1. Dans NetScaler Console, accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Cliquez sur **Paramètres** sur la page **Audit de configuration**.
3. Sélectionnez **Effectuer un audit lors de la réception de l'événement « netScalerConfigChange »**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

NetScaler Console effectue un audit de configuration pour chaque instance qui reçoit les traps SNMP netScalerConfigChange à l'avenir.

1. Dans le champ **Délai d'exécution du modèle d'audit** (en minutes), saisissez le nombre de minutes. NetScaler Console exécute le modèle d'audit de configuration sur l'instance NetScaler après ce délai lorsqu'elle reçoit le trap SNMP ConfigChange de cette instance.

Tâches de mise à niveau

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licence (LAS) est la technologie de nouvelle génération pour les activations de produits dans l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (Citrix Platform License/Universal Hybrid Multi-Cloud), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler compatibles avec LAS sont :

- NetScaler ADCs : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à compter du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version

© 1997–2026 Citrix Systems, Inc. All rights reserved.

14.1-51.x ou ultérieure de Console sur site et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées, telles que les licences NetScaler virtual CPU (Pooled vCPU), NetScaler VPX Check-In et Check-Out (CICO), perpétuelles, ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Vous pouvez créer les tâches de maintenance suivantes à l'aide de NetScaler Console. Vous pouvez ensuite planifier les tâches de maintenance à une date et une heure spécifiques.

- Mettre à niveau les instances NetScaler
- Mettre à niveau les instances NetScaler SDX
- Mettre à niveau les instances NetScaler BLX
- Mettre à niveau les instances NetScaler dans le groupe de mise à l'échelle automatique
- Configurer une paire HA d'instances NetScaler
- Convertir une paire HA d'instances en cluster

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Si une tâche de mise à niveau échoue, NetScaler Console supprime les fichiers de build et les autres fichiers extraits pour s'assurer que les instances NetScaler disposent de suffisamment d'espace disque pour la prochaine tentative de mise à niveau.
- Bien que vous puissiez sélectionner n'importe quel nombre d'instances NetScaler pour la mise à niveau, NetScaler Console sur site prend en charge un maximum de 40 threads de mise à niveau simultanés. Cela signifie que seules 40 instances peuvent être mises à niveau simultanément.
- Les transitions des builds non-FIPS vers les builds FIPS et les mises à niveau directes de version qui ignorent les mises à niveau séquentielles (par exemple, de la version 13.0 à 14.1) ne sont pas prises en charge. Ces restrictions sont nécessaires en raison des différences architecturales entre les types de builds et des changements incrémentiels requis entre les versions majeures. Pour garantir une mise à niveau réussie, vous devez soit déployer un nouveau build FIPS, soit suivre le chemin de mise à niveau séquentiel pris en charge à travers toutes les versions intermédiaires.

Validation avant la mise à niveau

Lors d'une tâche de mise à niveau NetScaler, NetScaler Console effectue les validations suivantes :

- Vérifications avant la mise à niveau effectuées par NetScaler Console
- Vérifications avant la mise à niveau effectuées par NetScaler (pris en charge à partir de NetScaler 14.1-66.x)

Les résultats des deux sources sont consolidés et présentés dans une seule réponse pour guider les décisions de mise à niveau. Aucune configuration supplémentaire n'est requise pour activer les vérifications avant la mise à niveau effectuées par NetScaler ou NetScaler Console. La validation avant la mise à niveau offre les avantages suivants :

- Confiance et sécurité améliorées pendant les mises à niveau
- Détection précoce des problèmes bloquants avant le début de la mise à niveau
- Expérience de pré-vérification cohérente sur toutes les versions de NetScaler prises en charge

Vérifications avant la mise à niveau effectuées par NetScaler Console

NetScaler Console effectue les vérifications suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Disponibilité de l'espace disque sur `/var`** : Vérifie qu'un espace libre suffisant est disponible sur la partition `/var` pour effectuer en toute sécurité les opérations d'extraction d'image et d'installation.
- **Disponibilité de l'espace disque sur /flash** : Vérifie que la partition `/flash` dispose de l'espace disque libre minimal requis pour prendre en charge les opérations système essentielles pendant l'installation.
- **Vérification de la configuration NSPEPI** : Valide le fichier de configuration NetScaler pour les politiques non prises en charge ou non valides afin d'éviter les erreurs de configuration après l'installation ou la mise à niveau.
- **Vérification de la configuration de la haute disponibilité (HA)** : Vérifie l'état HA et la cohérence des rôles pour garantir une configuration HA saine et prise en charge.
- **Vérification de la connectivité SSH** : Confirme l'accessibilité SSH, la validation de la confiance et la connectivité aux périphériques cibles requises pour les opérations d'installation et de gestion à distance.
- **Correspondance ns.conf pour la rétrogradation** : Garantit qu'un `ns.conf file` approprié et compatible est disponible pour les scénarios de rétrogradation afin d'éviter l'incompatibilité de configuration.

Tous les résultats de pré-vérification sont classés uniformément comme suit :

- **Critique (Bloquant)** : La mise à niveau est bloquée. Tous les problèmes signalés doivent être résolus avant de poursuivre.
- **Avertissement** : La mise à niveau peut se poursuivre avec l'approbation de l'administrateur.
- **Avis** : La mise à niveau peut se poursuivre avec l'approbation de l'administrateur.

Vérifications avant la mise à niveau effectuées par NetScaler

Pour des informations détaillées sur les vérifications avant la mise à niveau effectuées par NetScaler, consultez Vérifications de validation avant la mise à niveau pour NetScaler.

Planifier la mise à niveau des instances NetScaler

1. Accédez à **Infrastructure > Tâches de mise à niveau**. Cliquez sur **Créer une tâche**.

   Créer une tâche de maintenance (/en-us/netscaler-application-delivery-management-software/media/upgrade-1-m.png)

2. Dans **Créer des tâches de maintenance**, sélectionnez **Mettre à niveau NetScaler (autonome/haute disponibilité/cluster)** et cliquez sur **Continuer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sélectionner une tâche de maintenance de mise à niveau (/en-us/netscaler-application-delivery-management-software/media/upgrade-2.png)

3. Dans **Sélectionner une instance**, saisissez un nom de votre choix pour **Nom de la tâche**.
4. Cliquez sur **Ajouter des instances** pour ajouter les instances NetScaler que vous souhaitez mettre à niveau.

   - Pour mettre à niveau une paire HA, spécifiez l'adresse IP d'un nœud principal ou secondaire. Cependant, il est recommandé d'utiliser l'instance principale pour mettre à niveau la paire HA.
   - Pour mettre à niveau un cluster, spécifiez l'adresse IP du cluster.

   Ajouter des instances à la tâche de maintenance de mise à niveau (/en-us/netscaler-application-delivery-management-software/media/upgrade-3-m.png)

5. Cliquez sur **Suivant** pour sélectionner l'image. Sélectionnez l'une des options suivantes dans la liste **Image logicielle** :

   - **Local** - Sélectionnez le fichier de mise à niveau de l'instance depuis votre machine locale.
   - **Appliance** - Sélectionnez le fichier de mise à niveau de l'instance à partir du navigateur de fichiers de NetScaler Console. L'interface graphique de NetScaler Console affiche les fichiers d'instance présents à `/var/mps/mps_images`.

     - **Ignorer le téléchargement de l'image vers NetScaler si l'image sélectionnée est déjà disponible** - Sélectionnez cette option si l'image est déjà présente dans l'instance NetScaler.
     - **Nettoyer l'image logicielle de NetScaler après une mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Si les instances sélectionnées sont déjà sur la version cible, un avertissement s'affiche. Cet avertissement permet d'éviter la sélection d'instances incorrectes lors des tâches de mise à niveau. Si vous avez l'intention de mettre à niveau les instances à nouveau, ignorez l'avertissement et poursuivez la mise à niveau.

  

- Si une tâche de mise à niveau est déjà planifiée pour l'instance sélectionnée, NetScaler Console affiche un message d'avertissement. Ce message d'avertissement permet d'éviter de planifier involontairement des tâches de mise à niveau en double sur la même instance NetScaler.

6. Cliquez sur **Suivant** pour démarrer la validation préalable à la mise à niveau sur les instances sélectionnées.

   L'onglet **Validation préalable à la mise à niveau** affiche les instances ayant échoué. Supprimez les instances ayant échoué et cliquez sur **Suivant**.

   IMPORTANT

   Si vous spécifiez l'adresse IP du cluster, NetScaler Console effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

7. Facultatif, dans **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes :

   - **Importer des commandes à partir d'un fichier** - Sélectionnez le fichier d'entrée de commande depuis votre ordinateur local.
   - **Saisir des commandes** - Saisissez les commandes directement sur l'interface graphique.

     

   Vous pouvez utiliser des scripts personnalisés pour vérifier les modifications avant et après une mise à niveau d'instance. Par exemple :

   - La version de l'instance avant et après la mise à niveau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'état des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
- Les statistiques des serveurs virtuels et des services.
- Les routes dynamiques.

8. Cliquez sur **Suivant**. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mettre à niveau maintenant** - La tâche de mise à niveau s'exécute immédiatement.
   - **Planifier ultérieurement** - Sélectionnez cette option pour exécuter cette tâche de mise à niveau plus tard. Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau les instances.

     Si vous souhaitez mettre à niveau une paire HA NetScaler en deux étapes, sélectionnez **Effectuer une mise à niveau en deux étapes pour les nœuds en HA**.

     Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau une autre instance de la paire HA.

9. Cliquez sur **Suivant**. Dans **Créer une tâche**, spécifiez les détails suivants :

   a. Spécifiez quand vous souhaitez télécharger l'image vers une instance :

      - **Télécharger maintenant** - Sélectionnez cette option pour télécharger l'image immédiatement. Cependant, la tâche de mise à niveau s'exécute à l'heure prévue.
      - **Télécharger au moment de l'exécution** - Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.
      - **Sauvegarder les instances NetScaler avant de commencer la mise à niveau.** - Crée une sauvegarde des instances NetScaler sélectionnées.
      - **Enregistre la configuration NetScaler avant de commencer la mise à niveau** - Enregistre les tâches de configuration qui sont configurées sur l'instance avant la mise à niveau.
      - **Activer ISSU pour éviter une interruption du réseau sur une paire HA NetScaler** - L'activation de la mise à niveau logicielle en service (ISSU) vous permet de mettre à niveau une paire NetScaler haute disponibilité (HA) sans provoquer d'interruption du réseau. ISSU garantit que les connexions existantes sont respectées pendant la mise à niveau en migrant les sessions actives de manière transparente entre les nœuds. Après avoir activé ISSU dans le flux de travail de mise à niveau, le système peut également déclencher l'achèvement de la migration ISSU après le délai défini par le client. Le déclenchement par NetScaler Console d'un achèvement complet de la migration ISSU

© 1997–2026 Citrix Systems, Inc. All rights reserved.

garantit que la mise à niveau se termine même si les connexions persistent. Spécifiez le délai d'expiration de la migration ISSU en minutes pour définir le temps d'attente avant que NetScaler Console ne termine la migration.

- **NetScaler Console Service Connect** - Si vous effectuez une mise à niveau vers la version **13.0-64 ou ultérieure** et **12.1-58 ou ultérieure**, NetScaler Console Service Connect est activé automatiquement. Pour plus d'informations, consultez Intégration simplifiée des instances NetScaler à l'aide de NetScaler Console Service Connect.
- **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, consultez Créer une liste de distribution d'e-mails.
- **Recevoir le rapport d'exécution par Slack** - Envoie le rapport d'exécution par Slack. Pour ajouter un profil Slack, consultez Créer un profil Slack.



10. Cliquez sur **Créer une tâche**.

Planifier la mise à niveau des instances NetScaler SDX

1. Accédez à **Infrastructure > Tâches de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Mettre à niveau NetScaler SDX** et cliquez sur **Continuer**.
3. Sur la page **Mettre à niveau NetScaler SDX**, dans l'onglet **Sélection d'instance** :
   a. Ajoutez un **Nom de tâche**.
   b. Dans la liste **Image logicielle**, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de build doit être présent sur l'appliance virtuelle NetScaler Console).

      Le processus de téléchargement commence.
   c. Ajoutez les instances NetScaler SDX sur lesquelles vous souhaitez exécuter le processus de mise à niveau.
   d. Cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance NetScaler SDX maintenant, puis cliquez sur **Terminer**.
5. Pour mettre à niveau une instance NetScaler SDX ultérieurement, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début pour la mise à niveau de l'instance NetScaler, puis cliquez sur **Terminer**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Vous pouvez également activer les notifications par e-mail et Slack pour recevoir le rapport d'exécution de l'instance NetScaler SDX en cours de mise à niveau. Cochez la case **Recevoir le rapport d'exécution par e-mail** et la case **Recevoir le rapport d'exécution par Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution d'e-mails et du canal Slack, consultez l'**étape 8** dans Planifier la mise à niveau des instances NetScaler

Planifier la mise à niveau des instances NetScaler BLX

1. Accédez à **Infrastructure > Tâches de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Dans **Créer des tâches de maintenance**, sélectionnez **Mettre à niveau NetScaler BLX** et cliquez sur **Continuer**.
3. Dans **Sélectionner l'instance**, saisissez un nom de votre choix pour **Nom de la tâche**.
4. Cliquez sur **Ajouter des instances** pour ajouter les instances BLX que vous souhaitez mettre à niveau.

   - Pour mettre à niveau une paire HA, spécifiez l'adresse IP d'un nœud principal ou secondaire. Cependant, il est recommandé d'utiliser l'instance principale pour mettre à niveau la paire HA.
   - Pour mettre à niveau un cluster, spécifiez l'adresse IP du cluster.

5. Cliquez sur **Suivant** pour sélectionner l'image. Sélectionnez l'une des options suivantes dans la liste **Image logicielle** :

   - **Local** - Sélectionnez le fichier de mise à niveau de l'instance à partir de votre machine locale.
   - **Appliance** - Sélectionnez le fichier de mise à niveau de l'instance à partir de l'explorateur de fichiers de NetScaler Console. L'interface graphique de NetScaler Console affiche les fichiers d'instance qui sont présents à `/var/mps/mps_images`.
     - **Ignorer le téléchargement de l'image vers NetScaler si l'image sélectionnée est déjà disponible** - Sélectionnez cette option si l'image est déjà présente dans l'instance NetScaler.
     - **Nettoyer l'image logicielle de NetScaler après une mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Cliquez sur **Suivant** pour démarrer la validation préalable à la mise à niveau sur les instances sélectionnées.

   L'onglet **Validation avant la mise à niveau** affiche les instances ayant échoué. Supprimez les instances ayant échoué et cliquez sur **Suivant**.

   IMPORTANT

   Si vous spécifiez l'adresse IP du cluster, NetScaler Console effectue la validation avant la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

7. Facultatif, dans **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après la mise à niveau d'une instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes :

   - **Importer des commandes depuis un fichier** - Sélectionnez le fichier d'entrée de commande depuis votre ordinateur local.
   - **Saisir des commandes** - Saisissez les commandes directement dans l'interface graphique.

   

   Vous pouvez utiliser des scripts personnalisés pour vérifier les modifications avant et après la mise à niveau d'une instance. Par exemple :

   - La version de l'instance avant et après la mise à niveau.
   - L'état des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
   - Les statistiques des serveurs virtuels et des services.
   - Les routes dynamiques.

8. Cliquez sur **Suivant**. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mettre à niveau maintenant** - La tâche de mise à niveau s'exécute immédiatement.
   - **Planifier ultérieurement** - Sélectionnez cette option pour exécuter cette tâche de mise à niveau plus tard. Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau les instances.

     Si vous souhaitez mettre à niveau une paire HA en deux étapes, sélectionnez **Effectuer une mise à niveau en deux étapes pour les nœuds en HA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau une autre instance de la paire HA.

9. Cliquez sur **Suivant**. Dans **Créer une tâche**, spécifiez les détails suivants :

   a. Spécifiez quand vous souhaitez télécharger l'image vers une instance :

      - **Télécharger maintenant** - Sélectionnez cette option pour télécharger l'image immédiatement. Cependant, la tâche de mise à niveau s'exécute à l'heure prévue.
      - **Télécharger au moment de l'exécution** - Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.
      - **Sauvegarder les instances NetScaler avant de commencer la mise à niveau** - Crée une sauvegarde des instances NetScaler sélectionnées.
      - **Enregistrer la configuration NetScaler avant de commencer la mise à niveau** - Enregistre les tâches de configuration configurées sur l'instance avant la mise à niveau.
      - **Activer ISSU pour éviter les pannes réseau sur la paire HA NetScaler** - L'activation de la mise à niveau logicielle en service (ISSU) vous permet de mettre à niveau une paire NetScaler haute disponibilité (HA) sans provoquer d'interruption du réseau. ISSU garantit que les connexions existantes sont respectées pendant la mise à niveau en migrant les sessions actives de manière transparente entre les nœuds. Après avoir activé ISSU dans le flux de travail de mise à niveau, le système peut également déclencher l'achèvement de la migration ISSU après le délai défini par le client. Le déclenchement par NetScaler Console d'un achèvement complet de la migration ISSU garantit que la mise à niveau se termine même si les connexions persistent. Spécifiez le délai d'expiration de la migration ISSU en minutes pour définir le temps d'attente avant que NetScaler Console ne termine la migration.

   - **NetScaler Console Service Connect** - Si vous effectuez une mise à niveau vers la version **13.0-64 ou ultérieure** et **12.1-58 ou ultérieure**, NetScaler Console Service Connect est activé automatiquement. Pour plus d'informations, consultez Intégration simplifiée des instances NetScaler à l'aide de NetScaler Console Service Connect.
   - **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, consultez Créer une liste de distribution d'e-mails.
   - **Recevoir le rapport d'exécution via Slack** - Envoie le rapport d'exécution dans Slack. Pour ajouter un profil Slack, consultez Créer un profil Slack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Cliquez sur **Créer une tâche**.

Planifier la mise à niveau du groupe Autoscale™

Effectuez les étapes suivantes pour mettre à niveau toutes les instances des services cloud qui font partie du groupe Autoscale :

1. Accédez à **Infrastructure > Tâches de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Mettre à niveau le groupe Autoscale** et cliquez sur **Continuer**.
3. Dans l'onglet **Paramètres de mise à niveau** :
    a. Sélectionnez le **groupe Autoscale** que vous souhaitez mettre à niveau.
    b. Dans **Image**, sélectionnez la version de NetScaler. Cette image est la version existante des instances NetScaler dans le groupe Autoscale.
    c. Dans **Image NetScaler**, parcourez le fichier de version NetScaler vers lequel vous souhaitez effectuer la mise à niveau.

       Si vous cochez **Mise à niveau progressive**, la tâche de mise à niveau attend l'expiration de la période de drainage des connexions spécifiée.
    d. Cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche** :
    a. Sélectionnez l'une des options suivantes dans la liste Mode d'exécution :
        - **Maintenant :** Pour démarrer la mise à niveau des instances NetScaler immédiatement.
        - **Plus tard :** Pour démarrer la mise à niveau des instances NetScaler ultérieurement.
    b. Si vous sélectionnez l'option **Plus tard**, sélectionnez la date d'exécution et l'heure de début auxquelles vous souhaitez démarrer la tâche de mise à niveau.

    Vous pouvez également activer les notifications par e-mail et Slack pour recevoir le rapport d'exécution du groupe Autoscale en cours de mise à niveau. Cochez la case **Recevoir le rapport d'exécution par e-mail** et la case **Recevoir le rapport d'exécution via Slack** pour activer les notifications.
5. Cliquez sur **Terminer**.

Planifier la configuration d'une paire HA d'instances NetScaler

1. Accédez à **Infrastructure > Upgrade Jobs**. Cliquez sur **Créer une tâche**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sélectionnez **Configurer une paire HA d'instances NetScaler** et cliquez sur **Continuer**.
3. Sur la page **Paire HA NetScaler**, dans l'onglet **Sélection d'instance** :

   a. Ajoutez un **Nom de la tâche**.

   b. Sélectionnez l'adresse IP principale.

   c. Saisissez le mot de passe du nœud RPC principal.

   d. Sélectionnez l'adresse IP secondaire.

   REMARQUE :

   Les champs de mot de passe du nœud RPC sont disponibles dans la version 14.1 de NetScaler et les versions ultérieures.

   e. Saisissez le mot de passe du nœud RPC secondaire.

   f. Cliquez pour activer **Activer le mode INC (configuration réseau indépendante)** si les instances de la paire HA se trouvent dans deux sous-réseaux.

4. Dans l'onglet **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mettre à niveau maintenant** : Sélectionnez cette option pour mettre à niveau une instance NetScaler immédiatement. Cliquez sur **Terminer**.
   - **Planifier ultérieurement** : Sélectionnez cette option pour mettre à niveau une paire HA NetScaler ultérieurement.

5. Si vous sélectionnez l'option **Planifier ultérieurement**, choisissez la **Date d'exécution** et l'**Heure de début** pour la mise à niveau de l'instance NetScaler.

   a. Sélectionnez **Effectuer la mise à niveau des nœuds HA NetScaler en deux étapes**. Lorsque vous sélectionnez cette option, la synchronisation HA et la propagation HA sont désactivées jusqu'à ce que les deux nœuds soient mis à niveau avec succès.

   b. Sélectionnez l'une des options suivantes pour planifier la mise à niveau du nœud secondaire. Avec cette option, la mise à niveau de l'étape 2 n'est exécutée qu'après la réussite de l'étape 1.

      - **Après un délai défini** : Spécifiez un délai (en heures) après la fin de la mise à niveau du premier nœud avant le début de la mise à niveau du second nœud.
      - **À une heure spécifique** : Choisissez une date et une heure pour la mise à niveau du nœud secondaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Sélectionnez **Retarder le basculement HA jusqu'au début de la mise à niveau du nœud secondaire**. Cliquez sur **Suivant**.
7. Dans l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance NetScaler maintenant, puis cliquez sur **Terminer**.

   
8. Vous pouvez également activer les notifications par e-mail et Slack pour recevoir le rapport d'exécution de la création de la paire HA NetScaler. Cochez la case **Recevoir le rapport d'exécution par e-mail** et la case **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution d'e-mails et du canal Slack, consultez l'**étape 8** dans Planifier la mise à niveau des instances NetScaler

Planifier la conversion d'une paire d'instances HA en cluster

1. Accédez à **Infrastructure > Tâches de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Convertir une paire d'instances HA en cluster à 2 nœuds** et cliquez sur **Continuer**.
3. Sur la page **Migrer NetScaler HA vers un cluster**, dans l'onglet **Sélection d'instance**, ajoutez un **Nom de tâche**. Spécifiez l'adresse IP principale, l'adresse IP secondaire, l'ID du nœud principal, l'ID du nœud secondaire, l'adresse IP du cluster, l'ID du cluster et le fond de panier, puis cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance NetScaler immédiatement, puis cliquez sur **Terminer**.
5. Pour mettre à niveau ultérieurement, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la **Date d'exécution** et l'**Heure de début** pour la mise à niveau de l'instance de paire HA NetScaler, puis cliquez sur **Terminer**.
6. Vous pouvez également activer les notifications par e-mail et Slack pour recevoir le rapport d'exécution de la mise à niveau d'une instance NetScaler SDX. Cochez la case **Recevoir le rapport d'exécution par e-mail** et la case **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution d'e-mails et du canal Slack, consultez l'**étape 8** dans Planifier la mise à niveau des instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser les tâches pour mettre à niveau les instances NetScaler®

Vous pouvez utiliser NetScaler Console pour mettre à niveau une ou plusieurs instances NetScaler. Vous devez connaître le cadre de licences et les types de licences avant de mettre à niveau une instance.

REMARQUE : Si vous souhaitez mettre à niveau une instance qui utilise des stratégies classiques, nous vous recommandons de convertir les stratégies classiques en stratégies avancées avant de mettre à niveau l'instance, à l'aide de l'outil NSPEPI. Ceci s'applique aux fonctionnalités prises en charge par l'outil NSPEPI. Pour plus d'informations, consultez Considérations relatives à la mise à niveau pour les configurations avec des stratégies classiques.

Lorsque vous mettez à niveau votre instance NetScaler en créant une tâche de maintenance, effectuez la vérification de pré-validation sur les instances que vous souhaitez mettre à niveau.

Vérifications de pré-validation

1. **Vérifier les personnalisations** - Sauvegardez vos personnalisations et supprimez-les des instances. Vous pouvez réappliquer les personnalisations sauvegardées après la mise à niveau de l'instance.
2. **Vérifier l'utilisation du disque** - Si le dossier `/var` a moins de 6 Go d'espace et que le dossier `/flash` a moins de 200 Mo d'espace, libérez de l'espace disque. Vérifiez les chemins de dossier suivants pour libérer de l'espace disque :
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **Vérifier les problèmes matériels du disque** - Résolvez les problèmes matériels, le cas échéant.
4. **Vérifier les nœuds STAYPRIMARY et STAYSECONDARY** - Pour un NetScaler HA, la mise à niveau est bloquée pour les nœuds dans les états STAYPRIMARY et STAYSECONDARY. Ces

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nœuds sont identifiés lors de la vérification de pré-validation et répertoriés sous **Instances bloquées de la mise à niveau**.

Paire haute disponibilité NetScaler

Lorsque vous mettez à niveau une paire HA NetScaler, notez les points suivants :

- Le nœud secondaire est mis à niveau en premier.
- La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient mis à niveau avec succès.
- Après la mise à niveau réussie de la paire HA, un message d'erreur apparaît dans l'historique d'exécution. Ce message apparaît si vos nœuds de la paire HA sont sur des builds ou des versions différentes. Ce message indique que la synchronisation entre le nœud principal et le nœud secondaire est désactivée.

Vous pouvez mettre à niveau une paire HA NetScaler en deux étapes :

1. Créez une tâche de mise à niveau et exécutez-la immédiatement sur l'un des nœuds ou planifiez-la pour plus tard.
2. Planifiez l'exécution de la tâche de mise à niveau sur le nœud restant ultérieurement. Assurez-vous de planifier cette tâche après la mise à niveau du nœud initial.

Clusters NetScaler

Lorsque vous mettez à niveau un cluster NetScaler, la console NetScaler effectue une validation avant la mise à niveau uniquement sur l'instance spécifiée. Avant de procéder à la mise à niveau, vérifiez et résolvez les problèmes de personnalisation, d'utilisation du disque et de matériel sur les nœuds du cluster.

Créer une tâche de maintenance de mise à niveau pour mettre à niveau les instances NetScaler

REMARQUE

La mise à niveau de NetScaler d'une version supérieure vers une version inférieure n'est pas prise en charge. Par exemple, si votre instance NetScaler est 13.0 82.x, vous ne pouvez pas rétrograder l'instance NetScaler vers 13.0 79.x ou toute autre version antérieure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans NetScaler Console, accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur le bouton **Créer un travail**.
2. Dans **Créer des travaux de maintenance**, sélectionnez **Mettre à niveau NetScaler (autonome/haute disponibilité/cluster)** et cliquez sur **Continuer**.

   
3. Dans **Sélectionner l'instance**, tapez un nom de votre choix pour **Nom du travail**.
4. Cliquez sur **Ajouter des instances** pour ajouter les instances NetScaler que vous souhaitez mettre à niveau.

   - Pour mettre à niveau une paire haute disponibilité NetScaler, sélectionnez les adresses IP de la paire haute disponibilité (indiquées par l'exposant 'S' et 'P').
   - Pour mettre à niveau un cluster, sélectionnez l'adresse IP du cluster (indiquée par l'exposant 'C').

   
5. Dans l'onglet **Sélectionner l'image**, sélectionnez une image NetScaler à partir de votre lecteur local ou des images de build.

   - **Local** - Sélectionnez le fichier de mise à niveau de l'instance à partir de votre machine locale.
   - **Appliance** - Sélectionnez le fichier de mise à niveau de l'instance à partir d'un explorateur de fichiers NetScaler Console. L'interface graphique de NetScaler Console affiche les fichiers d'instance qui sont présents à `/var/mps/ns_images`.

   

   - **Ignorer le téléchargement de l'image vers NetScaler si l'image sélectionnée est déjà disponible** - Cette option vérifie si l'image sélectionnée est disponible dans NetScaler. Le travail de mise à niveau ignore le téléchargement d'une nouvelle image et utilise l'image disponible dans NetScaler.
   - **Nettoyer l'image logicielle de NetScaler après une mise à niveau réussie** - Cette option efface l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.

   Cliquez sur **Suivant** pour démarrer la validation préalable à la mise à niveau sur les instances sélectionnées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Les images NetScaler téléchargées sont stockées dans l'agent NetScaler Console et sont présentes dans `/var/mps/adcimages`. Ces images mises en cache peuvent être utilisées pour plusieurs mises à niveau NetScaler, éliminant ainsi la nécessité de télécharger une image à chaque fois pour une mise à niveau.
- NetScaler Console efface les images NetScaler mises en cache tous les trois jours en fonction de la dernière heure de modification des images. Seuls les deux derniers fichiers image sont mis en cache dans l'agent NetScaler Console à la fois.

6. L'onglet **Validation préalable à la mise à niveau** affiche les sections suivantes :

   - **Instances prêtes pour la mise à niveau**. Vous pouvez poursuivre la mise à niveau de ces instances.
   - **Instances bloquées pour la mise à niveau**. Ces instances NetScaler sont bloquées pour la mise à niveau en raison d'erreurs de validation préalable à la mise à niveau.

     Vous pouvez examiner, corriger les erreurs, puis cliquer sur **Déplacer vers Prêt pour la mise à niveau** pour les mettre à niveau. Si vous rencontrez un espace disque insuffisant sur une instance, vous pouvez vérifier et nettoyer l'espace disque. Voir, Nettoyer l'espace disque NetScaler.

   

   - **Vérification des politiques** : Si NetScaler Console détecte des politiques classiques non prises en charge, vous pouvez supprimer ces politiques pour créer une tâche de mise à niveau.

IMPORTANT :

Si vous spécifiez l'adresse IP du cluster, NetScaler Console effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

Pour afficher les écarts entre les nœuds primaire et secondaire lors d'une mise à niveau, sélectionnez le nœud haute disponibilité, puis cliquez sur **Détails**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Écarts de configuration trouvés dans le nœud principal de la haute disponibilité** - Affiche toutes les configurations trouvées dans le nœud secondaire de la paire haute disponibilité NetScaler mais manquantes dans le nœud principal.
- **Écarts de configuration trouvés dans le nœud secondaire de la haute disponibilité** - Affiche toutes les configurations trouvées dans le nœud principal de la paire haute disponibilité NetScaler mais manquantes dans le nœud secondaire.

REMARQUE :

Vous pouvez ignorer les écarts suivants qui peuvent apparaître dans les sections des écarts de configuration :

- Configurations spécifiques à l'appareil, telles que les adresses IP.
- Mots de passe ou certificats chiffrés, qui peuvent différer entre les nœuds, même si le mot de passe est le même.

Vous pouvez examiner les écarts et choisir de les ignorer s'ils ne sont pas pertinents.

7. Dans **Scripts de validation**, spécifiez les scripts à exécuter avant et après la mise à niveau d'une instance. Vous pouvez effectuer l'une des opérations suivantes :

   - **Scripts de validation par défaut** - Choisissez cette option pour exécuter les scripts de validation prédéfinis. Ces scripts sont exécutés avant et après la tâche de mise à niveau, générant un rapport de différence pour le script de validation.

     REMARQUE :

     Vous ne pouvez pas modifier ou éditer cet ensemble de commandes prédéfini.

   - **Scripts de validation personnalisés** - Choisissez cette option pour exécuter votre script de validation. Vous pouvez spécifier si vous souhaitez que les scripts soient exécutés avant ou après la mise à niveau. Un rapport de différences n'est généré que si les mêmes scripts sont sélectionnés avant et après la mise à niveau.

   Pour connaître l'ensemble des commandes dans chaque configuration, cliquez sur **Afficher les détails**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans **Scripts de validation personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes CLI NetScaler :

Les scripts personnalisés sont utilisés pour vérifier les modifications avant et après une mise à niveau d'instance NetScaler. Par exemple :

- La version de l'instance avant et après la mise à niveau.
- L'état des interfaces, des nœuds de haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
- Les statistiques des serveurs virtuels et des services.
- Les routes dynamiques.

Une mise à niveau d'instance comporte plusieurs étapes. Vous pouvez maintenant spécifier ces scripts à exécuter aux étapes suivantes :

- **Pré-mise à niveau** : Le script spécifié s'exécute avant la mise à niveau d'une instance.
- **Post-mise à niveau pré-basculement (applicable pour HA)** : Cette étape s'applique uniquement au déploiement de haute disponibilité. Le script spécifié s'exécute après la mise à niveau des nœuds, mais avant leur basculement.
- **Post-mise à niveau (applicable pour autonome) / Post-mise à niveau post-basculement (applicable pour HA)** : Le script spécifié s'exécute après la mise à niveau d'une instance dans le déploiement autonome. Dans le déploiement de haute disponibilité, le script s'exécute après la mise à niveau des nœuds et leur basculement.

REMARQUE :

Assurez-vous d'activer l'exécution des scripts aux étapes requises. Sinon, les scripts spécifiés ne s'exécutent pas.

Vous pouvez importer un fichier de script ou taper directement les commandes CLI NetScaler dans l'interface graphique de NetScaler Console.

- **Utiliser le même script que la pré-mise à niveau** : Utilisez le même script personnalisé pour la pré-mise à niveau, le pré-basculement et la post-mise à niveau.
- **Importer des commandes depuis un fichier** : Sélectionnez le fichier d'entrée de commande CLI NetScaler depuis votre ordinateur local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Saisir les commandes** : Saisissez les commandes CLI NetScaler directement sur l'interface graphique.

8. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mettre à niveau maintenant** - La tâche de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** - Sélectionnez cette option pour exécuter cette tâche de mise à niveau ultérieurement. Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau les instances.

     Si vous souhaitez mettre à niveau une paire HA NetScaler en deux étapes, sélectionnez **Effectuer une mise à niveau en deux étapes pour les nœuds en HA**.

     Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau une autre instance de la paire HA.

     

9. Dans **Créer une tâche**, spécifiez les détails suivants :

   a. Sélectionnez l'une des options suivantes dans la liste **Image logicielle** :

      - **Local** - Sélectionnez le fichier de mise à niveau de l'instance depuis votre machine locale.
      - **Appliance** - Sélectionnez le fichier de mise à niveau de l'instance à partir d'un explorateur de fichiers. L'interface graphique de NetScaler Console affiche les fichiers d'instance qui se trouvent à `/var/mps/mps_images`.

   b. Spécifiez quand vous souhaitez télécharger l'image vers une instance :

      - **Télécharger maintenant** - Sélectionnez cette option pour télécharger l'image immédiatement. Cependant, la tâche de mise à niveau s'exécute à l'heure prévue.
      - **Télécharger au moment de l'exécution** - Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.

     Pour une paire haute disponibilité, vous pouvez spécifier les nœuds sur lesquels vous souhaitez télécharger l'image :

      - **Télécharger vers les nœuds principal et secondaire** : Téléchargez le fichier image de build vers les nœuds principal et secondaire.
      - **Télécharger vers le nœud secondaire uniquement** : Téléchargez le fichier image de build uniquement vers le nœud secondaire. Une fois le nœud secondaire mis à niveau,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

un basculement se produit et le fichier image de build est téléchargé vers le nouveau nœud secondaire qui était auparavant le nœud principal.

Pour plus d'informations sur les scénarios de planification disponibles pour une paire haute disponibilité, consultez Planification des tâches de mise à niveau pour une paire haute disponibilité.

- **Nettoyer l'image logicielle de NetScaler après une mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.
- **Sauvegarder les instances NetScaler avant de commencer la mise à niveau.** - Crée une sauvegarde des instances NetScaler sélectionnées.
- **Maintenir le statut principal et secondaire des nœuds HA après la mise à niveau** : Sélectionnez cette option si vous souhaitez que la tâche de mise à niveau démarre un basculement après la mise à niveau de chaque nœud. De cette façon, la tâche de mise à niveau maintient le statut principal et secondaire des nœuds.
- **Enregistrer la configuration NetScaler avant de commencer la mise à niveau** - Enregistre la configuration NetScaler en cours d'exécution avant de mettre à niveau les instances NetScaler.
- **Activer ISSU pour éviter les pannes réseau sur une paire HA NetScaler** - ISSU garantit une mise à niveau sans interruption sur une paire haute disponibilité NetScaler. Cette option offre une fonctionnalité de migration qui respecte les connexions existantes pendant la mise à niveau. Ainsi, vous pouvez mettre à niveau une paire HA NetScaler sans temps d'arrêt. Spécifiez le délai d'expiration de la migration ISSU en minutes.
- **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, consultez Créer une liste de distribution d'e-mails.
- **Recevoir le rapport d'exécution via Slack** - Envoie le rapport d'exécution via Slack. Pour ajouter un profil Slack, consultez Créer un profil Slack.

Cliquez sur **Créer une tâche**.

La tâche de mise à niveau apparaît dans **Infrastructure > Tâches de mise à niveau**. Lorsque vous modifiez une tâche existante, vous pouvez passer à n'importe quel onglet si les champs requis sont déjà remplis. Par exemple, si vous êtes dans l'onglet **Sélectionner la configuration**, vous pouvez passer à l'onglet **Aperçu de la tâche**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Suspendre ou reprendre une tâche de mise à niveau planifiée

Vous pouvez également suspendre votre tâche de mise à niveau planifiée.

Pour utiliser cette fonctionnalité, accédez à **Infrastructure > Tâches de mise à niveau**, sélectionnez une tâche de mise à niveau planifiée existante, puis cliquez sur **Arrêter** pour suspendre la tâche. Pour reprendre la tâche de mise à niveau planifiée, cliquez sur **Reprendre**.



REMARQUE :

Si l'heure planifiée pour la tâche de mise à niveau est dépassée après que vous ayez décidé de la reprendre, vous devez créer à nouveau la tâche de mise à niveau.

Relancer les tâches de mise à niveau ayant échoué

1. Dans **Infrastructure > Tâches de mise à niveau**, sélectionnez la tâche de mise à niveau ayant échoué et cliquez sur **Relancer**. Vous pouvez également accéder à **Sélectionner une action > Relancer la tâche de mise à niveau** pour relancer une tâche ayant échoué.

   

2. Dans **Sélectionner une instance**, spécifiez les détails suivants :

   - **Nom de la tâche** - Saisissez un nom pour la mise à niveau.
   - Sélectionnez les instances NetScaler que vous souhaitez mettre à niveau dans la liste. Pour supprimer des instances, cliquez sur **Supprimer**.

   Cliquez sur **Suivant** pour lancer le processus de validation.

   

3. L'onglet **Validation avant la mise à niveau** affiche les sections suivantes :

   - **Instances prêtes pour la mise à niveau**. Vous pouvez poursuivre la mise à niveau de ces instances.
   - **Instances bloquées pour la mise à niveau**. Ces instances NetScaler sont bloquées pour la mise à niveau en raison d'erreurs de validation avant la mise à niveau.

     Vous pouvez examiner, corriger les erreurs, puis cliquer sur **Passer à prêt pour la mise à niveau** pour les mettre à niveau. Si vous rencontrez un espace disque insuffisant sur une instance, vous pouvez vérifier et nettoyer l'espace disque. Voir, Nettoyer l'espace disque NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Vérification de la politique** : Si NetScaler Console détecte des politiques classiques non prises en charge, vous pouvez supprimer ces politiques pour créer une tâche de mise à niveau.



Cliquez sur **Suivant**.

4. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mettre à niveau maintenant** : La tâche de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** : Sélectionnez cette option pour exécuter cette tâche de mise à niveau ultérieurement. Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau les instances.

   

   Cliquez sur **Réessayer**.

Nettoyer l'espace disque NetScaler

Si vous rencontrez un problème d'espace disque insuffisant lors de la mise à niveau d'une instance NetScaler, nettoyez l'espace disque directement depuis l'interface graphique de NetScaler Console.

1. Dans l'onglet **Validation avant la mise à niveau**, la section **Instances bloquées de la mise à niveau** affiche les instances dont la mise à niveau a échoué en raison d'un espace disque insuffisant. Sélectionnez l'instance qui présente un problème d'espace disque.
2. Cliquez sur **Vérifier l'espace disque**.

   Une page **Détails de l'espace disque** apparaît. Cette page affiche les instances, la mémoire utilisée et la mémoire disponible.

   

3. Dans le volet **Détails de l'espace disque**, sélectionnez l'instance qui nécessite un nettoyage et effectuez l'une des opérations suivantes :

   a. **Nettoyage de disque** - Accédez aux dossiers ou répertoires requis et supprimez-les pour libérer de l'espace disque.

   b. **Nettoyage rapide** - Libérez rapidement de l'espace disque en supprimant plusieurs dossiers. Dans le volet **Confirmer** qui apparaît, sélectionnez les dossiers que vous souhaitez supprimer et cliquez sur **Oui**.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Après avoir libéré de l'espace disque, vous pouvez vérifier si suffisamment d'espace disque est maintenant disponible pour mettre à niveau l'instance. Dans la section **Instances bloquées pour la mise à niveau**, cliquez sur **Revalider**.

   Dans l'exemple suivant, l'espace disque est disponible. Vous pouvez maintenant cliquer sur **Déplacer vers prêt pour la mise à niveau** pour mettre à niveau l'instance ou cliquer sur **Suivant** pour passer à l'étape suivante.



Planification des tâches de mise à niveau pour une paire haute disponibilité NetScaler

Le tableau suivant répertorie les différents scénarios de planification dans la page **Planifier la tâche** et les options de mise à niveau correspondantes disponibles dans la page **Créer une tâche** :

QUAND SOUHAITEZ-VOUS EXÉCUTER LA TÂCHE DE MISE À NIVEAU ?	QUAND SOUHAITEZ-VOUS TÉLÉCHARGER L'IMAGE LOGICIELLE SUR NETSCALER ?	COMMENT SOUHAITEZ-VOUS TÉLÉCHARGER L'IMAGE DE BUILD VERS LES NŒUDS HA ?
Mettre à niveau maintenant	Non applicable	**Télécharger vers les nœuds principal et secondaire** (option par défaut)
	Télécharger uniquement vers le nœud secondaire	
Planifier ultérieurement	**Télécharger au moment de l'exécution** (option par défaut)	**Télécharger vers les nœuds principal et secondaire** (option par défaut)
	Télécharger uniquement vers le nœud secondaire	
	Télécharger maintenant	Non applicable
Planifier ultérieurement (lorsque **Effectuer une mise à niveau en deux étapes**	**Télécharger au moment de l'exécution** (option par défaut)	**Télécharger uniquement vers le nœud secondaire** (option par défaut et unique)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

QUAND SOUHAITEZ-VOUS EXÉCUTER LA TÂCHE DE MISE À NIVEAU ?	QUAND SOUHAITEZ-VOUS TÉLÉCHARGER L'IMAGE LOGICIELLE SUR NETSCALER ?	COMMENT SOUHAITEZ-VOUS TÉLÉCHARGER L'IMAGE DE BUILD VERS LES NŒUDS HA ?
pour les nœuds en HA est sélectionné)		
	Télécharger maintenant	Non applicable

Télécharger un rapport de différences combiné d'une tâche de mise à niveau NetScaler

Vous pouvez télécharger un rapport de différences d'une tâche de mise à niveau NetScaler si des scripts personnalisés sont spécifiés. Un rapport de différences contient les différences entre les sorties des scripts de pré-mise à niveau et de post-mise à niveau. Grâce à ce rapport, vous pouvez déterminer les modifications survenues sur l'instance NetScaler après la mise à niveau.

REMARQUE

Le rapport de différences est généré uniquement si vous spécifiez le même script dans les étapes de pré-mise à niveau et de post-mise à niveau.

Pour télécharger un rapport de différences d'une tâche de mise à niveau, procédez comme suit :

1. Accédez à **Infrastructure > Tâches de mise à niveau**.
2. Sélectionnez la tâche de mise à niveau pour laquelle vous souhaitez télécharger un rapport de différences.
3. Cliquez sur **Rapports de différences**.
4. Dans **Rapports de différences**, téléchargez un rapport de différences consolidé de la tâche de mise à niveau sélectionnée.

   Sur cette page, vous pouvez télécharger l'un des rapports de différences suivants :

   - **Rapport de différences pré-mise à niveau vs post-mise à niveau avant basculement**
   - **Rapport de différences pré-mise à niveau vs post-mise à niveau**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Avis de sécurité

Une infrastructure sûre, sécurisée et résiliente est la pierre angulaire de toute organisation. Les organisations doivent suivre les nouvelles Vulnérabilités et Expositions Communes (CVE), évaluer l'impact des CVE sur leur infrastructure, et comprendre et planifier les mesures correctives pour résoudre les vulnérabilités.

La fonctionnalité d'avis de sécurité de NetScaler Console vous permet de :

- Analyser les paramètres de configuration de votre NetScaler pour identifier toute mauvaise configuration, point faible ou déviation par rapport aux meilleures pratiques qui pourrait exposer votre système à des attaques.
- Suivre les nouvelles Vulnérabilités et Expositions Communes (CVE), évaluer l'impact des CVE, comprendre les mesures correctives et résoudre les vulnérabilités.
- Examiner l'intégrité de vos fichiers de build NetScaler.

Page d'accueil des avis de sécurité

La page d'accueil des avis de sécurité offre une vue d'ensemble complète de la posture de sécurité de votre déploiement NetScaler. L'interface est améliorée et conçue pour fournir aux administrateurs et aux professionnels de la sécurité des informations immédiates sur l'état général de santé et de vulnérabilité de leur infrastructure NetScaler.

NetScaler Console propose trois types d'avis de sécurité :

- **Recommandations de configuration sécurisée** - Vous permet de configurer les instances NetScaler conformément aux meilleures pratiques.
- **Détection des Vulnérabilités et Expositions Communes (CVE)** - Vous permet d'identifier les CVE qui mettent vos instances NetScaler en danger et recommande des mesures correctives.
- **Surveillance de l'intégrité des fichiers** - Vous permet d'identifier si des modifications ou des ajouts ont été apportés à vos fichiers de build NetScaler.

Le tableau de bord des avis de sécurité de NetScaler Console comprend également les éléments suivants :

- **Gravité globale de la posture de sécurité** - Représente l'état de la posture de sécurité et est calculée en fonction de la gravité maximale des trois types d'avis. L'état peut être l'un des suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Critique** : Plusieurs observations de gravité critique sont détectées et doivent être traitées avec la plus grande urgence.
    - **Élevé** : Des vulnérabilités ou des erreurs de configuration critiques sont détectées et doivent être corrigées immédiatement. Bien que moins urgentes que les découvertes critiques, ces problèmes posent un risque significatif pour la sécurité et la stabilité.
    - **Moyen** : Observations de sécurité importantes qui doivent être traitées en temps opportun. Ces problèmes ne posent pas de menace critique immédiate, mais ils pourraient potentiellement être exploités ou entraîner des problèmes plus graves s'ils ne sont pas résolus.
    - **Faible** : Problèmes de sécurité mineurs ou violations des meilleures pratiques qui ne posent pas de risque de sécurité significatif. Bien qu'ils ne constituent pas une menace immédiate, il est toujours judicieux de résoudre ces problèmes pour améliorer la posture de sécurité globale.

- **Dernière analyse** - La date de la dernière analyse. Les données fournies dans le tableau de bord sont basées sur les résultats de la dernière analyse.
- **Prochaine analyse planifiée** - La date de la prochaine analyse système planifiée.
- **Fréquence d'analyse planifiée** - La fréquence à laquelle les analyses système sont exécutées.
- **Analyser maintenant** - Permet une analyse à la demande qui vous permet d'analyser les instances à tout moment, selon vos besoins, en dehors du calendrier d'analyse du système.
- **Historique des analyses** - Fournit une vue historique de toutes les analyses qui ont été exécutées sur vos instances NetScaler.
- **NetScaler impactés** - Liste les instances NetScaler qui sont impactées.
- **Paramètres** - Vous permet de configurer les paramètres d'analyse du système et de définir des notifications pour les événements selon vos besoins.

Grâce aux informations disponibles sur le tableau de bord, vous pouvez rapidement identifier les vulnérabilités critiques, les recommandations de configuration sécurisée, y compris les étapes d'atténuation, et les liens vers la documentation pertinente.

La page d'accueil vous permet de filtrer les problèmes par criticité et par adresse IP NetScaler. Lorsqu'un niveau de criticité spécifique est sélectionné, seules les instances NetScaler de ce niveau de gravité sont affichées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT :

Dans l'interface graphique ou le rapport **Security Advisory**, tous les CVE peuvent ne pas apparaître, et vous ne pouvez voir qu'un seul CVE. Pour contourner ce problème, cliquez sur **Analyser maintenant** et sélectionnez **CVE** pour exécuter une analyse à la demande. Une fois l'analyse terminée, tous les CVE concernés (environ 15) apparaissent dans l'interface utilisateur ou le rapport.-->

Recommandations de configuration sécurisée

L'onglet **Recommandations de configuration sécurisée** fournit une analyse approfondie, au niveau de l'instance, des observations de configuration, conçue pour fournir aux utilisateurs des informations exploitables. Pour plus d'informations, consultez Recommandations de configuration sécurisée.

Détection des CVE

La détection des CVE se concentre principalement sur l'identification et l'atténuation des vulnérabilités de sécurité. Pour plus d'informations, consultez Détection des CVE.

Surveillance de l'intégrité des fichiers

La surveillance de l'intégrité des fichiers vérifie les modifications non autorisées ou malveillantes apportées aux fichiers principaux d'une instance NetScaler. C'est un élément clé de l'avis de sécurité. Pour plus d'informations, consultez Surveillance de l'intégrité des fichiers.

Analyser maintenant

Vous pouvez analyser les instances à tout moment, selon vos besoins, et également choisir les types d'analyses que vous souhaitez exécuter en fonction de vos exigences de sécurité.

Procédez comme suit pour exécuter l'analyse :

1. Cliquez sur **Analyser maintenant**.

   

2. Sélectionnez les types d'analyses que vous souhaitez exécuter.

   - Recommandations de configuration de sécurité
   - Détection des CVE
   - Surveillance de l'intégrité des fichiers

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Cliquez sur **Analyser maintenant**. Une fois l'analyse terminée, les détails de sécurité révisés apparaissent dans le tableau de bord des avis de sécurité.

Historique des analyses

Cliquez sur **Historique des analyses** pour afficher toutes les analyses historiques qui ont été exécutées sur vos instances NetScaler.



Vous pouvez afficher le type d'analyse (analyse à la demande ou analyse système), l'heure de début et de fin de l'analyse, l'état général de l'analyse, et également télécharger les détails de chaque analyse au format CSV ou PDF.



NetScaler impactés

La section **NetScaler impactés** répertorie toutes les instances NetScaler qui sont affectées par les configurations de sécurité, les CVE et les vérifications d'intégrité des fichiers de surveillance.



Vous pouvez également cliquer sur le nombre sous **CONFIGURATION DE RECOMMANDATION SÉCURISÉE**, **DÉTECTION DE CVE** ou **SURVEILLANCE DE L'INTÉGRITÉ DES FICHIERS** pour afficher plus de détails. Voici un exemple d'image pour votre référence.



Paramètres

En tant qu'administrateur, vous pouvez recevoir des notifications Citrix Cloud, qui indiquent le nombre d'instances NetScaler vulnérables aux CVE. Pour configurer quand et comment vous souhaitez recevoir des notifications, cliquez sur l'icône des paramètres dans le coin supérieur droit de la page d'avis de sécurité.



Vous pouvez effectuer les actions suivantes :

- Sélectionnez le type d'événements pour lesquels vous devez recevoir la notification.
- Sélectionnez comment vous souhaitez être averti. Par exemple, par e-mail, Slack, PagerDuty.
- Sélectionnez le type d'analyse qui doit être inclus dans les analyses système. Par défaut, seule l'analyse CVE est activée pour l'analyse système.
- Désactivez l'analyse personnalisée de l'avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez également configurer le type d'analyses qui doivent être incluses dans les analyses système.



AVERTISSEMENT :

Veuillez noter que la surveillance de l'intégrité des fichiers NetScaler (« la Fonctionnalité ») n'est pas capable de détecter toutes les techniques, tactiques ou procédures (TTP) que les acteurs de la menace peuvent utiliser lorsqu'ils ciblent des environnements pertinents. Les acteurs de la menace modifient fréquemment les TTP et l'infrastructure, et par conséquent, la Fonctionnalité peut avoir une valeur médico-légale limitée, voire nulle, concernant certaines menaces. Il vous est fortement conseillé de faire appel aux services d'enquêteurs médico-légaux expérimentés pour évaluer votre environnement en cas de menace possible.

Ce document et les informations qu'il contient sont fournis « tels quels ». Cloud Software Group, Inc. ne fait aucune garantie ou déclaration, expresse ou implicite, concernant le document ou son contenu, y compris, sans limitation, que ce document ou les informations qu'il contient sont exempts d'erreurs ou répondent à des conditions de qualité marchande ou d'adéquation à un usage particulier.

Recommandations de configuration sécurisée

L'avis de configuration sécurisée NetScaler sert de guide complet offrant des recommandations d'experts et des instructions spécifiques pour améliorer la posture de sécurité des configurations NetScaler. Grâce à cette fonctionnalité, vous pouvez protéger votre infrastructure de contrôleur de livraison d'applications (ADC) contre les vulnérabilités potentielles et les cybermenaces évolutives. En suivant méticuleusement les directives recommandées, vous pouvez atténuer de manière proactive les risques, améliorer la résilience du système et maintenir une défense robuste contre les accès non autorisés et les activités malveillantes.

Cette fonctionnalité non seulement analyse la configuration NetScaler à la recherche de vulnérabilités potentielles, mais suggère également de manière proactive des commandes précises pour corriger ces configurations. Les administrateurs réseau peuvent rapidement identifier les lacunes de sécurité et mettre en œuvre les modifications nécessaires pour renforcer leur déploiement NetScaler.

L'onglet **Recommandations de configuration sécurisée** offre une vue complète méticuleusement catégorisée par gravité, permettant une approche priorisée pour traiter les vulnérabilités de configuration potentielles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Priorisation basée sur la gravité

La catégorisation par gravité permet aux utilisateurs d'allouer efficacement leurs efforts. Les observations sont généralement classées en niveaux tels que :

- **Critique** : Problèmes qui posent un risque immédiat et significatif pour la sécurité et l'intégrité de l'instance NetScaler. Ces problèmes doivent être traités avec la plus grande urgence.
- **Élevé** : Configurations qui pourraient entraîner des failles de sécurité substantielles si elles sont exploitées, nécessitant une attention rapide.
- **Moyen** : Observations qui indiquent des faiblesses ou des erreurs de configuration potentielles. Bien que ces problèmes ne soient pas critiques, ils pourraient contribuer à un incident de sécurité plus important s'ils ne sont pas traités.
- **Faible** : Recommandations mineures ou meilleures pratiques qui améliorent la posture de sécurité globale. Ces problèmes ne représentent pas une menace immédiate.

Avantages d'une vue détaillée au niveau de l'instance

- **Correction ciblée** : Au lieu de conseils génériques, les utilisateurs reçoivent des recommandations spécifiques adaptées à chaque instance NetScaler individuelle, garantissant une correction précise et efficace.
- **Surface d'attaque réduite** : En traitant systématiquement les erreurs de configuration observées, les organisations peuvent réduire considérablement leur surface d'attaque et minimiser la probabilité d'exploits réussis.
- **Conformité** : Les observations détaillées peuvent aider les organisations à identifier et à corriger les configurations qui pourraient violer les normes de conformité réglementaire (par exemple, GDPR, HIPAA, PCI DSS).
- **Amélioration de la posture de sécurité** : L'identification et la résolution proactives des faiblesses de configuration conduisent à une posture de sécurité globale plus solide et à une résilience accrue contre les cybermenaces.
- **Efficacité opérationnelle** : En fournissant des informations claires et exploitables, le système rationalise le processus de correction de la sécurité, ce qui permet d'économiser du temps et des ressources.

Vous pouvez **choisir** les observations à traiter en premier, en fonction de vos priorités, de votre tolérance au risque et des ressources disponibles. Cette flexibilité garantit que les problèmes de sécurité les plus urgents sont traités sans délai, tout en fournissant les informations nécessaires pour parvenir à un renforcement complet de la configuration au fil du temps. Cette option permet

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aux administrateurs de sécurité de prendre des décisions éclairées et des mesures décisives pour protéger leurs déploiements NetScaler.



La fonctionnalité de recherche en texte libre vous permet d'affiner les résultats en fonction de divers identifiants clés. Par exemple, vous pouvez rechercher efficacement une instance par son nom d'hôte unique, ce qui constitue une méthode directe pour identifier un périphérique particulier. Alternativement, la recherche par adresse IP offre un autre moyen précis de localiser les instances, particulièrement utile dans les environnements centrés sur le réseau.

Au-delà de l'identification de base, la recherche prend également en charge le filtrage par modèle NetScaler. Cela signifie que vous pouvez spécifier des modèles tels que MPX, SDX ou VPX pour afficher uniquement les instances appartenant à une catégorie matérielle ou logicielle particulière. Vous pouvez également affiner la recherche par niveau de gravité, ce qui vous permet de hiérarchiser les instances en fonction de leur criticité, des alertes informatives aux avertissements critiques.



Corriger les recommandations de configuration

Une fois que vous avez évalué les observations de configuration et déterminé celles qui nécessitent une action, une vue complète des configurations recommandées est présentée. Le système affiche ensuite une page dédiée, comme illustré dans l'image suivante, affichant les étapes de correction adaptées à vos sélections. Par exemple, si vous choisissez de ne traiter que les problèmes de gravité critique pour une instance NetScaler spécifique (dans ce scénario particulier, l'instance avec l'adresse IP 10.102.56.45), la page se remplit dynamiquement avec les recommandations pertinentes et hautement prioritaires pour guider efficacement le processus de correction.



Les recommandations de configuration peuvent être classées en deux types :

- **Recommandations nécessitant une saisie de l'utilisateur** : Cette catégorie englobe les suggestions de configuration qui nécessitent des informations contextuelles spécifiques ou des décisions de la part de l'administrateur NetScaler ou de l'équipe de sécurité. Il s'agit généralement de scénarios où une valeur par défaut générique pourrait ne pas être appropriée, ou lorsque le paramètre optimal dépend de l'environnement opérationnel unique, des politiques de sécurité ou des exigences de l'application. Voici quelques exemples de recommandations :
    - **Définition d'adresses IP ou de plages d'adresses IP spécifiques** : Par exemple, la configuration de règles de pare-feu pour autoriser le trafic uniquement à partir de sous-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

réseaux internes approuvés ou d'adresses IP client spécifiques. Le système ne peut pas déduire ces détails réseau uniques.

- **Définition de numéros de port personnalisés** : Bien que des ports standard existent pour de nombreux services, les applications peuvent être configurées pour utiliser des ports non par défaut pour des raisons de sécurité ou opérationnelles. L'administrateur réseau doit spécifier les numéros de port.
- **Spécification de noms d'hôte ou de noms de domaine** : Lors de la configuration de certificats SSL, de serveurs virtuels d'équilibrage de charge ou de stratégies de commutation de contenu, les noms d'hôte ou de domaine exacts que l'instance NetScaler sert ou avec lesquels elle interagit doivent être fournis par l'utilisateur.
- **Fourniture des détails du serveur d'authentification** : L'intégration de NetScaler avec des systèmes d'authentification externes tels que LDAP, RADIUS, SAML ou OAuth exige que l'utilisateur saisisse les adresses IP du serveur, les secrets partagés, les chemins d'accès aux répertoires et d'autres détails spécifiques au protocole.
- **Configuration de politiques spécifiques de réécriture d'URL ou de commutation de contenu** : Les URL, les modèles et les destinations cibles précis pour ces fonctionnalités avancées sont très spécifiques à l'architecture de l'application et doivent être définis par l'utilisateur.
- **Implications** : Ces recommandations impliquent souvent une compréhension plus approfondie des besoins spécifiques du déploiement, des politiques de sécurité et de la topologie du réseau. Les erreurs de saisie de l'utilisateur peuvent entraîner des interruptions de service ou des vulnérabilités de sécurité, soulignant la nécessité d'une planification et d'une validation minutieuses. Les outils ou scripts automatisés qui les implémentent demandent généralement les paramètres nécessaires, ou les lisent à partir d'un fichier de configuration.

- **Recommandations ne nécessitant pas de saisie utilisateur** : Cette catégorie comprend des suggestions de configuration qui peuvent être appliquées universellement ou impliquent des bonnes pratiques standard qui ne dépendent pas de variables environnementales uniques. Il s'agit souvent d'améliorations de sécurité fondamentales ou d'optimisations de performances qui sont bénéfiques pour la plupart des déploiements NetScaler. Voici quelques exemples de recommandations :

  - **Désactivation des chiffrements ou protocoles faibles** : Il est recommandé de désactiver les versions SSL/TLS, telles que SSLv3 ou TLS 1.0, ou les suites de chiffrement faibles spécifiques (par exemple, RC4, 3DES), car ce sont des vulnérabilités connues et leur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

suppression est une bonne pratique de sécurité universelle. Le système n'a pas besoin d'une saisie spécifique pour savoir quels chiffrements sont faibles.

- **Activation de HTTP Strict Transport Security (HSTS)** : Il s'agit d'une politique appliquée par les navigateurs web pour n'interagir avec un serveur qu'en utilisant des connexions HTTPS sécurisées. Son activation est une étape standard de renforcement de la sécurité.
- **Définition d'indicateurs de cookie sécurisés (par exemple, `Secure`, `HttpOnly`)** : Ces indicateurs améliorent la sécurité des cookies de session, les empêchant d'être transmis sur des canaux non chiffrés ou d'être accédés via des scripts côté client. Leur application est une recommandation générale.
- **Activation des en-têtes de sécurité courants** : Des en-têtes comme X-Frame-Options, X-Content-Type-Options et Content-Security-Policy (avec une politique de sécurité par défaut) peuvent être recommandés sans saisie spécifique de l'utilisateur, car ils améliorent universellement la sécurité côté client.
- **Implémentation d'une limitation de débit par défaut pour les attaques courantes** : Bien que les limites de débit personnalisées puissent nécessiter une saisie, une recommandation d'appliquer une limite de débit générale aux vecteurs d'attaque courants (par exemple, les tentatives de connexion échouées excessives) pourrait être applicable comme base.
- **Configuration de tailles de tampon ou de délais d'attente optimaux** : Recommandations générales de performances liées aux tailles de tampon internes ou aux délais d'attente de connexion qui sont déterminées par l'architecture du système plutôt que par la logique d'application spécifique.
- **Assurer des niveaux de journalisation appropriés pour les événements de sécurité** : Une recommandation visant à garantir un certain niveau de journalisation pour les événements liés à la sécurité est une bonne pratique générale pour l'audit et la réponse aux incidents.

- **Implications** : Ces recommandations sont souvent d'excellents candidats pour l'automatisation ou les scripts de configuration de base, car elles peuvent être appliquées uniformément à plusieurs instances NetScaler sans nécessiter d'intervention manuelle pour des détails spécifiques. Elles contribuent à une posture de sécurité solide en traitant les vulnérabilités courantes et en appliquant des normes largement acceptées.

En résumé, la classification des recommandations de configuration en fonction des exigences de saisie de l'utilisateur rationalise le processus de mise en œuvre. Les recommandations qui nécessitent une saisie exigent une collecte et une validation minutieuses des données de la part

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de l'utilisateur, tandis que celles qui ne nécessitent pas de saisie peuvent souvent être appliquées comme bases de sécurité standard ou via des mécanismes de déploiement automatisés.

Une fois qu'un utilisateur a décidé quelle configuration aborder, le flux de travail des tâches de configuration existant prend le relais pour appliquer les modifications de configuration.

Par exemple, voici un exemple de recommandation de configuration qui nécessite une saisie utilisateur. On peut saisir les valeurs de configuration une par une ou choisir de télécharger un fichier contenant les valeurs de configuration, comme illustré dans l'image suivante.

Détection des CVE

NetScaler détecte les CVE en analysant les versions d'instances, les configurations et les fichiers système pour identifier les vulnérabilités. Il utilise un référentiel CVE mis à jour et fournit une analyse d'impact détaillée ainsi que des suggestions de correction.

La section **Détection des CVE** du tableau de bord **Avis de sécurité** répertorie les éléments suivants :

- Nombre de CVE détectées
- Nombre d'instances NetScaler impactées
- Date de la dernière analyse
- Instances NetScaler impactées classées par gravité : Critique, Élevée, Moyenne et Faible

En tant qu'administrateur, vous pouvez autoriser NetScaler à exécuter les analyses système planifiées périodiquement ou choisir d'exécuter des analyses à la demande selon vos besoins.

- **Analyse système** - Analyse toutes les instances gérées par défaut. NetScaler Console décide de la date et de l'heure des analyses système, et vous ne pouvez pas les modifier.
- **Analyse à la demande** - Vous pouvez analyser manuellement les instances si nécessaire. Si le temps écoulé depuis la dernière analyse système est significatif, vous pouvez exécuter une analyse à la demande pour évaluer la posture de sécurité actuelle. Ou analyser après l'application d'une correction, pour évaluer la posture révisée. Pour exécuter l'analyse à la demande, cliquez sur **Analyser maintenant** dans l'avis de sécurité.

Vous pouvez cliquer sur la section **Détection des CVE** pour afficher des informations détaillées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



La section **Détection des CVE** comporte deux vues :

- Vue d'instance
- Vue CVE

Vue de l'instance

La vue de l'instance contient les onglets **Instances impactées** et **Référentiel CVE**.

L'onglet **Instances impactées** affiche la liste des instances NetScaler impactées.



Les instances impactées sont classées en fonction des facteurs de forme suivants :

- MPX et VPX
- SDX
- CPX
- BLX

Vous pouvez également rechercher les instances en fonction des éléments suivants :

- CVE détectée
- Nom d'hôte
- Modèle
- Instance NetScaler
- État

Le tableau affiche les détails suivants :

- Adresse IP du NetScaler
- Nom d'hôte
- Numéro de modèle du NetScaler
- État du NetScaler
- Version et build du logiciel
- Liste des CVE affectant le NetScaler.

La plupart des CVE nécessitent une mise à niveau comme mesure corrective, tandis que d'autres nécessitent une mise à niveau et une étape supplémentaire comme mesure corrective.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pour la correction de CVE-2020-8300, consultez Corriger les vulnérabilités pour CVE-2020-8300.
- Pour CVE-2021-22927 et CVE-2021-22920, consultez Corriger les vulnérabilités pour CVE-2021-22927 et CVE-2021-22920.
- Pour CVE CVE-2021-22956, consultez Identifier et corriger les vulnérabilités pour CVE-2021-22956
- Pour CVE CVE-2022-27509, consultez Corriger les vulnérabilités pour CVE-2022-27509

REMARQUE

Si vos instances NetScaler ont des personnalisations, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Vous pouvez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Pour mettre à niveau, effectuez l'une des opérations suivantes :

- **Flux de travail de mise à niveau** - Sélectionnez une instance et cliquez sur **Procéder au flux de travail de mise à niveau**.
- **Flux de travail de tâche de configuration** - Sélectionnez une instance et cliquez sur **Flux de travail de tâche de configuration**.

Le flux de travail de mise à niveau démarre et le NetScaler vulnérable est automatiquement renseigné comme NetScaler cible. Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Utiliser les tâches pour mettre à niveau les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

- Les versions 13.0, 12.1, 12.0, 11.0, 10.5 et inférieures sont déjà en fin de vie (EOL). Si vos instances NetScaler fonctionnent sur l'une de ces versions, mettez à niveau vers une version prise en charge.
- La version et la build vers lesquelles vous souhaitez effectuer la mise à niveau sont à votre discrétion. Consultez les conseils sous la colonne de remédiation pour savoir quelles versions et builds contiennent le correctif de sécurité. Et sélectionnez en conséquence une version et une build prises en charge, qui n'ont pas encore atteint la fin de vie.

Pour passer à la vue CVE, cliquez sur **Basculer vers la vue CVE**.

Vue CVE

La vue CVE affiche les résultats de toutes les CVE impactant votre infrastructure et toutes les instances NetScaler impactées, et suggère des mesures correctives. Vous pouvez utiliser ces informations pour appliquer des mesures correctives afin de résoudre les risques de sécurité.

Le tableau affichant le nombre de CVE impactant les instances NetScaler contient les détails suivants.

- **ID CVE** : L'ID de la CVE qui impacte les instances.
- **Date de publication** : La date à laquelle le bulletin de sécurité a été publié pour cette CVE.
- **Score de gravité** : Le type de gravité (élevée/moyenne/critique) et le score. Pour voir le score, survolez le type de gravité.
- **Type de vulnérabilité** : Le type de vulnérabilité pour ce CVE.
- **Instances NetScaler affectées** : Le nombre d'instances impactées par l'ID CVE. Au survol, la liste des instances NetScaler apparaît.
- **Correction** : Les corrections disponibles, qui sont la mise à niveau de l'instance (généralement) ou l'application de packs de configuration.

La même instance peut être impactée par plusieurs CVE. Ce tableau vous aide à voir combien d'instances sont impactées par un CVE particulier ou par plusieurs CVE sélectionnés. Pour vérifier l'adresse IP de l'instance impactée, survolez Détails NetScaler sous **Instances NetScaler affectées**. Pour vérifier les détails de l'instance impactée, cliquez sur **Afficher les instances**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

affectées en bas du tableau. Vous pouvez également ajouter ou supprimer des colonnes dans le tableau en cliquant sur le signe plus.

Référentiel CVE

Les vues d'instance et de CVE contiennent toutes deux l'onglet **Référentiel CVE**. Cet onglet offre une vue détaillée de tous les CVE liés à NetScaler que Citrix a annoncés depuis décembre 2019 et qui pourraient impacter votre infrastructure NetScaler.

- ID de CVE
- Type de vulnérabilité
- Date de publication
- Niveau de gravité
- Correction
- Liens vers les bulletins de sécurité

Vous pouvez utiliser cette vue pour comprendre les CVE dans le cadre de l'avis de sécurité et pour en savoir plus sur le CVE. Pour plus d'informations sur les CVE non pris en charge, consultez CVE non pris en charge dans l'avis de sécurité.

Points à noter

- L'avis de sécurité ne prend pas en charge les versions de NetScaler ayant atteint la fin de vie (EOL). Nous vous recommandons de passer aux versions ou builds NetScaler prises en charge.
- Instances prises en charge pour la détection des CVE : tous les NetScaler (SDX, MPX, VPX) et Gateway.
- Instances prises en charge pour la surveillance de l'intégrité des fichiers : instances MPX, VPX et Gateway.
- CVE prises en charge : toutes les CVE après décembre 2019.

REMARQUE :

La détection et la correction des vulnérabilités affectant le plug-in NetScaler Gateway pour Windows ne sont pas prises en charge par l'avis de sécurité de NetScaler Console. Pour plus d'informations sur les CVE non prises en charge, consultez CVE non prises en charge dans l'avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'avis de sécurité de NetScaler Console ne tient pas compte de tout type de mauvaise configuration de fonctionnalité lors de l'identification de la vulnérabilité.
- L'avis de sécurité de NetScaler Console ne prend en charge que l'identification et la correction des CVE. Il ne prend pas en charge l'identification et la correction des problèmes de sécurité mis en évidence dans l'article de sécurité.
- Portée des versions NetScaler, Gateway : La fonctionnalité est limitée aux versions principales. L'avis de sécurité n'inclut aucune version spéciale dans son champ d'application.
    - L'avis de sécurité n'est pas pris en charge dans la partition d'administration.
- Les types d'analyse suivants sont disponibles pour les CVE :
    - **Analyse de version** : Cette analyse nécessite que NetScaler Console compare la version d'une instance NetScaler avec les versions et les builds sur lesquelles le correctif est disponible. Cette comparaison de versions aide l'avis de sécurité de NetScaler Console à identifier si le NetScaler est vulnérable à la CVE. Par exemple, si une CVE est corrigée sur une version et une build NetScaler xx.yy, l'avis de sécurité considère toutes les instances NetScaler sur des builds inférieures à xx.yy comme vulnérables. L'analyse de version est prise en charge aujourd'hui dans l'avis de sécurité.
    - **Analyse de configuration** : Cette analyse nécessite que NetScaler Console fasse correspondre un modèle spécifique à l'analyse CVE avec le fichier de configuration NetScaler (`nsconf`). Si le modèle de configuration spécifique est présent dans le fichier ns.conf de NetScaler, l'instance est considérée comme vulnérable à cette CVE. Cette analyse est généralement utilisée avec l'analyse de version. L'analyse de configuration est prise en charge aujourd'hui dans l'avis de sécurité.
    - **Analyse personnalisée** : Cette analyse nécessite que NetScaler Console se connecte à l'instance NetScaler gérée, y pousse un script et l'exécute. La sortie du script aide NetScaler Console à identifier si le NetScaler est vulnérable à la CVE. Les exemples incluent la sortie de commandes shell spécifiques, la sortie de commandes CLI spécifiques, certains journaux, et l'existence ou le contenu de certains répertoires ou fichiers. Pour les CVE qui nécessitent des analyses personnalisées, le script s'exécute chaque fois que votre analyse planifiée ou à la demande s'exécute. En savoir plus sur les données collectées et les options pour les analyses personnalisées spécifiques dans la documentation de l'avis de sécurité pour cette CVE.
- Les analyses n'ont pas d'impact sur le trafic de production sur NetScaler et ne modifient aucune configuration NetScaler sur NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L'avis de sécurité de NetScaler Console ne prend pas en charge l'atténuation des CVE. Si vous avez appliqué une atténuation (solution temporaire) à l'instance NetScaler, NetScaler Console identifie toujours le NetScaler comme un NetScaler vulnérable tant que vous n'avez pas terminé la correction.
- Pour les instances FIPS, l'analyse des CVE n'est pas prise en charge.

Surveillance de l'intégrité des fichiers

La surveillance de l'intégrité des fichiers vous permet d'identifier si des modifications ou des ajouts ont été apportés à votre système de fichiers NetScaler. Cette fonctionnalité évalue l'intégrité des fichiers NetScaler en comparant la valeur de hachage binaire de votre version actuelle de NetScaler avec le hachage binaire original lié à la même version de NetScaler.

La section **Surveillance de l'intégrité des fichiers** du tableau de bord **Conseils de sécurité** répertorie les éléments suivants :

- Nombre de problèmes détectés
- Nombre d'instances NetScaler impactées
- Date de la dernière exécution de l'analyse
- Instances NetScaler impactées classées par gravité : Critique, Élevée, Moyenne et Faible
- Instances NetScaler impactées ayant signalé des problèmes à l'aide de la signature et de la vérification binaires



En tant qu'administrateur, vous pouvez autoriser NetScaler à exécuter les analyses système planifiées périodiquement ou vous pouvez choisir d'exécuter des analyses à la demande selon vos besoins.

- **Analyse système** - Analyse toutes les instances gérées par défaut. NetScaler Console décide de la date et de l'heure des analyses système, qui sont désactivées par défaut.
- **Analyse à la demande** - Vous pouvez déclencher l'analyse manuellement si nécessaire. Pour exécuter l'analyse à la demande, cliquez sur **Analyser maintenant** sur le tableau de bord des conseils de sécurité.

Vous pouvez cliquer sur la section **Surveillance de l'intégrité des fichiers** pour afficher des informations détaillées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Détecté par la console

L'onglet **Détecté par la console** répertorie les instances NetScaler impactées en comparant le hachage binaire de la version actuelle avec le hachage de la version originale pour détecter les fichiers modifiés ou nouvellement ajoutés. Le tableau affiche les détails suivants :

- Adresse IP - L'adresse IP des instances impactées.
- Statut de l'analyse - Affiche les résultats d'erreur de l'analyse.
- Fichier existant modifié - La liste des fichiers existants qui sont modifiés.
- Nouveaux fichiers ajoutés - La liste des nouveaux fichiers ajoutés.
- Heure de l'analyse - L'heure de la dernière analyse.
- Nom d'hôte - Le nom d'hôte du NetScaler impacté.
- Modèle - Le nom du modèle du NetScaler impacté.

Les résultats d'erreur de l'analyse sont affichés dans la vue principale du tableau de bord afin que vous n'ayez pas à cliquer sur les résultats d'analyse individuels ou les éléments de ligne pour accéder aux détails de l'erreur. Tout problème d'intégrité, tel que des incohérences de hachage ou des erreurs d'analyse, est présenté dans un format clair et accessible sur le tableau de bord, vous aidant à identifier et à comprendre rapidement les problèmes.

Cliquez sur les nombres sous **Fichiers existants modifiés** et **Nouveaux fichiers ajoutés** pour afficher les détails.



Vous pouvez créer une liste d'autorisation personnalisée et exclure des fichiers spécifiques des analyses de surveillance de l'intégrité des fichiers. En définissant les fichiers à exclure de l'analyse, vous pouvez rationaliser la surveillance et réduire les alertes inutiles pour les fichiers fiables.

Pour exclure des fichiers spécifiques des analyses de surveillance de l'intégrité des fichiers :

1. Cliquez sur **Exclure les fichiers/répertoires**.
2. Sélectionnez les fichiers ou répertoires requis.

   ou

   cliquez sur **Ajouter des fichiers/répertoires** pour ajouter de nouveaux fichiers. Vous pouvez ajouter des modèles de caractères génériques shell standard et exclure tous les chemins qui

© 1997–2026 Citrix Systems, Inc. All rights reserved.

correspondent aux critères définis. Lorsqu'un répertoire est ajouté, tous ses fichiers sont exclus de l'analyse. Cliquez sur **Ajouter**.

Vous pouvez également effectuer une recherche pour localiser des fichiers ou des dossiers particuliers. Vous pouvez également trouver les chemins de la liste d'exclusion en saisissant une partie d'un fichier ou d'un dossier dans la barre de recherche sous l'option `path`. La fonctionnalité de recherche facilite la gestion et la révision des chemins exclus.

Si vous ne souhaitez pas exclure les fichiers de l'analyse, vous pouvez sélectionner les fichiers ou répertoires requis et cliquer sur **Supprimer les fichiers/répertoires**. Les fichiers ou répertoires spécifiés sont inclus dans la prochaine analyse planifiée.



Points à noter

- Instances prises en charge pour la surveillance de l'intégrité des fichiers : instances MPX, VPX et Gateway.
- L'analyse suivante est disponible pour la surveillance de l'intégrité des fichiers :
  - **Analyse de la surveillance de l'intégrité des fichiers** : Cette analyse nécessite que NetScaler Console se connecte à l'instance NetScaler gérée. NetScaler Console compare les valeurs de hachage en exécutant un script dans NetScaler et en collectant les valeurs de hachage binaires actuelles pour les fichiers système NetScaler. Après la comparaison, NetScaler Console fournit le résultat avec le nombre total de fichiers existants modifiés et le nombre total de fichiers nouvellement ajoutés. En tant qu'administrateur, vous pouvez contacter le service de criminalistique numérique de votre organisation pour des investigations supplémentaires sur les résultats de l'analyse.
- Voici la liste des plateformes non prises en charge : BLX

Rapporté par l'appareil

L'onglet **Rapporté par l'appareil** répertorie les instances NetScaler qui ont signalé des problèmes à l'aide de la signature et de la vérification binaires. Grâce à cette vérification, la signature numérique de chaque fichier est validée pour confirmer l'authenticité et détecter toute altération. Si vous constatez des instances affectées, vous pouvez poursuivre les activités de criminalistique numérique de votre organisation. Le tableau répertorie les instances NetScaler impactées ainsi que d'autres détails tels que le nom d'hôte, le binaire ajouté, le binaire modifié. Vous pouvez cliquer sur **Détails** correspondant à l'instance requise pour afficher des informations détaillées.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Détection des indicateurs de compromission dans NetScaler Console

La fonctionnalité de détection des indicateurs de compromission (IoC) dans NetScaler Console est conçue pour détecter si vos appliances NetScaler ont potentiellement été affectées en raison d'une vulnérabilité.

S'il y a des événements CVE, l'une des premières préoccupations est que des acteurs malveillants aient pu exploiter la vulnérabilité. Un exploit cause des dommages catastrophiques à l'activité d'un client et il est donc essentiel de détecter de tels incidents immédiatement. Des indicateurs de compromission ont été distribués pour NetScaler par le passé via les canaux de support, ce qui répond aux besoins du client mais implique un effort supplémentaire pour passer par le processus de support consistant à ouvrir un ticket, à parler avec un professionnel du support, ce qui peut parfois ne pas être idéal. La fonctionnalité de détection des indicateurs de compromission dans NetScaler Console est conçue pour court-circuiter le processus actuel axé sur le support et aider un client à réaliser une évaluation rapide de son infrastructure NetScaler.

Prérequis

Cette fonctionnalité vous demande d'envoyer des données de télémétrie d'utilisation du produit. Pour plus d'informations sur la télémétrie NetScaler, consultez `<https://docs.netscaler.com/fr-fr/netscaler-application-delivery-management-software/current-release/ns-telemetry.html>`.

Avantages

- Vous pouvez exécuter des analyses de détection de compromission depuis la page **Security Advisory** de NetScaler Console.

  

- L'analyse fournit l'un des résultats suivants :
  - **Potentiellement compromis** – Si la logique de détection a détecté une compromission potentielle pour une CVE.
  - **Aucune compromission détectée** – Si la logique de détection n'a détecté aucune compromission.
  - **Ignoré** – Si l'analyse a été ignorée manuellement pour une instance NetScaler particulière.
  - **Échec de l'exécution** – Si l'analyse n'a pas été exécutée avec succès.
  - **Exécution en cours** – Si l'analyse est en cours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La logique IoC est mise à jour en permanence à mesure que de nouveaux IoC sont découverts. Dans un tel cas, la page d'accueil indique qu'une mise à jour est disponible.
- Chaque fois qu'une mise à jour est disponible pour la logique de détection des IoC, vous pouvez la voir sur la page d'accueil.

  Tableau de bord des indicateurs de compromission(/en-us/netscaler-console-service/media/indicators-of-compromise-dashboard.png)
- Les résultats des analyses précédentes sont enregistrés et peuvent être consultés à tout moment.

  Historique des documents des indicateurs de compromission(/en-us/netscaler-console-service/media/indicators-of-comprimise-scan-history.png)
- La solution utilise une architecture en étoile où un service cloud central ingère les actifs à partir d'un emplacement cloud sécurisé et les installe sur les périphériques cibles.

REMARQUE :

Les informations IoC n'englobent pas toutes les techniques, tactiques ou procédures (« TTP ») que les acteurs de la menace pourraient utiliser lors du ciblage d'environnements pertinents. De plus, les acteurs de la menace modifient fréquemment leurs TTP et leur infrastructure. Pour ces raisons et d'autres, les informations IoC peuvent avoir une valeur médico-légale limitée et peuvent ne pas identifier les compromissions réelles. Il vous est conseillé de faire appel aux services d'enquêteurs médico-légaux expérimentés pour évaluer votre environnement.

CVE pris en charge via l'avis de sécurité

Dans votre NetScaler Console sur site, la version complète de l'avis de sécurité est prise en charge si vous avez activé l'avis de sécurité via Cloud Connect ou le canal activé automatiquement. Pour plus d'informations, consultez Avis de sécurité.

Derniers CVE pris en charge

Le tableau suivant fournit les détails des derniers CVE pris en charge que vous pouvez identifier et corriger dans l'avis de sécurité :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE DE PUBLICATION	ID CVE	IDENTIFICATION	CORRECTION	LIEN VERS LA RESSOURCE
27 Sep 2026	CVE-2026-88771	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité.	Bulletin de sécurité
27 Sep 2026	CVE-2026-88772	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité.	Bulletin de sécurité
27 Sep 2026	CVE-2026-88773	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité.	Bulletin de sécurité
27 Sep 2026	CVE-2026-88774	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité.	Bulletin de sécurité
27 Sep 2026	CVE-2026-88775	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité.	Bulletin de sécurité
27 Sep 2026	CVE-2026-88776	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée	Bulletin de sécurité

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE DE PUBLICATION	ID CVE	IDENTIFICATION	CORRECTION	LIEN VERS LA RESSOURCE
			dans le bulletin de sécurité.	
27 Sep 2026	CVE-2026-88777	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité.	Bulletin de sécurité
27 Sep 2026	CVE-2026-88778	Nécessite une analyse de version.	Mettez à niveau vers la version recommandée mentionnée dans le bulletin de sécurité et appliquez la tâche de configuration.	Bulletin de sécurité

REMARQUE :

L'avis de sécurité ne prend pas en charge les versions de NetScaler ayant atteint la fin de vie (EOL). Nous vous recommandons de passer aux versions ou builds NetScaler pris en charge.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Utiliser les tâches pour mettre à niveau les instances NetScaler.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact des CVE dans le module d'avis de sécurité. Pour voir l'impact plus tôt, vous pouvez lancer une analyse à la demande en cliquant sur **Analyser maintenant**.

CVE prises en charge

Voici les CVE existantes prises en charge dans l'avis de sécurité :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE DE PUBLICATION	ID CVE	LIEN VERS LA RESSOURCE
19 Aug 2026	CVE-2026-19490	Bulletin de sécurité
19 Aug 2026	CVE-2026-19489	Bulletin de sécurité
30 Jun 2026	CVE-2026-13474	Bulletin de sécurité
30 Jun 2026	CVE-2026-10817	Bulletin de sécurité
30 Jun 2026	CVE-2026-10816	Bulletin de sécurité
30 Jun 2026	CVE-2026-8655	Bulletin de sécurité
30 Jun 2026	CVE-2026-8452	Bulletin de sécurité
30 Jun 2026	CVE-2026-8451	Bulletin de sécurité
Mar 23, 2026	CVE-2026-4368	Bulletin de sécurité
Mar 23, 2026	CVE-2026-3055	Bulletin de sécurité
Nov 11, 2025	CVE-2025-12101	Bulletin de sécurité
Aug 26, 2025	CVE-2025-8424	Bulletin de sécurité
Aug 26, 2025	CVE-2025-7776	Bulletin de sécurité
Aug 26, 2025	CVE-2025-7775	Bulletin de sécurité
Jun 25, 2025	CVE-2025-6543	Bulletin de sécurité
Jun 17, 2025	CVE-2025-5349	Bulletin de sécurité
Jun 17, 2025	CVE-2025-5777	Bulletin de sécurité
Nov 12, 2024	CVE-2024-8535	Bulletin de sécurité
Jul 09, 2024	CVE-2024-5491	Bulletin de sécurité
Jul 09, 2024	CVE-2024-5492	Bulletin de sécurité
Jan 16, 2024	CVE-2023-6549	Bulletin de sécurité

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE DE PUBLICATION	ID CVE	LIEN VERS LA RESSOURCE
Jan 16, 2024	CVE-2023-6548	Bulletin de sécurité
Oct 10, 2023	CVE-2023-4967	Bulletin de sécurité
Oct 10, 2023	CVE-2023-4966	Bulletin de sécurité
Jul 18, 2023	CVE-2023-3519	Bulletin de sécurité
Jul 18, 2023	CVE-2023-3467	Bulletin de sécurité
Jul 18, 2023	CVE-2023-3466	Bulletin de sécurité
May 09, 2023	CVE-2023-24488	Bulletin de sécurité
May 09, 2023	CVE-2023-24487	Bulletin de sécurité
Dec 13, 2022	CVE-2022-27518	Bulletin de sécurité
Nov 08, 2022	CVE-2022-27516	Bulletin de sécurité
Nov 08, 2022	CVE-2022-27513	Bulletin de sécurité
Nov 08, 2022	CVE-2022-27510	Bulletin de sécurité
Jul 26, 2022	CVE-2022-27509	Bulletin de sécurité
May 25, 2022	CVE-2022-27508	Bulletin de sécurité
May 25, 2022	CVE-2022-27507	Bulletin de sécurité
Nov 09, 2021	CVE-2021-22956	Bulletin de sécurité
Nov 09, 2021	CVE-2021-22955	Bulletin de sécurité
Jul 19, 2021	CVE-2021-22927	Bulletin de sécurité
Jul 19, 2021	CVE-2021-22920	Bulletin de sécurité
Jul 19, 2021	CVE-2021-22919	Bulletin de sécurité
Jun 08, 2021	CVE-2020-8300	Bulletin de sécurité

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATE DE PUBLICATION	ID CVE	LIEN VERS LA RESSOURCE
Jun 08, 2021	CVE-2020-8299	Bulletin de sécurité
Sep 17, 2020	CVE-2020-8247	Bulletin de sécurité
Sep 17, 2020	CVE-2020-8246	Bulletin de sécurité
Sep 17, 2020	CVE-2020-8245	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8197	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8199	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8195	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8196	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8193	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8187	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8191	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8190	Bulletin de sécurité
Jul 07, 2020	CVE-2019-18177	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8194	Bulletin de sécurité
Jul 07, 2020	CVE-2020-8198	Bulletin de sécurité
Dec 17, 2019	CVE-2019-19781	Bulletin de sécurité

Identifier et corriger les vulnérabilités pour CVE-2026-88771

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88771. La liste des instances NetScaler impactées par CVE-2026-88771 s'affiche.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88771 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-88771

Pour les instances NetScaler impactées par CVE-2026-88771, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-88772

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88772. La liste des instances NetScaler impactées par CVE-2026-88772 s'affiche.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88772 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Corriger CVE-2026-88772

Pour les instances NetScaler impactées par CVE-2026-88772, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-88773

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88773. La liste des instances NetScaler impactées par CVE-2026-88773 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88773 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-88773

Pour les instances NetScaler impactées par CVE-2026-88773, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-88774

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88774. La liste des instances NetScaler impactées par CVE-2026-88774 s'affiche.

Tableau de bord des avis de sécurité pour CVE-2026-sep(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88774 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-88774

Pour les instances NetScaler impactées par CVE-2026-88774, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identifier et corriger les vulnérabilités pour CVE-2026-88775

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88775. La liste des instances NetScaler impactées par CVE-2026-88775 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88775 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-88775

Pour les instances NetScaler impactées par CVE-2026-88775, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-88776

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88776. La liste des instances NetScaler impactées par CVE-2026-88776 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88776 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-88776

Pour les instances NetScaler impactées par CVE-2026-88776, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-88777

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-88777. La liste des instances NetScaler impactées par CVE-2026-88777 s'affiche.

Tableau de bord des avis de sécurité pour CVE-2026-sep(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-88777 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Corriger CVE-2026-88777

Pour les instances NetScaler impactées par CVE-2026-88777, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Corriger les vulnérabilités pour CVE-2026-88778

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles** `<number of>` **Les instances NetScaler sont affectées par des CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2026-88778. Pour vérifier les détails des instances affectées par les CVE, sélectionnez CVE-2026-88778 et cliquez sur **Afficher les instances affectées**.



Corriger CVE-2026-88778

Pour les instances NetScaler affectées par CVE-2026-88778, la remédiation est un processus en deux étapes. Dans l'interface graphique, sous **CVE actuelles > Les instances NetScaler sont affectées par des CVE**, vous pouvez voir les étapes 1 et 2.



Les deux étapes incluent :

1. Mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration.

Sous **CVE actuelles > Les instances NetScaler sont affectées par des CVE**, vous voyez deux workflows distincts pour ce processus de remédiation en 2 étapes : **Passer au workflow de mise à niveau** et **Passer au workflow de tâche de configuration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 1 : Mettre à niveau les instances NetScaler affectées

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.



Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances affectées, dans la fenêtre **`<number of >` Les instances NetScaler sont affectées par des CVE**, sélectionnez l'instance affectée par CVE-2026-88778 et cliquez sur **Passer au workflow de tâche de configuration**. Le workflow comprend les étapes suivantes.

1. Personnalisation de la configuration.
2. Vérification des instances impactées pré-remplies.
3. Spécification des entrées pour les variables du travail.
4. Vérification de la configuration finale avec les entrées de variables renseignées.
5. Exécution du travail.

Gardez le point suivant à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au flux de travail du travail de configuration** :

- Pour plusieurs instances NetScaler qui sont impactées uniquement par CVE-2026-88778 : vous pouvez exécuter des tâches de configuration sur toutes les instances à la fois. Par exemple, vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et toutes sont impactées uniquement par CVE-2026-88778. Sélectionnez toutes ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail du travail de configuration, le modèle de base de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.



Étape 2 : Sélectionner l'instance

L'instance impactée est pré-remplie sous **Sélectionner les instances**. Sélectionnez l'instance. Cliquez sur **Suivant**. À l'étape suivante, prévisualisez les configurations. Cliquez sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour les instances NetScaler en mode cluster, en utilisant l'avis de sécurité, NetScaler Console prend en charge l'exécution du travail de configuration uniquement sur le nœud coordinateur de configuration de cluster (CCO). Exécutez les commandes sur les nœuds non-CCO séparément.

ÉTAPE 3 : EXÉCUTER LA CONFIGURATION

Cliquez sur **Terminer** pour exécuter la tâche de configuration.

Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

Identifier et corriger les vulnérabilités pour CVE-2026-19490

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-19490. La liste des instances NetScaler impactées par CVE-2026-19490 s'affiche.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-19490 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-19490

Pour les instances NetScaler impactées par CVE-2026-19490, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-19489

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-19489. La liste des instances NetScaler impactées par CVE-2026-19489 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-19489 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-19489

Pour les instances NetScaler impactées par CVE-2026-19489, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Corriger les vulnérabilités pour CVE-2026-13474

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVEs actuelles > `<number of>` Les instances NetScaler sont affectées par des vulnérabilités et expositions courantes (CVE)**, vous pouvez voir toutes les instances vulnérables en raison de cette CVE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

spécifique. Pour vérifier les détails des instances affectées par CVE-2026-13474, sélectionnez **CVE-2026-13474** et cliquez sur **Afficher les instances affectées**.

La fenêtre `<number of>` **Instances NetScaler affectées par des CVE** apparaît. Vous y voyez le nombre et les détails des instances NetScaler affectées par CVE-2026-13474.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

Corriger CVE-2026-13474

Pour les instances NetScaler affectées par CVE-2026-13474, la correction est un processus en deux étapes. Dans l'interface graphique, sous **CVEs actuelles > Les instances NetScaler sont affectées par des CVE**, vous pouvez voir les étapes 1 et 2.

Les deux étapes incluent :

1. Mise à niveau des instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.
2. Application des commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration.

Sous **CVEs actuelles > Instances NetScaler affectées par des CVE**, vous voyez deux flux de travail distincts pour ce processus de correction en 2 étapes, qui sont **Passer au flux de travail de mise à niveau** et **Passer au flux de travail des tâches de configuration**.

Étape 1 : Mettre à niveau les instances NetScaler affectées

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Flux de travail de mise à niveau pour CVE-2026-13474(/en-us/netscaler-application-delivery-management-software/media/cve-2026-13474-remediation-step-0.png)

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances impactées, dans la fenêtre `<number of>` **Instances NetScaler impactées par les CVE**, sélectionnez l'instance impactée par CVE-2026-13474 et

© 1997–2026 Citrix Systems, Inc. All rights reserved.

cliquez sur **Passer au flux de travail de la tâche de configuration**. Le flux de travail comprend les étapes suivantes.

1. Personnalisation de la configuration.
2. Examen des instances impactées pré-remplies.
3. Spécification des entrées pour les variables de la tâche.
4. Examen de la configuration finale avec les entrées de variables renseignées.
5. Exécution de la tâche.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au flux de travail de la tâche de configuration** :

- Pour plusieurs instances NetScaler impactées uniquement par CVE-2026-13474 : vous pouvez exécuter des tâches de configuration sur toutes les instances à la fois. Par exemple, vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et tous sont impactés uniquement par CVE-2026-13474. Sélectionnez toutes ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail de la tâche de configuration, le modèle de base de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.

Étapes de correction pour CVE-2026-13474(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-1.png)

ÉTAPE 2 : SÉLECTIONNER L'INSTANCE

L'instance impactée est automatiquement renseignée sous **Sélectionner les instances**. Sélectionnez les instances et cliquez sur **Suivant**. À l'étape suivante, prévisualisez les configurations et cliquez sur **Suivant**.

REMARQUE :

Pour les instances NetScaler en mode cluster, en utilisant l'avis de sécurité, la console NetScaler prend en charge l'exécution de la tâche de configuration uniquement sur le nœud coordinateur de configuration de cluster (CCO). Exécutez les commandes sur les nœuds non-CCO séparément.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTAPE 3 : EXÉCUTER LA CONFIGURATION

Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

Identifier et corriger les vulnérabilités pour CVE-2026-10817

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-10817. La liste des instances NetScaler impactées par CVE-2026-10817 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-10817 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-10817

Pour les instances NetScaler impactées par CVE-2026-10817, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identifier et corriger les vulnérabilités pour CVE-2026-10816

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Sous l'onglet **Instances impactées**, recherchez CVE-2026-10816. La liste des instances NetScaler impactées par CVE-2026-10816 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-10816 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-10816

Pour les instances NetScaler impactées par CVE-2026-10816, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-8655

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Sous l'onglet **Instances impactées**, recherchez CVE-2026-8655. La liste des instances NetScaler impactées par CVE-2026-8655 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-8655 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-8655

Pour les instances NetScaler impactées par CVE-2026-8655, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et un build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-8452

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-8452. La liste des instances NetScaler impactées par CVE-2026-8452 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-8452 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Corriger CVE-2026-8452

Pour les instances NetScaler impactées par CVE-2026-8452, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-8451

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-8451. La liste des instances NetScaler impactées par CVE-2026-8451 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-8451 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-8451

Pour les instances NetScaler impactées par CVE-2026-8451, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. Pour plus d'informations, consultez Détection CVE.

Identifier et corriger les vulnérabilités pour CVE-2026-4368

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-4368. La liste des instances NetScaler impactées par CVE-2026-4368 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-4368 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-4368

Pour les instances NetScaler impactées par CVE-2026-4368, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Identifier et corriger les vulnérabilités pour CVE-2026-3055

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2026-3055. La liste des instances NetScaler impactées par CVE-2026-3055 s'affiche.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2026-3055 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2026-3055

Pour les instances NetScaler impactées par CVE-2026-3055, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui incluent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Procéder au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.



Identifier et corriger les vulnérabilités pour CVE-2025-12101

Dans le tableau de bord des avis de sécurité de NetScaler Console®, cliquez sur **Détection CVE**. Dans l'onglet **Instances impactées**, recherchez CVE-2025-12101. La liste des instances NetScaler impactées par CVE-2025-12101 s'affiche.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-12101 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2025-12101

Pour les instances NetScaler impactées par CVE-2025-12101, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.

Dans l'interface graphique, sous **Détection CVE > Instances impactées**, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.



Identifier et corriger les vulnérabilités pour CVE-2025-8424

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles** `<number of>` **Les instances NetScaler sont affectées par des CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2025-8424. Pour vérifier les détails des instances affectées par les CVE, sélectionnez CVE-2025-8424 et cliquez sur **Afficher les instances affectées**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet **Journaux d'analyse** de l'avis de sécurité.

La fenêtre `<number of>` **Instances NetScaler affectées par des CVE** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler affectées par CVE-2025-8424.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-8424 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2025-8424

Pour les instances NetScaler affectées par CVE-2025-8424, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Dans l'interface graphique, sous **CVE actuelles > Les instances NetScaler sont affectées par des CVE**, vous pouvez voir l'étape de correction.

Sous **CVE actuelles > Instances NetScaler affectées par des CVE**, vous voyez le flux de travail suivant pour ce processus de correction en une seule étape, qui est **Passer au flux de travail de mise à niveau**.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Identifier et corriger les vulnérabilités pour CVE-2025-7776

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles** `<number of>` **Les instances NetScaler sont impactées par des CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2025-7776. Pour vérifier les détails des instances impactées par les CVE, sélectionnez CVE-2025-7776 et cliquez sur **Afficher les instances affectées**.

REMARQUE :

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet **Journaux d'analyse** de l'avis de sécurité.

La fenêtre `<number of>` **Instances NetScaler impactées par des CVE** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler impactées par CVE-2025-7776.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-7776 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2025-7776

Pour les instances NetScaler impactées par CVE-2025-7776, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Dans l'interface graphique, sous **CVE actuelles > Les instances NetScaler sont impactées par des CVE**, vous pouvez voir l'étape de correction.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sous **CVE actuelles > Instances NetScaler impactées par des CVE**, vous voyez le flux de travail suivant pour ce processus de correction en une seule étape, qui est **Passer au flux de travail de mise à niveau**.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Identifier et corriger les vulnérabilités pour CVE-2025-7775

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles** `<number of>` **Les instances NetScaler sont impactées par des CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2025-7775. Pour vérifier les détails des instances impactées par les CVE, sélectionnez CVE-2025-7775 et cliquez sur **Afficher les instances affectées**.

REMARQUE :

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet **Journaux d'analyse** de l'avis de sécurité.

La fenêtre `<number of>` **Instances NetScaler impactées par des CVE** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler impactées par CVE-2025-7775.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-7775 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2025-7775

Pour les instances NetScaler impactées par CVE-2025-7775, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Dans l'interface graphique, sous **CVE actuelles > Les instances NetScaler sont impactées par des CVE**, vous pouvez voir l'étape de correction.

Sous **CVE actuelles > Instances NetScaler impactées par des CVE**, vous voyez le flux de travail suivant pour ce processus de correction en une seule étape, qui est **Passer au flux de travail de mise à niveau**.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations de mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Identifier et corriger les vulnérabilités pour CVE-2025-6543

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVEs actuels** `<number of>` **Les instances NetScaler sont affectées par des CVEs**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2025-6543. Pour vérifier les détails des instances affectées par les CVEs, sélectionnez CVE-2025-6543 et cliquez sur **Afficher les instances affectées**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau de bord des avis de sécurité pour CVE-2025-6543(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2025-6543.png)

REMARQUE :

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet **Journaux d'analyse** de l'avis de sécurité.

La fenêtre `<number of>` **Instances NetScaler affectées par des CVEs** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler affectées par CVE-2025-6543.

Instances affectées par CVE-2025-6543(/en-us/netscaler-application-delivery-management-software/media/cve-2025-6543-impacted-instance.png)

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-6543 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2025-6543

Pour les instances NetScaler affectées par CVE-2025-6543, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Dans l'interface graphique, sous **CVEs actuels > Les instances NetScaler sont affectées par des CVEs**, vous pouvez voir l'étape de correction.

Sous **CVEs actuels > Instances NetScaler affectées par des CVEs**, vous voyez le workflow suivant pour ce processus de correction en une seule étape, qui est **Passer au workflow de mise à niveau**.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations de mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Identifier et corriger les vulnérabilités pour CVE-2025-5349

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles** `<number of>` **Instances NetScaler impactées par les CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2025-5349. Pour vérifier les détails des instances impactées par les CVE, sélectionnez CVE-2025-5349 et cliquez sur **Afficher les instances affectées**.

REMARQUE :

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet **Journaux d'analyse** dans Avis de sécurité.

La fenêtre `<number of>` **Instances NetScaler impactées par les CVE** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler impactées par CVE-2025-5349.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-5349 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Corriger CVE-2025-5349

Pour les instances NetScaler impactées par CVE-2025-5349, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Dans l'interface graphique, sous **CVE actuelles > Instances NetScaler impactées par les CVE**, vous pouvez voir l'étape de correction.

Sous **CVE actuelles > Instances NetScaler impactées par les CVE**, vous voyez le workflow suivant pour ce processus de correction en une seule étape, qui est **Passer au workflow de mise à niveau**.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

Corriger les vulnérabilités pour CVE-2025-5777

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles** `<number of>` **Les instances NetScaler sont affectées par des CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2025-5777. Pour vérifier les détails des instances affectées par les CVE, sélectionnez CVE-2025-5777 et cliquez sur **Afficher les instances affectées**.

REMARQUE :

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet **Journaux d'analyse** de l'avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La fenêtre `<number of>` **Instances NetScaler affectées par des CVE** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler affectées par CVE-2025-5777.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE :

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2025-5777 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2025-5777

Pour les instances NetScaler affectées par CVE-2025-5777, la correction est un processus en deux étapes. Dans l'interface graphique, sous **CVE actuelles > Les instances NetScaler sont affectées par des CVE**, vous pouvez voir les étapes 1 et 2.



Les deux étapes comprennent :

1. Mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration.

Sous **CVEs actuelles > Instances NetScaler impactées par les CVEs**, vous voyez deux workflows distincts pour ce processus de remédiation en 2 étapes : **Passer au workflow de mise à niveau** et **Passer au workflow de tâche de configuration**.

Étape 1 : Mettre à niveau les instances NetScaler vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances impactées, dans la fenêtre `<number of` **> Instances NetScaler impactées par les CVEs**, sélectionnez l'instance impactée par CVE-2025-5777 et cliquez sur **Passer au workflow de tâche de configuration**. Le workflow comprend les étapes suivantes.

1. Personnalisation de la configuration.
2. Examen des instances impactées pré-remplies.
3. Exécution de la tâche.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au workflow de tâche de configuration** :

- Pour une instance NetScaler impactée par plusieurs CVEs (telles que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, CVE-2021-22956 et CVE-2025-5777) : lorsque vous sélectionnez l'instance et cliquez sur **Passer au workflow de tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous **Sélectionner la configuration**. Vous devez faire glisser et déposer manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet de tâche de configuration sur le côté droit.
- Pour plusieurs instances NetScaler qui sont impactées uniquement par CVE-2025-5777 : vous pouvez exécuter des tâches de configuration sur toutes les instances en une seule fois. Par exemple, vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et toutes sont impactées uniquement par CVE-2025-5777. Sélectionnez toutes ces instances et cliquez sur **Passer au workflow de tâche de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances NetScaler impactées par CVE-2025-5777 et un ou plusieurs autres CVE (tels que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent que la remédiation soit appliquée à chaque NetScaler l'un après l'autre : lorsque vous sélectionnez ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, un message d'erreur apparaît vous indiquant d'exécuter la tâche de configuration sur chaque NetScaler l'un après l'autre.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail de la tâche de configuration, le modèle de base de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.



Étape 2 : Sélectionner l'instance

L'instance impactée est automatiquement renseignée sous **Sélectionner les instances**. Sélectionnez l'instance. Si cette instance fait partie d'une paire HA, sélectionnez **Exécuter sur les nœuds secondaires**. Cliquez sur **Suivant**.



REMARQUE :

Pour les instances NetScaler en mode cluster, en utilisant l'avis de sécurité, la console NetScaler prend en charge l'exécution de la tâche de configuration uniquement sur le nœud coordinateur de configuration de cluster (CCO). Exécutez les commandes sur les nœuds non-CCO séparément.

ÉTAPE 3 : EXÉCUTER LA TÂCHE

Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de remédiation pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

Corriger les vulnérabilités pour CVE-2024-8535

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVEs actuelles > `<number of>`** Les instances NetScaler sont impactées par des vulnérabilités et expositions courantes (CVEs), vous pouvez voir toutes les instances vulnérables en raison de cette CVE spécifique. Pour vérifier les détails des instances impactées par CVE-2024-8535, sélectionnez CVE-2024-8535 et cliquez sur **Afficher les instances affectées**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

La fenêtre `<number of>` Instances NetScaler impactées par les CVEs apparaît. Vous y voyez le nombre et les détails des instances NetScaler impactées par CVE-2024-8535.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE

Il peut falloir un certain temps pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2024-8535 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Corriger CVE-2024-8535

Pour les instances NetScaler impactées par CVE-2024-8535, la correction est un processus en deux étapes. Dans l'interface graphique, sous **CVEs actuelles > Instances NetScaler impactées par les CVEs**, vous pouvez voir les étapes 1 et 2.



Les deux étapes comprennent :

1. Mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contient le correctif.
2. Appliquer les commandes de configuration requises en utilisant le modèle de configuration intégré personnalisable dans les tâches de configuration.

Sous **CVEs actuelles > Instances NetScaler** impactées par les CVEs, vous voyez deux workflows distincts pour ce processus de correction en 2 étapes : qui sont **Passer au workflow de mise à niveau** et **Passer au workflow de tâche de configuration**.



Étape 1 : Mettre à niveau les instances NetScaler vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances impactées, dans la fenêtre `<number of` **> Instances NetScaler impactées par les CVE**, sélectionnez l'instance impactée par CVE-2024-8535 et cliquez sur **Passer au flux de travail de la tâche de configuration**.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au flux de travail de la tâche de configuration** :

- Pour une instance NetScaler impactée par plusieurs CVE (telles que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et cliquez sur **Passer au flux de travail de la tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous **Sélectionner la configuration**. Faites glisser et déposez manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet de la tâche de configuration sur le côté droit.
- Pour plusieurs instances NetScaler qui sont impactées uniquement par CVE-2024-8535, vous pouvez exécuter des tâches de configuration sur toutes les instances en une seule fois. Par exemple, vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et tous sont impactés uniquement par CVE-2024-8535. Sélectionnez toutes ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances NetScaler impactées par CVE-2024-8535 et une ou plusieurs autres CVE (telles que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent l'application d'une remédiation à chaque NetScaler individuellement : lorsque vous sélectionnez ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, un message d'erreur apparaît vous indiquant d'exécuter la tâche de configuration sur chaque NetScaler individuellement.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail de la tâche de configuration, le modèle de base de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 2 : Sélectionner l'instance

L'instance impactée est automatiquement renseignée sous **Sélectionner les instances**. Sélectionnez l'instance. Si cette instance fait partie d'une paire HA, sélectionnez **Exécuter sur les nœuds secondaires**. Cliquez sur **Suivant**.



REMARQUE :

Pour les instances NetScaler en mode cluster, en utilisant l'avis de sécurité, la console NetScaler prend en charge l'exécution de la tâche de configuration uniquement sur le nœud coordinateur de configuration de cluster (CCO). Exécutez les commandes sur les nœuds non-CCO séparément.

ÉTAPE 3 : SPÉCIFIER LES VALEURS DES VARIABLES

Aucune variable n'est requise à spécifier à cette étape. Sélectionnez **Valeurs de variables communes pour toutes les instances** et cliquez sur **Suivant**.

ÉTAPE 4 : PRÉVISUALISER LA CONFIGURATION

Prévisualisez les valeurs des variables insérées dans la configuration et cliquez sur **Suivant**.



ÉTAPE 5 : EXÉCUTER LA TÂCHE

Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

Corriger les vulnérabilités pour CVE-2020-8300

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles > `<number of>` Instances NetScaler impactées par des CVE**, vous pouvez voir toutes les instances vulnérables en raison de cette CVE spécifique. Pour vérifier les détails des instances impactées par CVE-2020-8300, sélectionnez **CVE-2020-8300** et cliquez sur **Afficher les instances affectées**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

La fenêtre `<number of>` **Instances NetScaler impactées par des CVE** apparaît. Vous y voyez le nombre et les détails des instances NetScaler impactées par CVE-2020-8300.



Corriger CVE-2020-8300

Pour les instances NetScaler impactées par CVE-2020-8300, la correction est un processus en deux étapes. Dans l'interface graphique, sous **CVE actuelles > Instances NetScaler impactées par des CVE**, vous pouvez voir les étapes 1 et 2.



Les deux étapes comprennent :

1. Mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contient le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration. Suivez cette étape pour chaque NetScaler vulnérable, une à la fois, et incluez toutes les actions SAML et les profils SAML pour ce NetScaler.

Sous **CVE actuelles > Instances NetScaler impactées par des CVE**, vous voyez deux workflows distincts pour ce processus de correction en 2 étapes : **Passer au workflow de mise à niveau** et **Passer au workflow de tâche de configuration**.



Étape 1 : Mettre à niveau les instances NetScaler vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Passer au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.



Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances concernées, dans la fenêtre `<number of` **> Instances NetScaler affectées par des CVE**, sélectionnez une instance affectée par CVE-2020-8300 et cliquez sur **Passer au flux de travail de la tâche de configuration**. Le flux de travail comprend les étapes suivantes.

1. Personnalisation de la configuration.
2. Examen des instances impactées pré-remplies.
3. Spécification des entrées pour les variables de la tâche.
4. Examen de la configuration finale avec les entrées de variables renseignées.
5. Exécution de la tâche.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au flux de travail de la tâche de configuration** :

- Pour une instance NetScaler affectée par plusieurs CVE (telles que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et cliquez sur **Passer au flux de travail de la tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous Sélectionner la configuration. Faites glisser et déposez manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet de tâche de configuration sur le côté droit.
- Pour plusieurs instances NetScaler qui sont impactées uniquement par CVE-2021-22956 : vous pouvez exécuter des tâches de configuration sur toutes les instances à la fois. Par exemple, vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et toutes sont impactées uniquement par CVE-2021-22956. Sélectionnez toutes ces instances et cliquez sur **Passer au flux de travail des tâches de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances NetScaler impactées par CVE-2021-22956 et un ou plusieurs autres CVE (tels que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent l'application d'une correction à chaque NetScaler une à la fois : lorsque vous sélectionnez ces instances et cliquez sur **Passer au flux de travail des tâches de configuration**, un message

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d'erreur apparaît vous indiquant d'exécuter la tâche de configuration sur chaque NetScaler une à la fois.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail des tâches de configuration, le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.

Exécutez une tâche de configuration distincte pour chaque instance NetScaler impactée, une à la fois, et incluez toutes les actions SAML et les profils SAML pour ce NetScaler. Par exemple, si vous avez deux instances NetScaler vulnérables ayant chacune deux actions SAML et deux profils SAML, vous devez exécuter cette tâche de configuration deux fois. Une fois par NetScaler, couvrant toutes ses actions SAML et ses profils SAML.

NETSCALER 1	NETSCALER 2
Tâche 1 : deux actions SAML + deux profils SAML	Tâche 2 : deux actions SAML + deux profils SAML

Donnez un nom à la tâche et personnalisez le modèle selon les spécifications suivantes. Le modèle de configuration intégré n'est qu'un aperçu ou un modèle de base. Personnalisez le modèle en fonction de votre déploiement pour les exigences suivantes :

a. **Actions SAML et leurs domaines associés**

Selon le nombre d'actions SAML que vous avez dans votre déploiement, vous devez reproduire les lignes 1 à 3 et personnaliser les domaines pour chaque action SAML.

Par exemple, si vous avez deux actions SAML, répétez les lignes 1 à 3 deux fois et personnalisez en conséquence les définitions de variables pour chaque action SAML.

Et si vous avez N domaines pour une action SAML, vous devez taper manuellement la ligne `bind patset $saml_action_patset$ “$saml_action_domain1$”` plusieurs fois pour vous assurer que la ligne apparaît N fois pour cette action SAML. Et modifiez les noms de définition de variable suivants :

- `saml_action_patset` : est la variable de modèle de configuration, et elle représente la valeur du nom de l'ensemble de motifs (patset) pour l'action SAML. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail du job de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `saml_action_domain1` : est la variable de modèle de configuration, et elle représente le nom de domaine pour cette action SAML spécifique. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail du job de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.

Pour trouver toutes les actions SAML pour un appareil, exécutez la commande `show samlaction`.

b. **Profils SAML et leurs URL associées**

Selon le nombre de profils SAML que vous avez dans votre déploiement, reproduisez les lignes 4 à 6. Personnalisez les URL pour chaque profil SAML.

Par exemple, si vous avez deux profils SAML, saisissez manuellement les lignes 4 à 6 deux fois et personnalisez en conséquence les définitions de variables pour chaque action SAML.

Et si vous avez N domaines pour une action SAML, vous devez taper manuellement la ligne `bind patset $saml_profile_patset$ “$saml_profile_url1$”` plusieurs fois pour vous assurer que la ligne apparaît N fois pour ce profil SAML. Et modifiez les noms de définition de variable suivants :

- `saml_profile_patset` : est la variable de modèle de configuration, et elle représente la valeur du nom de l'ensemble de motifs (patset) pour le profil SAML. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail du job de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.
- `saml_profile_url1` : est la variable de modèle de configuration, et elle représente le nom de domaine pour ce profil SAML spécifique. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail du job de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.

Pour trouver tous les profils SAM pour un appareil, exécutez la commande `show samlidpProfile`.

Étape 2 : Sélectionner l'instance

L'instance impactée est pré-remplie sous **Sélectionner les instances**. Sélectionnez l'instance et cliquez sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉTAPE 3 : SPÉCIFIER LES VALEURS DES VARIABLES

Saisissez les valeurs des variables.

- `saml_action_patset` : ajoutez un nom pour l'action SAML
- `saml_action_domain1` : saisissez un domaine au format `https://<example1.com>/`
- `saml_action_name` : saisissez le nom de l'action SAML pour laquelle vous configurez la tâche
- `saml_profile_patset` : ajoutez un nom pour le profil SAML
- `saml_profile_url1` : saisissez l'URL dans ce format `https://<example2.com>/cgi/samlauth`
- `saml_profile_name` : saisissez le nom du profil SAML pour lequel vous configurez la tâche

REMARQUE

Pour les URL, l'extension n'est pas toujours `cgi/samlauth`. Cela dépend de l'autorisation tierce que vous avez, et vous devez donc mettre l'extension en conséquence.



ÉTAPE 4 : PRÉVISUALISER LA CONFIGURATION

Prévisualise les valeurs des variables insérées dans la configuration et cliquez sur **Suivant**.

ÉTAPE 5 : EXÉCUTER LA TÂCHE

Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour afficher la posture de sécurité révisée.

Points à noter pour le compte NetScaler Console Express

Le compte NetScaler Console Express dispose de fonctionnalités limitées, qui incluent des limitations de deux tâches de configuration seulement.

Pour la correction de CVE-2020-8300, vous devez exécuter autant de tâches de configuration que le nombre de vos instances NetScaler vulnérables. Ainsi, si vous avez un compte Express et que

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vous devez exécuter plus de deux tâches de configuration, suivez cette solution de contournement.

Solution de contournement : Exécutez deux tâches de configuration pour deux instances NetScaler vulnérables, puis supprimez les deux tâches pour continuer à exécuter les deux tâches suivantes pour les deux instances NetScaler vulnérables suivantes. Continuez ainsi jusqu'à ce que vous ayez couvert toutes les instances vulnérables. Avant de supprimer les tâches, vous pouvez télécharger le rapport pour référence future. Pour télécharger le rapport, sous **Réseau > Tâches**, sélectionnez les tâches et cliquez sur **Télécharger** sous **Actions**.

Exemple : Si vous avez six instances NetScaler vulnérables, exécutez deux tâches de configuration sur deux instances vulnérables respectivement, puis supprimez les deux tâches de configuration. Répétez cette étape deux fois de plus. Au final, vous auriez exécuté six tâches de configuration pour six instances NetScaler respectivement. Dans l'interface utilisateur de NetScaler Console, sous **Infrastructure > Tâches**, vous ne voyez que les deux dernières tâches de configuration.

Scénario

Dans ce scénario, trois instances NetScaler sont vulnérables à CVE-2020-8300 et vous devez corriger toutes les instances. Suivez ces étapes :

1. Mettez à niveau les trois instances NetScaler en suivant les étapes indiquées dans la section **Mettre à niveau une instance** de ce document.
2. Appliquez le correctif de configuration à une instance NetScaler à la fois, à l'aide du flux de travail des tâches de configuration. Consultez les étapes indiquées dans la section **Appliquer les commandes de configuration** de ce document.

Le NetScaler 1 vulnérable a la configuration suivante :

DEUX ACTIONS SAML	DEUX PROFILS SAML

Sélectionnez NetScaler 1 et cliquez sur **Proceed to configuration job workflow**. Le modèle intégré se remplit automatiquement. Ensuite, donnez un nom de tâche et personnalisez le modèle en fonction de la configuration donnée.

Les tableaux suivants répertorient les définitions de variables pour les paramètres personnalisés.

Tableau 1. Définitions de variables pour l'action SAML

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONFIGURATION NETSCALER	DÉFINITION DE VARIABLE POUR PATSET	DÉFINITION DE VARIABLE POUR LE NOM DE L'ACTION SAML	DÉFINITION DE VARIABLE POUR LE DOMAINE
L'action SAML 1 a un domaine	saml_action_patset1	saml_action_name1	saml_action_domain 1
L'action SAML 2 possède deux domaines	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

Tableau 2. Définitions des variables pour le profil SAML

CONFIGURATION NETSCALER	DÉFINITION DE VARIABLE POUR PATSET	DÉFINITION DE VARIABLE POUR LE NOM DU PROFIL SAML	DÉFINITION DE VARIABLE POUR L'URL
Le profil SAML 1 possède une URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
Le profil SAML 2 comporte deux URL	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

Sous **Sélectionner les instances**, sélectionnez NetScaler 1 et cliquez sur **Suivant**. La fenêtre **Spécifier les valeurs des variables** apparaît. Dans cette étape, vous devez fournir des valeurs pour toutes les variables définies à l'étape précédente.

- [ ] Ensuite, examinez les variables.

Cliquez sur **Suivant**, puis sur **Terminer** pour exécuter la tâche.

Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour NetScaler1, suivez les mêmes étapes pour corriger NetScaler 2 et NetScaler 3. Une fois la correction terminée, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Corriger les vulnérabilités pour CVE-2021-22927 et CVE-2021-22920

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles > `<number of>` Instances NetScaler impactées par les CVE**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2021-22927 et CVE-2021-22920. Pour vérifier les détails des instances impactées par ces deux CVE, sélectionnez une ou plusieurs CVE et cliquez sur **Afficher les instances affectées**.



REMARQUE

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2021-22927 et CVE-2021-22920 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité. La fenêtre **`<number of>` Instances NetScaler impactées par les CVE** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler impactées par CVE-2021-22927 et CVE-2021-22920.



Corriger CVE-2021-22927 et CVE-2021-22920

Pour les instances NetScaler impactées par CVE-2021-22927 et CVE-2021-22920, la correction est un processus en deux étapes. Dans l'interface graphique, sous **CVE actuelles > Instances NetScaler impactées par les CVE**, vous pouvez voir les étapes 1 et 2.



Les deux étapes comprennent :

1. Mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contient le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration. Suivez cette étape pour chaque NetScaler vulnérable, un à la fois, et incluez toutes les actions SAML pour ce NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Ignore l'étape 2 si vous avez déjà exécuté des tâches de configuration sur l'instance NetScaler pour CVE-2020-8300.

Sous **CVEs actuelles > Instances NetScaler impactées par les CVEs**, vous voyez deux workflows distincts pour ce processus de remédiation en 2 étapes : **Procéder au workflow de mise à niveau** et **Procéder au workflow de tâche de configuration**.



Étape 1 : Mettre à niveau les instances NetScaler vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.



Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

REMARQUE

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables. **Remarque**

Une fois l'étape 1 terminée pour toutes les instances NetScaler vulnérables aux CVE-2021-22920 et CVE-2021-22927, effectuez une analyse à la demande. La posture de sécurité mise à jour sous **CVEs actuelles** vous aide à comprendre si les instances NetScaler sont toujours vulnérables à l'une de ces CVEs. À partir de la nouvelle posture, vous pouvez également vérifier si vous devez exécuter des tâches de configuration. Si vous avez déjà appliqué les tâches de configuration appropriées à l'instance NetScaler pour CVE-2020-8300 et que vous avez maintenant mis à niveau l'instance NetScaler, après avoir effectué l'analyse à la demande, l'instance n'apparaît plus comme vulnérable pour CVE-2020-8300, CVE-2021-22920 et CVE-2021-22927.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances impactées, dans la fenêtre `<number of>` **Instances NetScaler impactées par les CVEs**, sélectionnez une instance impactée par CVE-2021-22927 et

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2021-22920 et cliquez sur **Procéder au workflow de tâche de configuration**. Le workflow comprend les étapes suivantes.

1. Personnalisation de la configuration.
2. Examen des instances impactées pré-remplies.
3. Spécification des entrées pour les variables de la tâche.
4. Vérification de la configuration finale avec les entrées variables renseignées.
5. Exécution du travail.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au flux de travail du travail de configuration** :

- Pour une instance NetScaler affectée par plusieurs CVE (telles que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et cliquez sur **Passer au flux de travail du travail de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous Sélectionner la configuration. Faites glisser et déposez manuellement le modèle de travail de configuration approprié sous **Modèle d'avis de sécurité** dans le volet du travail de configuration sur le côté droit.
- Pour plusieurs instances NetScaler qui ne sont affectées que par CVE-2021-22956 : vous pouvez exécuter des travaux de configuration sur toutes les instances à la fois. Par exemple, si vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et que tous sont affectés uniquement par CVE-2021-22956. Sélectionnez toutes ces instances et cliquez sur **Passer au flux de travail du travail de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances NetScaler affectées par CVE-2021-22956 et une ou plusieurs autres CVE (telles que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent l'application d'une correction à chaque NetScaler l'un après l'autre : lorsque vous sélectionnez ces instances et cliquez sur **Passer au flux de travail du travail de configuration**, un message d'erreur apparaît vous indiquant d'exécuter le travail de configuration sur chaque NetScaler l'un après l'autre.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail du travail de configuration, le modèle de base de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si l'instance NetScaler sélectionnée à l'étape 2 pour l'application des commandes de configuration est vulnérable à CVE-2021-22927, CVE-2021-22920 et également à CVE-2020-8300, le modèle de base pour CVE-2020-8300 est automatiquement renseigné. Le modèle CVE-2020-8300 est un sur-ensemble des commandes de configuration requises pour les trois CVE. Personnalisez ce modèle de base en fonction du déploiement et des exigences de votre instance NetScaler.

Vous devez exécuter un travail de configuration distinct pour chaque instance NetScaler affectée, une à la fois, et inclure toutes les actions SAML pour ce NetScaler. Par exemple, si vous avez deux instances NetScaler vulnérables ayant chacune deux actions SAML, vous devez exécuter ce travail de configuration deux fois. Une fois par NetScaler, couvrant toutes ses actions SAML.

NETSCALER 1	NETSCALER 2
Travail 1 : deux actions SAML	Tâche 2 : deux actions SAML

Donnez un nom à la tâche et personnalisez le modèle selon les spécifications suivantes. Le modèle de configuration intégré n'est qu'un aperçu ou un modèle de base. Personnalisez le modèle en fonction de votre déploiement pour les exigences suivantes :

a. **Actions SAML et leurs domaines associés**

Selon le nombre d'actions SAML que vous avez dans votre déploiement, vous devez reproduire les lignes 1 à 3 et personnaliser les domaines pour chaque action SAML.

Par exemple, si vous avez deux actions SAML, répétez les lignes 1 à 3 deux fois et personnalisez en conséquence les définitions de variables pour chaque action SAML.

Et si vous avez N domaines pour une action SAML, vous devez taper manuellement la ligne `bind patset $saml_action_patset$ “$saml_action_domain1$”` plusieurs fois pour vous assurer que la ligne apparaît N fois pour cette action SAML. Et modifiez les noms de définition de variable suivants :

- `saml_action_patset` : est la variable du modèle de configuration, et elle représente la valeur du nom de l'ensemble de motifs (patset) pour l'action SAML. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de la tâche de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `saml_action_domain1` : est la variable du modèle de configuration, et elle représente le nom de domaine pour cette action SAML spécifique. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de la tâche de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.

Pour trouver toutes les actions SAML pour un appareil, exécutez la commande `show samlaction`.

Étape 2 : Sélectionner l'instance

L'instance impactée est automatiquement renseignée sous **Sélectionner les instances**. Sélectionnez l'instance et cliquez sur **Suivant**.

ÉTAPE 3 : SPÉCIFIER LES VALEURS DES VARIABLES

Saisissez les valeurs des variables.

- `saml_action_patset` : ajoutez un nom pour l'action SAML
- `saml_action_domain1` : saisissez un domaine au format `https://<example1.com>/`
- `saml_action_name` : saisissez le nom de l'action SAML pour laquelle vous configurez la tâche

ÉTAPE 4 : PRÉVISUALISER LA CONFIGURATION

Prévisualisez les valeurs des variables insérées dans la configuration et cliquez sur **Suivant**.

ÉTAPE 5 : EXÉCUTER LA TÂCHE

Cliquez sur **Terminer** pour exécuter la tâche de configuration.

Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scénario

Dans ce scénario, deux instances NetScaler sont vulnérables à CVE-2021-22920, et vous devez corriger toutes les instances. Suivez ces étapes :

1. Mettez à niveau les trois instances NetScaler en suivant les étapes indiquées dans la section « Mettre à niveau une instance » de ce document.
2. Appliquez le correctif de configuration à un NetScaler à la fois, en utilisant le flux de travail de tâche de configuration. Consultez les étapes indiquées dans la section « Appliquer les commandes de configuration » de ce document.

Le NetScaler 1 vulnérable a deux actions SAML :

- L'action SAML 1 a un domaine
- L'action SAML 2 a deux domaines

Démarrer un flux de travail de tâche de configuration (/en-us/netscaler-application-delivery-management-software/media/scenario-config-job-workflow-cve-2021-22927-2021-22920.png)

Sélectionnez NetScaler 1 et cliquez sur **Passer au flux de travail de tâche de configuration**. Le modèle de base intégré se remplit automatiquement. Ensuite, donnez un nom de tâche et personnalisez le modèle selon la configuration donnée.

Personnaliser le modèle pour le scénario donné (/en-us/netscaler-application-delivery-management-software/media/scenario-customize-template-cve-2021-22927-2021-22920.png)

Le tableau suivant répertorie les définitions de variables pour les paramètres personnalisés.

Tableau. Définitions de variables pour l'action SAML

CONFIGURATION NETSCALER	DÉFINITION DE VARIABLE POUR PATSET	DÉFINITION DE VARIABLE POUR LE NOM DE L'ACTION SAML	DÉFINITION DE VARIABLE POUR LE DOMAINE
L'action SAML 1 a un domaine	saml_action_patset1	saml_action_name1	saml_action_domain 1
L'action SAML 2 a deux domaines	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sous **Sélectionner les instances**, sélectionnez NetScaler 1 et cliquez sur **Suivant**. La fenêtre **Spécifier les valeurs des variables** apparaît. Dans cette étape, vous devez fournir des valeurs pour toutes les variables définies à l'étape précédente.

- [ ] Ensuite, examinez les variables.

- [ ] Cliquez sur **Suivant**, puis sur **Terminer** pour exécuter la tâche.

Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour NetScaler1, suivez les mêmes étapes pour corriger NetScaler 2 et NetScaler 3. Une fois la correction terminée, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

Identifier et corriger les vulnérabilités pour CVE-2021-22956

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVE actuelles >** `<number of>` Les instances NetScaler sont affectées par des vulnérabilités et expositions communes (CVE), vous pouvez voir toutes les instances vulnérables en raison de cette CVE spécifique. Pour vérifier les détails des instances affectées par CVE-2021-22956, sélectionnez CVE-2021-22956 et cliquez sur **Afficher les instances affectées**.

- [ ] La fenêtre `<number of>` Instances NetScaler affectées par les CVE apparaît. Vous y voyez le nombre et les détails des instances NetScaler affectées par CVE-2021-22956.

- [ ] Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE

Il peut s'écouler un certain temps avant que l'analyse du système d'avis de sécurité ne se termine et ne reflète l'impact de CVE-2021-22956 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Identifier les instances affectées par CVE-2021-22956

CVE-2021-22956 nécessite une analyse personnalisée, dans laquelle le service NetScaler Console se connecte à l'instance NetScaler gérée et pousse un script vers l'instance. Le script

© 1997–2026 Citrix Systems, Inc. All rights reserved.

s'exécute sur l'instance NetScaler et vérifie le fichier de configuration Apache (`httpd.conf file`) et les paramètres de connexions client maximales (`maxclient`) pour déterminer si une instance est vulnérable ou non. Les informations que le script partage avec le service NetScaler Console sont l'état de la vulnérabilité en booléen (vrai ou faux). Le script renvoie également au service NetScaler Console une liste de comptes pour max_clients pour différentes interfaces réseau, par exemple l'hôte local, NSIP et SNIP avec accès de gestion.

Ce script s'exécute chaque fois que vos analyses planifiées ou à la demande sont exécutées. Une fois l'analyse terminée, le script est supprimé de l'instance NetScaler.

Corriger CVE-2021-22956

Pour les instances NetScaler affectées par CVE-2021-22956, la correction est un processus en deux étapes. Dans l'interface graphique, sous **CVE actuelles > Les instances NetScaler sont affectées par les CVE**, vous pouvez voir les étapes 1 et 2.

Les deux étapes incluent :

1. Mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contient le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration.

Sous « CVEs actuelles > Instances NetScaler impactées par les CVEs », vous voyez deux workflows distincts pour ce processus de correction en 2 étapes : « Procéder au workflow de mise à niveau » et « Procéder au workflow de tâche de configuration ».

Étape 1 : Mettre à niveau les instances NetScaler vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Cette étape peut être effectuée en une seule fois pour toutes les instances NetScaler vulnérables.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances impactées, dans la fenêtre `<number of` **> Instances NetScaler impactées par les CVEs**, sélectionnez l'instance impactée par CVE-2021-2295 et cliquez sur **Procéder au workflow de tâche de configuration**. Le workflow comprend les étapes suivantes.

1. Personnalisation de la configuration.
2. Examen des instances impactées pré-remplies.
3. Spécification des entrées pour les variables de la tâche.
4. Examen de la configuration finale avec les entrées de variables renseignées.
5. Exécution de la tâche.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Passer au flux de travail de la tâche de configuration** :

- Pour une instance NetScaler affectée par plusieurs CVE (telles que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et cliquez sur **Passer au flux de travail de la tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous Sélectionner la configuration. Faites glisser et déposez manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet de la tâche de configuration sur le côté droit.
- Pour plusieurs instances NetScaler affectées uniquement par CVE-2021-22956 : vous pouvez exécuter des tâches de configuration sur toutes les instances à la fois. Par exemple, vous avez NetScaler 1, NetScaler 2 et NetScaler 3, et tous sont affectés uniquement par CVE-2021-22956. Sélectionnez toutes ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, et le modèle de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances NetScaler affectées par CVE-2021-22956 et une ou plusieurs autres CVE (telles que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent que la correction soit appliquée à chaque NetScaler individuellement : lorsque vous sélectionnez ces instances et cliquez sur **Passer au flux de travail de la tâche de configuration**, un

© 1997–2026 Citrix Systems, Inc. All rights reserved.

message d'erreur apparaît vous indiquant d'exécuter la tâche de configuration sur chaque NetScaler individuellement.

ÉTAPE 1 : SÉLECTIONNER LA CONFIGURATION

Dans le flux de travail de la tâche de configuration, le modèle de base de configuration intégré se remplit automatiquement sous **Sélectionner la configuration**.



Étape 2 : Sélectionner l'instance

L'instance affectée est automatiquement renseignée sous **Sélectionner les instances**. Sélectionnez l'instance. Si cette instance fait partie d'une paire HA, sélectionnez **Exécuter sur les nœuds secondaires**. Cliquez sur **Suivant**.



REMARQUE

Pour les instances NetScaler en mode cluster, en utilisant l'avis de sécurité de NetScaler Console, NetScaler Console prend en charge l'exécution de la tâche de configuration uniquement sur le nœud coordinateur de configuration de cluster (CCO). Exécutez les commandes sur les nœuds non-CCO séparément.

`rc.netscaler` est synchronisé sur tous les nœuds HA et de cluster, rendant la correction persistante après chaque redémarrage.

ÉTAPE 3 : SPÉCIFIER LES VALEURS DES VARIABLES

Saisissez les valeurs des variables.



Sélectionnez l'une des options suivantes pour spécifier les variables de vos instances :

Valeurs de variable communes à toutes les instances : Saisissez une valeur commune pour la variable `max_client`.

Charger le fichier d'entrée pour les valeurs des variables : Cliquez sur **Télécharger le fichier de clés d'entrée** pour télécharger un fichier d'entrée. Dans le fichier d'entrée, saisissez les valeurs de la variable `max_client`, puis téléchargez le fichier sur le serveur NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Pour les deux options mentionnées ci-dessus, la valeur `max_client` recommandée est 30. Vous pouvez définir la valeur en fonction de votre valeur actuelle. Cependant, elle ne doit pas être nulle et doit être inférieure ou égale à la valeur max_client définie dans le fichier `/etc/httpd.conf`. Vous pouvez vérifier la valeur actuelle définie dans le fichier de configuration du serveur HTTP Apache `/etc/httpd.conf` en recherchant la chaîne `MaxClients`, dans l'instance NetScaler.

ÉTAPE 4 : PRÉVISUALISER LA CONFIGURATION

Prévisualisez les valeurs des variables insérées dans la configuration et cliquez sur **Suivant**.



ÉTAPE 5 : EXÉCUTER LA TÂCHE

Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour toutes les instances NetScaler vulnérables, vous pouvez exécuter une analyse à la demande pour voir la posture de sécurité révisée.

Identifier et corriger les vulnérabilités pour CVE-2022-27509

Dans le tableau de bord des avis de sécurité de NetScaler Console, sous **CVEs actuelles** **`<number of>`** **Instances NetScaler impactées par les CVEs**, vous pouvez voir toutes les instances vulnérables en raison de CVE-2022-27509. Pour vérifier les détails des instances impactées par les CVEs, sélectionnez CVE-2022-27509 et cliquez sur **Afficher les instances affectées**.



REMARQUE

Pour comprendre la raison de la vulnérabilité de NetScaler, téléchargez le rapport CSV dans l'onglet Journaux d'analyse de l'avis de sécurité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La fenêtre `<number of>` **Instances NetScaler impactées par les CVEs** apparaît. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances NetScaler impactées par CVE-2022-27509.



Pour plus d'informations sur le tableau de bord des avis de sécurité, consultez Avis de sécurité.

REMARQUE

Il peut falloir quelques heures pour que l'analyse du système d'avis de sécurité se termine et reflète l'impact de CVE-2022-27509 dans le module d'avis de sécurité. Pour voir l'impact plus tôt, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

Identifier les instances impactées par CVE-2022-27509

CVE-2022-27509 nécessite une combinaison d'analyse personnalisée et d'analyse de version. Dans le cadre de l'analyse personnalisée, le service NetScaler Console se connecte à l'instance NetScaler gérée et envoie un script à l'instance. Le script s'exécute sur l'instance NetScaler et détermine si l'instance est vulnérable. Ce script s'exécute chaque fois que votre analyse planifiée ou à la demande est exécutée.

Une fois l'analyse terminée, le script est supprimé de l'instance NetScaler.

Vous pouvez également désactiver ces analyses personnalisées d'avis de sécurité. Pour plus d'informations sur les paramètres d'analyse personnalisée et la désactivation des analyses personnalisées, consultez la section **Configurer les paramètres d'analyse personnalisée** sur la page **Avis de sécurité**.

Corriger CVE-2022-27509

Pour les instances NetScaler impactées par CVE-2022-27509, la correction est un processus en une seule étape et vous devez mettre à niveau les instances NetScaler vulnérables vers une version et une build qui contiennent le correctif. Dans l'interface graphique, sous **CVEs actuelles > Instances NetScaler impactées par les CVEs**, vous pouvez voir l'étape de correction.

Sous **CVEs actuelles > Instances NetScaler impactées par les CVEs**, vous voyez le workflow suivant pour ce processus de correction en une seule étape, qui est **Procéder au workflow de mise à niveau**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au workflow de mise à niveau**. Le workflow de mise à niveau s'ouvre avec les instances NetScaler vulnérables déjà renseignées.

IMPORTANT

Si votre ou vos instances NetScaler vulnérables ont le fichier /etc/httpd.conf copié dans le répertoire /nsconfig, consultez Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler Console pour mettre à niveau les instances NetScaler, consultez Créer une tâche de mise à niveau NetScaler.



CVE non prises en charge dans l'avis de sécurité

L'avis de sécurité de NetScaler Console suit toutes les nouvelles vulnérabilités et expositions courantes (CVE) et évalue l'impact des CVE sur l'infrastructure. Vous pouvez examiner les recommandations et prendre les mesures appropriées. Cependant, quelques CVE ne sont pas prises en charge et la détection et la correction des vulnérabilités sont hors du champ d'application de l'avis de sécurité de NetScaler Console.

- **CVE-2022-21827** :

  La CVE-2022-21827 affecte le plug-in NetScaler Gateway pour Windows dans les versions prises en charge antérieures à 21.9.1.2.

  La détection et la correction des vulnérabilités affectant le plug-in NetScaler Gateway pour Windows ne sont pas prises en charge par NetScaler Console. De plus, les vulnérabilités du plug-in NetScaler Gateway ne peuvent pas être évaluées en effectuant des vérifications côté NetScaler, en vérifiant la version de NetScaler ou en vérifiant la configuration de NetScaler. La détection et la correction de cette CVE ne peuvent être évaluées qu'en fonction de la version du plug-in NetScaler Gateway pour Windows déployée sur le client.

  Par conséquent, la détection et la correction de cette vulnérabilité sont hors du champ d'application de l'avis de sécurité de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Avis de mise à niveau

À partir de la version 14.1 build 66.x de NetScaler Console, la fonctionnalité d'avis de mise à niveau est entièrement prise en charge. Vous pouvez accéder et utiliser cette fonctionnalité en activant Cloud Connect. L'avis de mise à niveau est automatiquement activé une fois que Cloud Connect est correctement établi.

IMPORTANT

Assurez-vous que Cloud Connect est entièrement activé et que toutes les conditions préalables sont remplies. Tout problème de connexion à Cloud Connect rendra l'avis de mise à niveau indisponible.



En tant qu'administrateur réseau, vous pouvez gérer de nombreuses instances NetScaler exécutées sur différentes versions de NetScaler dans NetScaler Console. Le suivi du cycle de vie de chaque instance NetScaler peut être une tâche fastidieuse. Vous devez consulter la Matrice des produits NetScaler, identifier les instances NetScaler qui atteignent ou ont atteint la fin de vie (EOL) ou la fin de maintenance (EOM). Ensuite, planifiez leur mise à niveau.

Pour faciliter ce processus, l'avis de mise à niveau de NetScaler Console vous aide à surveiller le cycle de vie de vos instances NetScaler de la manière suivante :

- Identifie les instances atteignant ou ayant atteint l'EOL ou l'EOM. Ainsi, vous pouvez planifier les mises à niveau de NetScaler avant la date d'EOL ou d'EOM.
- Met en évidence les instances qui ne sont pas sur la dernière version ou build. Vous pouvez mettre à niveau ces instances vers la dernière version ou build. Grâce à cette mise à niveau, vous recevez des mises à jour sur les nouvelles fonctionnalités et les problèmes résolus.
- Met en évidence les instances qui ne sont pas sur les builds NetScaler préférées. Certaines organisations peuvent avoir une build NetScaler préférée pour leurs instances. Dans NetScaler Console, vous pouvez définir la build préférée pour votre organisation en fonction de la stabilité de la build, des fonctionnalités et d'autres considérations. Ensuite, examinez et mettez à niveau les instances qui ne sont pas sur les builds préférées. Les instances exécutant les builds préférées sont indiquées par une icône en forme d'étoile.
- Met en évidence les instances exécutant les versions ou builds les plus populaires. Les instances exécutant les builds populaires sont indiquées par une icône en forme de ruban.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'avis de mise à niveau fournit des liens vers les notes de publication correspondantes. Grâce à ces informations, vous pouvez examiner et décider d'une build NetScaler pour la mise à niveau. Vous pouvez ensuite créer une tâche de maintenance pour mettre à niveau les instances NetScaler depuis la page d'avis de mise à niveau.

IMPORTANT :

L'avis de mise à niveau ne surveille que l'EOL des versions logicielles de NetScaler. Il ne vérifie pas l'EOL des appliances NetScaler.

Afficher l'avis de mise à niveau

Accédez à **Infrastructure > Instance Advisory > Upgrade Advisory** et consultez les informations suivantes :

- Nombre total d'instances NetScaler.
- Instances arrivant en fin de vie.
- Instances arrivant en fin de maintenance.
- Instances dans une version plus ancienne.
- Instances ne correspondant pas à la version préférée.
- Dates de fin de vie et de fin de maintenance pour les différentes versions de NetScaler.



La page **Upgrade Advisory** regroupe les instances NetScaler par leurs versions. Le lien **Release Notes** vous dirige vers les notes de publication spécifiques de NetScaler. Passez en revue les nouvelles fonctionnalités, les problèmes résolus et les problèmes connus avant de décider de la mise à niveau. Vous pouvez sélectionner plusieurs instances NetScaler de différentes versions à mettre à niveau en même temps. Lorsque vous procédez à une mise à niveau, cela crée une tâche de mise à niveau. Voir, Mettre à niveau les instances NetScaler.

Définir les versions préférées

En tant qu'administrateur, vous pouvez définir une version NetScaler préférée pour l'organisation. Procédez comme suit pour définir la version préférée :

1. Dans **Infrastructure > Instance Advisory > Upgrade Advisory**, cliquez sur **Settings**.
2. Sélectionnez la version et la build préférées.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, les versions préférées sont `13.0-58.30` et `13.0-67.39`.

3. Cliquez sur **Enregistrer**.

Mettre à niveau les instances NetScaler

Dans la page **Avis de mise à niveau**, après votre examen, effectuez les étapes suivantes pour mettre à niveau les instances NetScaler requises :

1. Sélectionnez les versions d'instance que vous souhaitez mettre à niveau et cliquez sur **Sélectionner les instances à mettre à niveau**.
2. Sélectionnez l'instance NetScaler que vous souhaitez mettre à niveau et cliquez sur **Passer au flux de travail de mise à niveau**.

   Ce flux de travail crée une tâche de mise à niveau.
3. Dans l'onglet **Sélectionner l'instance**,
   a. Spécifiez un nom pour la tâche de mise à niveau.
   b. (Facultatif) si vous souhaitez ajouter d'autres instances, cliquez sur **Ajouter des instances**.
   c. Cliquez sur **Suivant**.
4. Dans l'onglet **Sélectionner l'image**, sélectionnez une image NetScaler à partir de la bibliothèque d'images, locale ou de l'appliance.

   - **Sélectionner dans la bibliothèque d'images** : Sélectionnez une image NetScaler dans la liste. Cette option répertorie toutes les images NetScaler disponibles sur le site Web de téléchargement NetScaler.

     Les images logicielles NetScaler affichent les versions préférées avec l'icône en forme d'étoile. Et, les versions les plus téléchargées avec l'icône en forme de signet.
   - **Sélectionner depuis l'ordinateur local ou l'appliance** : Vous pouvez télécharger l'image depuis votre ordinateur local ou l'appliance NetScaler. Lorsque vous sélectionnez l'appliance NetScaler, l'interface graphique de NetScaler Console affiche les fichiers d'instance présents dans `/var/mps/mps_images`. Sélectionnez l'image depuis l'interface graphique de NetScaler Console.
   - **Ignorer le téléchargement de l'image vers NetScaler si l'image sélectionnée est déjà disponible** - Cette option vérifie si l'image sélectionnée est disponible dans NetScaler. La

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tâche de mise à niveau ignore le téléchargement d'une nouvelle image et utilise l'image disponible dans NetScaler.

- **Nettoyer l'image logicielle de NetScaler après une mise à niveau réussie** - Cette option efface l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.

Cliquez sur **Suivant** pour démarrer la validation avant la mise à niveau sur les instances sélectionnées.

5. L'onglet **Validation avant la mise à niveau** affiche les instances ayant échoué. Vous pouvez supprimer les instances ayant échoué et cliquer sur **Suivant**.

   - **Vérification de l'espace disque** : Si vous rencontrez un espace disque insuffisant sur une instance, vous pouvez vérifier et nettoyer l'espace disque. Voir, Nettoyer l'espace disque de NetScaler.
   - **Vérification des politiques** : Si NetScaler Console détecte des politiques classiques non prises en charge, vous pouvez supprimer ces politiques pour créer une tâche de mise à niveau.

   REMARQUE :

   Si vous spécifiez l'adresse IP du cluster, NetScaler Console effectue la validation avant la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

6. Facultatif, dans l'onglet **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance.

   Pour plus d'informations, consultez Utiliser des scripts personnalisés.

7. Dans la **Tâche de planification**, sélectionnez l'une des options suivantes :

   - **Mettre à niveau maintenant** - La tâche de mise à niveau s'exécute immédiatement.
   - **Planifier ultérieurement** - Sélectionnez cette option pour exécuter cette tâche de mise à niveau ultérieurement. Spécifiez la **Date d'exécution** et l'**Heure de début** auxquelles vous souhaitez mettre à niveau les instances.

   Si vous souhaitez mettre à niveau une paire NetScaler haute disponibilité en deux étapes, sélectionnez Effectuer une mise à niveau en deux étapes pour les nœuds en HA.

   Pour plus d'informations, consultez Mettre à niveau une paire NetScaler haute disponibilité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Dans l'onglet **Créer une tâche**, spécifiez les détails suivants :

   Si vous planifiez la tâche de mise à niveau, vous pouvez spécifier quand vous souhaitez télécharger l'image vers une instance :

   - **Télécharger maintenant** : Sélectionnez cette option pour télécharger l'image immédiatement. Cependant, la tâche de mise à niveau s'exécute à l'heure prévue.
   - **Télécharger au moment de l'exécution** : Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.

Pour plus d'informations sur les autres options, consultez Options de mise à niveau NetScaler.

Orchestration

Dans les réseaux définis par logiciel (SDN), un contrôleur d'application logicielle gère un réseau et ses activités au lieu du matériel qui prend en charge le réseau. Autrement dit, le SDN permet aux administrateurs réseau de virtualiser une connectivité réseau physique en une connectivité réseau logique et de gérer les services réseau à l'aide d'un outil de gestion centralisé basé sur logiciel. Le SDN permet aux ingénieurs et aux administrateurs réseau de répondre aux exigences commerciales en évolution rapide.

Bien que les avantages les plus connus du SDN soient la programmabilité du trafic, une plus grande agilité, la capacité à créer une supervision réseau basée sur des politiques et la mise en œuvre de l'automatisation du réseau, certains des avantages spécifiques du SDN sont énumérés ci-dessous :

- Provisionnement réseau centralisé
- Sécurité réseau accrue au niveau granulaire
- Coûts d'exploitation réduits
- Niveaux d'abstraction cloud accrus
- Livraison de contenu garantie
- Temps d'arrêt réseau réduit

NetScaler Console prend en charge le SDN dans les réseaux d'entreprise en s'intégrant aux contrôleurs SDN de différents fournisseurs. NetScaler Console prend en charge à la fois VMware NSX Manager et Cisco Application Policy Infrastructure Controller (APIC).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VMware NSX Manager

NetScaler Console s'intègre à la plateforme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services NetScaler. Cette intégration élimine les complexités traditionnelles associées à la topologie réseau physique, permettant aux administrateurs vSphere/vCenter de déployer les services NetScaler plus rapidement et de manière programmatique.

VMware NSX Manager expose des pare-feu logiques, des commutateurs, des routeurs, des ports et d'autres éléments de mise en réseau pour permettre la mise en réseau virtuelle entre divers hyperviseurs, systèmes de gestion cloud et matériel réseau associé. Il prend également en charge les services de mise en réseau externe et de sécurité.

La fonctionnalité d'orchestration cloud de NetScaler Console permet l'intégration des produits NetScaler avec VMware NSX et offre les capacités suivantes :

- Possibilité d'allouer un VPX pré-provisionné à la demande à une passerelle Edge spécifique dans le cadre de l'insertion de service.
- Capacité à configurer des fonctionnalités avancées de NetScaler telles que SSL et CS, ainsi que l'équilibrage de charge de base, via des modèles d'application sur les instances exécutées dans l'environnement NSX.
- Capacité à désallouer un VPX d'une passerelle Edge spécifique dans le cadre de la suppression d'un service et à réallouer le même VPX à une autre passerelle Edge.
- Capacité à déployer rapidement les fonctions NetScaler depuis la console vCenter dans le cadre du flux de travail de déploiement de toute l'infrastructure requise pour une application.

Avantages :

- Allocation automatisée et à la demande de nouveaux services NetScaler dans le cadre d'un flux de travail de déploiement d'applications
- Configuration simplifiée des fonctionnalités NetScaler avancées et spécifiques aux applications via des modèles d'application
- Séparation des tâches multi-locataires et un modèle de consommation en libre-service tout en offrant aux administrateurs cloud un point de contrôle unique
- Intégration plus facile avec les API de NetScaler Console, ce qui aide à prendre en charge les utilisations futures imprévues.

Pour plus d'informations sur la configuration de VMware NSX Manager sur NetScaler Console, consultez Intégration des appliances NetScaler avec VMware NSX Manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OpenStack : Intégration des instances NetScaler

La fonctionnalité d'orchestration cloud de NetScaler Console permet l'intégration des produits NetScaler avec la plateforme OpenStack. En utilisant cette fonctionnalité avec la plateforme OpenStack, les utilisateurs OpenStack peuvent bénéficier de la fonctionnalité d'équilibrage de charge (LBaaS) de NetScaler. Après cela, les utilisateurs OpenStack peuvent déployer leurs configurations d'équilibrage de charge depuis OpenStack dans l'instance NetScaler.

Les sections suivantes fournissent une brève description des fonctionnalités de NetScaler Console et du workflow d'intégration OpenStack.

Pilote NetScaler pour OpenStack Neutron LBaaS

Le plug-in OpenStack Neutron LBaaS inclut un pilote NetScaler qui permet à OpenStack de communiquer avec NetScaler Console. OpenStack utilise ce pilote pour transmettre toute configuration d'équilibrage de charge effectuée via les API LBaaS à NetScaler Console, qui crée la configuration d'équilibrage de charge sur les instances NetScaler souhaitées. OpenStack utilise également le pilote pour appeler NetScaler Console à intervalles réguliers afin de récupérer l'état des différentes entités (telles que les VIP et les pools) de toutes les configurations d'équilibrage de charge des NetScaler. Le logiciel de pilote NetScaler pour la plateforme OpenStack est fourni avec NetScaler Console. Pour télécharger et installer les pilotes, vous devez d'abord installer NetScaler Console et lancer l'application.

Enregistrement mutuel de NetScaler Console et OpenStack

Vous devez d'abord enregistrer les informations OpenStack sur NetScaler Console. Spécifiez l'adresse IP du contrôleur OpenStack et les informations d'identification de l'utilisateur administratif du cloud, ainsi que les informations d'identification de l'utilisateur du pilote NetScaler OpenStack. Vous pourrez ensuite spécifier les mêmes informations d'identification de connexion dans la section NetScaler_driver du fichier de configuration Neutron (neutron.conf) afin que le pilote NetScaler dans OpenStack puisse se connecter à NetScaler Console pendant les configurations LB.

Une fois qu'OpenStack et NetScaler Console sont enregistrés l'un avec l'autre, ils peuvent communiquer. De plus, les utilisateurs OpenStack peuvent utiliser leurs informations d'identification existantes dans OpenStack pour se connecter à l'interface utilisateur de NetScaler Console afin de vérifier les performances de leurs configurations LB dans les NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Locataires dans OpenStack

Dans OpenStack, un locataire est également appelé un projet. Un locataire est un groupe d'utilisateurs ; un locataire ou un projet peut également être défini comme un ensemble de ressources (calcul, réseau, stockage, etc.) attribuées à un groupe d'utilisateurs isolé.

Stratégies de placement

Les stratégies de placement offrent la flexibilité de décider de l'instance NetScaler utilisée dans chaque configuration d'équilibrage de charge créée par les utilisateurs. Alternativement, NetScaler Console offre également une option pour attribuer une instance NetScaler basée sur les locataires OpenStack.

Packages de services

Les packages de services sont des ensembles qui lient des stratégies/SLA, des spécifications de configuration d'appareils ou d'auto-provisionnement, et des locataires/stratégies de placement. Un package de services est généralement défini en termes de stratégies d'isolation fournies au locataire.

Voici quelques points liés aux packages de services :

- Un locataire ne peut pas faire partie de plus d'un package de services.
- Plusieurs locataires peuvent être associés au même package de services.
- Dans un package de services configuré pour l'auto-provisionnement, les instances NetScaler virtuelles ne peuvent être créées qu'à partir d'un seul type de plateforme (sur la plateforme SDX ou sur la plateforme OpenStack Compute).

Fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2

Alors que le pilote LBaaS V1 dans OpenStack prend en charge les opérations depuis l'interface utilisateur OpenStack Horizon, le pilote LBaaS V2 ne prend en charge que les opérations en ligne de commande.

La liste suivante présente les fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2 sur OpenStack :

- LBaaS V1
    - Équilibrage de charge
- LBaaS V2
    - Équilibrage de charge

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Déchargement SSL avec des certificats gérés par **Barbican**, le gestionnaire de clés dans OpenStack
- Bundles de certificats (inclut les autorités de certification intermédiaires)
- Prise en charge SNI

Ce document fournit des informations sur :

- Scénario de cas d'utilisation
- Intégration de NetScaler Console avec le flux de travail OpenStack
- Prérequis
- Tâches de pré-configuration dans NetScaler Console et OpenStack
- Étapes de configuration pour LBaaS V1 à l'aide d'Horizon
- Étapes de configuration pour LBaaS V2 à l'aide de la ligne de commande
- Provisionnement manuel d'une instance NetScaler VPX sur OpenStack
- Intégration de NetScaler Console avec les services OpenStack Heat
- Surveillance des applications OpenStack dans NetScaler Console

Scénario de cas d'utilisation

Le scénario de cas d'utilisation suivant explique le flux de travail d'intégration de NetScaler Console avec la plateforme OpenStack :

Une entreprise, Example-Cloud-Provider, a utilisé des composants OpenStack pour configurer un cloud afin de fournir une infrastructure à ses locataires. Steve est l'administrateur de ce fournisseur de cloud, tandis que Tom est un locataire de l'infrastructure cloud d'Example-Cloud-Provider. L'organisation de Tom, Example-SportsOnline.com, nécessite deux serveurs S1 et S1, et Tom a également besoin d'un dispositif NetScaler dédié pour équilibrer la charge du trafic entre les serveurs S1 et S2 sur la plateforme OpenStack.

Pour répondre à cette exigence, Steve doit installer et configurer OpenStack et NetScaler Console, et les préparer à être compatibles l'un avec l'autre. Steve doit créer un compte locataire nommé Example-SportsOnline dans OpenStack, puis allouer des ressources à ce compte locataire. Steve doit également créer différentes informations d'identification de connexion (utilisateurs) pour Example-SportsOnline afin de gérer ses ressources et sa configuration. Tom peut maintenant créer les deux serveurs S1 et S2 sur OpenStack pour gérer le trafic dans son organisation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Steve doit enregistrer les détails d'OpenStack auprès de NetScaler Console et configurer le pilote NetScaler LBaaS dans le composant réseau OpenStack, Neutron. Une fois l'enregistrement terminé, NetScaler Console affiche les détails de tous les locataires d'OpenStack. Steve peut sélectionner Example-SportsOnline dans la liste des locataires qui souhaitent les fonctionnalités NetScaler LBaaS et configurer Tom pour qu'il obtienne un NetScaler dédié alloué pour ses configurations d'équilibrage de charge dans NetScaler Console.

Pour cela, Steve peut soit provisionner une instance NetScaler VPX sur la couche de calcul (Nova) d'OpenStack à l'aide de l'interface utilisateur de NetScaler Console, soit activer MAS pour provisionner automatiquement une instance NetScaler VPX à la demande, lorsque Tom effectue sa configuration LB dans OpenStack. Dans les deux cas, NetScaler Console gère l'instance VPX. Pour y parvenir, Steve crée un package de services dans NetScaler Console et définit les conditions du package de services qui ont été convenues dans le SLA avec Tom. Par exemple, Steve sélectionne la politique d'isolation 'dédiée' pour fournir une instance dédiée pour les configurations d'équilibrage de charge à Tom. C'est-à-dire que Steve sélectionne une instance non partagée pour Tom dans le package de services. Il attribue ensuite de nombreuses instances NetScaler VPX au package de services et associe Example-SportsOnline, ainsi que d'autres locataires, qui nécessitent un NetScaler dédié au package de services. En conséquence, lorsque Tom effectue sa première configuration d'équilibrage de charge, NetScaler Console alloue l'une des instances NetScaler VPX du package de services à Example-SportsOnline et déploie également sa configuration dans ce NetScaler.

Tom peut maintenant créer des configurations d'équilibrage de charge en créant des pools, des adresses IP virtuelles (VIP) et des moniteurs de santé à l'aide d'OpenStack LBaaS/UI. Les pools et les VIP dans OpenStack sont déployés en tant que groupes de services et serveurs virtuels sur l'instance NetScaler. Tom peut également créer des moniteurs de santé pour surveiller les serveurs et envoyer le trafic d'application uniquement aux serveurs qui sont ACTIFS à tout moment et accessibles depuis NetScaler.

La configuration d'équilibrage de charge créée dans OpenStack est maintenant implémentée sur l'instance NetScaler. Une fois entièrement configurée, l'instance NetScaler VPX prend en charge la fonctionnalité d'équilibrage de charge et commence à accepter le trafic applicatif et à équilibrer la charge du trafic entre les serveurs S1 et S2 créés par Tom.

Flux de travail d'intégration de NetScaler Console avec OpenStack

L'organigramme suivant décrit le flux de travail que vous devez suivre lors de la configuration de LBaaS V1 et LBaaS V2.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

OpenStack : Intégration des instances NetScaler

La fonctionnalité d'orchestration cloud de NetScaler Console permet l'intégration des produits NetScaler avec la plateforme OpenStack. En utilisant cette fonctionnalité avec la plateforme OpenStack, les utilisateurs OpenStack peuvent bénéficier de la fonctionnalité d'équilibrage de charge (LBaaS) de NetScaler. Après cela, les utilisateurs OpenStack peuvent déployer leurs configurations d'équilibrage de charge depuis OpenStack dans l'instance NetScaler.

Les sections suivantes fournissent une brève description des fonctionnalités de NetScaler Console et du workflow d'intégration OpenStack.

Pilote NetScaler pour OpenStack Neutron LBaaS

Le plug-in OpenStack Neutron LBaaS inclut un pilote NetScaler qui permet à OpenStack de communiquer avec NetScaler Console. OpenStack utilise ce pilote pour transmettre toute configuration d'équilibrage de charge effectuée via les API LBaaS à NetScaler Console, qui crée la configuration d'équilibrage de charge sur les instances NetScaler souhaitées. OpenStack utilise également le pilote pour appeler NetScaler Console à intervalles réguliers afin de récupérer l'état des différentes entités (telles que les VIP et les pools) de toutes les configurations d'équilibrage de charge des NetScaler. Le logiciel de pilote NetScaler pour la plateforme OpenStack est fourni avec NetScaler Console. Pour télécharger et installer les pilotes, vous devez d'abord installer NetScaler Console et lancer l'application.

Enregistrement mutuel de NetScaler Console et OpenStack

Vous devez d'abord enregistrer les informations OpenStack sur NetScaler Console. Spécifiez l'adresse IP du contrôleur OpenStack et les informations d'identification de l'utilisateur administratif du cloud, ainsi que les informations d'identification de l'utilisateur du pilote NetScaler OpenStack. Vous pourrez ensuite spécifier les mêmes informations d'identification de connexion dans la section NetScaler_driver du fichier de configuration Neutron (neutron.conf) afin que le pilote NetScaler dans OpenStack puisse se connecter à NetScaler Console pendant les configurations LB.

Une fois qu'OpenStack et NetScaler Console sont enregistrés l'un avec l'autre, ils peuvent communiquer. De plus, les utilisateurs OpenStack peuvent utiliser leurs informations d'identification existantes dans OpenStack pour se connecter à l'interface utilisateur de NetScaler Console afin de vérifier les performances de leurs configurations LB dans les NetScaler.

Locataires dans OpenStack

Dans OpenStack, un locataire est également appelé un projet. Un locataire est un groupe d'utilisateurs ; un locataire ou un projet peut également être défini comme un ensemble de ressources (calcul, réseau, stockage, etc.) attribuées à un groupe d'utilisateurs isolé.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Stratégies de placement

Les stratégies de placement offrent la flexibilité de décider de l'instance NetScaler utilisée dans chaque configuration d'équilibrage de charge créée par les utilisateurs. Alternativement, NetScaler Console offre également une option pour attribuer une instance NetScaler basée sur les locataires OpenStack.

Packages de services

Les packages de services sont des ensembles qui lient des stratégies/SLA, des spécifications de configuration d'appareils ou d'auto-provisionnement, et des locataires/stratégies de placement. Un package de services est généralement défini en termes de stratégies d'isolation fournies au locataire.

Voici quelques points liés aux packages de services :

- Un locataire ne peut pas faire partie de plus d'un package de services.
- Plusieurs locataires peuvent être associés au même package de services.
- Dans un package de services configuré pour l'auto-provisionnement, les instances NetScaler virtuelles ne peuvent être créées qu'à partir d'un seul type de plateforme (sur la plateforme SDX ou sur la plateforme OpenStack Compute).

Fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2

Alors que le pilote LBaaS V1 dans OpenStack prend en charge les opérations depuis l'interface utilisateur OpenStack Horizon, le pilote LBaaS V2 ne prend en charge que les opérations en ligne de commande.

La liste suivante présente les fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2 sur OpenStack :

- LBaaS V1
  - Équilibrage de charge
- LBaaS V2
  - Équilibrage de charge
  - Déchargement SSL avec des certificats gérés par **Barbican**, le gestionnaire de clés dans OpenStack
  - Bundles de certificats (inclut les autorités de certification intermédiaires)
  - Prise en charge SNI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ce document fournit des informations sur :

- Scénario de cas d'utilisation
- Intégration de NetScaler Console avec le flux de travail OpenStack
- Prérequis
- Tâches de pré-configuration dans NetScaler Console et OpenStack
- Étapes de configuration pour LBaaS V1 à l'aide d'Horizon
- Étapes de configuration pour LBaaS V2 à l'aide de la ligne de commande
- Provisionnement manuel d'une instance NetScaler VPX sur OpenStack
- Intégration de NetScaler Console avec les services OpenStack Heat
- Surveillance des applications OpenStack dans NetScaler Console

Scénario de cas d'utilisation

Le scénario de cas d'utilisation suivant explique le flux de travail d'intégration de NetScaler Console avec la plateforme OpenStack :

Une entreprise, Example-Cloud-Provider, a utilisé des composants OpenStack pour configurer un cloud afin de fournir une infrastructure à ses locataires. Steve est l'administrateur de ce fournisseur de cloud, tandis que Tom est un locataire de l'infrastructure cloud d'Example-Cloud-Provider. L'organisation de Tom, Example-SportsOnline.com, nécessite deux serveurs S1 et S1, et Tom a également besoin d'un dispositif NetScaler dédié pour équilibrer la charge du trafic entre les serveurs S1 et S2 sur la plateforme OpenStack.

Pour répondre à cette exigence, Steve doit installer et configurer OpenStack et NetScaler Console, et les préparer à être compatibles l'un avec l'autre. Steve doit créer un compte locataire nommé Example-SportsOnline dans OpenStack, puis allouer des ressources à ce compte locataire. Steve doit également créer différentes informations d'identification de connexion (utilisateurs) pour Example-SportsOnline afin de gérer ses ressources et sa configuration. Tom peut maintenant créer les deux serveurs S1 et S2 sur OpenStack pour gérer le trafic dans son organisation.

Steve doit enregistrer les détails d'OpenStack auprès de NetScaler Console et configurer le pilote NetScaler LBaaS dans le composant réseau OpenStack, Neutron. Une fois l'enregistrement terminé, NetScaler Console affiche les détails de tous les locataires d'OpenStack. Steve peut sélectionner Example-SportsOnline dans la liste des locataires qui souhaitent les fonctionnalités NetScaler LBaaS et configurer Tom pour qu'il obtienne un NetScaler dédié alloué pour ses configurations d'équilibrage de charge dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour cela, Steve peut soit provisionner une instance NetScaler VPX sur la couche de calcul (Nova) d'OpenStack à l'aide de l'interface utilisateur de NetScaler Console, soit activer MAS pour provisionner automatiquement une instance NetScaler VPX à la demande, lorsque Tom effectue sa configuration LB dans OpenStack. Dans les deux cas, NetScaler Console gère l'instance VPX. Pour y parvenir, Steve crée un package de services dans NetScaler Console et définit les conditions du package de services qui ont été convenues dans le SLA avec Tom. Par exemple, Steve sélectionne la politique d'isolation 'dédiée' pour fournir une instance dédiée pour les configurations d'équilibrage de charge à Tom. C'est-à-dire que Steve sélectionne une instance non partagée pour Tom dans le package de services. Il attribue ensuite de nombreuses instances NetScaler VPX au package de services et associe Example-SportsOnline, ainsi que d'autres locataires, qui nécessitent un NetScaler dédié au package de services. En conséquence, lorsque Tom effectue sa première configuration d'équilibrage de charge, NetScaler Console alloue l'une des instances NetScaler VPX du package de services à Example-SportsOnline et déploie également sa configuration dans ce NetScaler.

Tom peut maintenant créer des configurations d'équilibrage de charge en créant des pools, des adresses IP virtuelles (VIP) et des moniteurs de santé à l'aide d'OpenStack LBaaS/UI. Les pools et les VIP dans OpenStack sont déployés en tant que groupes de services et serveurs virtuels sur l'instance NetScaler. Tom peut également créer des moniteurs de santé pour surveiller les serveurs et envoyer le trafic d'application uniquement aux serveurs qui sont ACTIFS à tout moment et accessibles depuis NetScaler.

La configuration d'équilibrage de charge créée dans OpenStack est maintenant implémentée sur l'instance NetScaler. Une fois entièrement configurée, l'instance NetScaler VPX prend en charge la fonctionnalité d'équilibrage de charge et commence à accepter le trafic applicatif et à équilibrer la charge du trafic entre les serveurs S1 et S2 créés par Tom.

Flux de travail d'intégration de NetScaler Console avec OpenStack

L'organigramme suivant décrit le flux de travail que vous devez suivre lors de la configuration de LBaaS V1 et LBaaS V2.



Prérequis

Avant d'intégrer l'instance virtuelle NetScaler à la plateforme OpenStack, assurez-vous que les exigences suivantes sont remplies :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exigences logicielles de NetScaler Console et OpenStack

- NetScaler Console 13.1 est installé sur un poste de travail hyperviseur pris en charge qui répond aux exigences matérielles minimales du système.
- Les composants OpenStack sont installés et en cours d'exécution.
- NetScaler Console 13.1 prend en charge les versions OpenStack suivantes : **Newton**, **Ocata**, **Pike** et **Queens**.

Exigences matérielles de NetScaler Console

Assurez-vous que les ressources de calcul virtuelles suivantes sont disponibles sur votre serveur OpenStack pour installer les instances virtuelles NetScaler :

COMPOSANT	EXIGENCE
RAM	8 Go
Processeur virtuel	8
Espace de stockage	500 Go
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

REMARQUE

Les exigences de mémoire et de disque dur spécifiées sont destinées au déploiement de NetScaler Console sur la plateforme OpenStack, en considérant qu'aucune autre machine virtuelle n'est exécutée sur l'hôte. Les exigences matérielles pour OpenStack dépendent du nombre de machines virtuelles qui y sont exécutées.

Tâches de pré-configuration dans NetScaler Console et OpenStack

Cette section vous aide à effectuer les tâches de pré-configuration avant de configurer NetScaler Console et OpenStack.

Installation de NetScaler Console

Installez NetScaler Console sur un hyperviseur pris en charge. Pour plus d'informations sur le téléchargement et l'installation de NetScaler Console, consultez (/fr-fr/netscaler-application-delivery-management-software/current-release/deploy.html).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installation du logiciel de pilote NetScaler et enregistrement de NetScaler Console sur OpenStack

Téléchargez le bundle NetScaler pour OpenStack depuis la page Téléchargements de NetScaler Console.

Pour installer le pilote NetScaler sur la plateforme OpenStack à l'aide de l'interface graphique de NetScaler Console :

1. Dans NetScaler Console, cliquez sur **Téléchargements**. La page **Téléchargements** de NetScaler Console vous fournit des liens pour télécharger le logiciel **NetScaler bundle for OpenStack** requis pour les versions OpenStack **Newton**, **Ocata** et **Pike**.
2. Téléchargez le dernier fichier tar du bundle NetScaler dans un répertoire temporaire (par exemple, /tmp) dans OpenStack Controller. Ce bundle inclut le pilote LBaaS V2 et le plug-in Heat pour toutes les versions d'OpenStack.

   
3. Exécutez la commande suivante pour extraire les fichiers du fichier tar du pilote NetScaler : `tar -xvzf <name_of_tar_file>`
4. Si vous avez une configuration OpenStack \<Release Name\>, à l'invite, tapez la commande suivante :

   `cd <Release Name>`

   Exemple :

   `cd Newton`
5. Exécutez la commande suivante pour installer le pilote et spécifier l'adresse IP de NetScaler Console, le mot de passe du pilote NetScaler que vous avez configuré lors de l'enregistrement d'OpenStack auprès de NetScaler Console, et le protocole :

   `./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>`

   Exemple pour une configuration OpenStack à nœud unique :

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas`

   Exemple pour une configuration OpenStack multinœud :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

REMARQUE

La spécification du chemin du répertoire `neutron-lbaas` du système est facultative. La spécification du chemin peut aider le script à trouver les pilotes.

Une fois NetScaler Console enregistré avec succès sur OpenStack, vous pouvez également vous connecter à NetScaler Console en utilisant vos informations d'identification d'utilisateur OpenStack.
Une fois NetScaler Console enregistré avec succès sur OpenStack, redémarrez les services OpenStack Neutron.

Enregistrement d'OpenStack auprès de NetScaler Console

Pour enregistrer OpenStack auprès de NetScaler Console à l'aide de l'interface graphique de NetScaler Console :

1. Dans NetScaler Console, accédez à **Orchestration** \> **Cloud Orchestration** \> **OpenStack**.
2. Cliquez sur **Configurer les paramètres OpenStack**.
3. Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack dans NetScaler Console. Vous avez deux options ici : Par défaut et Personnalisé.

   Pour les versions Newton et **Ocata** d'OpenStack, vous pouvez utiliser un type de déploiement par défaut ou personnalisé. Mais pour la version Pike, vous devez utiliser un type de déploiement personnalisé pour enregistrer OpenStack auprès de NetScaler Console.

- **Type de déploiement par défaut**

  Sélectionnez **Par défaut** si les services OpenStack s'exécutent sur les ports par défaut. Par exemple, le port par défaut pour les services Neutron est 9696, le port par défaut pour les services Keystone est 5000.

1. Adresse IP du contrôleur OpenStack - Adresse IP du contrôleur OpenStack (les services **KeyStone** et **Neutron** doivent être accessibles sur cette adresse IP). Par exemple, entrez l'adresse IP 10.102.205.23.
2. Nom d'utilisateur administrateur OpenStack - Nom d'utilisateur administratif du contrôleur OpenStack. Par exemple, entrez admin1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Mot de passe - Mot de passe de l'utilisateur administratif du contrôleur OpenStack.
4. Tenant administrateur OpenStack - Nom du tenant administratif sur OpenStack. Par exemple, entrez admin.



- **Type de déploiement personnalisé**

  Sélectionnez le type de déploiement **Personnalisé** si les services OpenStack s'exécutent sur des ports différents des ports par défaut. Si ces services s'exécutent sur des ports différents, spécifiez-les ici. L'enregistrement des versions OpenStack Newton et **Ocata** auprès de NetScaler Console est différent de l'enregistrement de la version OpenStack Pike.

  Version Newton et Ocata d'OpenStack :

  a. Spécifiez les numéros de port pour les différents services OpenStack si vous enregistrez la version Newton d'OpenStack.
  b. Spécifiez le nom d'utilisateur administrateur OpenStack, le mot de passe et le nom d'utilisateur du tenant administrateur OpenStack comme vous l'avez spécifié précédemment dans les paramètres **Par défaut**.

  

  Version Pike d'OpenStack :

  Si vous enregistrez la version Pike d'OpenStack, saisissez les détails des services OpenStack comme indiqué dans l'image suivante. Vous devez également spécifier le nom d'utilisateur administrateur OpenStack, le mot de passe et le nom d'utilisateur du locataire administrateur OpenStack comme dans les paramètres par défaut.

  

1. Dans la section **OpenStack Neutron LBaaS - Informations d'identification utilisées par le pilote NetScaler**, définissez le mot de passe du pilote NetScaler pour le compte d'utilisateur du pilote NetScaler OpenStack. NetScaler Console authentifie les appels du pilote NetScaler OpenStack en utilisant ces informations d'identification. Vous devez spécifier le même mot de passe lorsque vous exécutez le script d'installation du pilote NetScaler dans le contrôleur OpenStack.



2. Cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Création d'un locataire sur OpenStack

Créez un projet ou un locataire sur OpenStack, ajoutez des utilisateurs au projet ou au locataire, et attribuez des rôles à tous les utilisateurs. **KeyStone**, le service d'identité d'OpenStack, fournit des services d'authentification pour chaque service OpenStack. Le service d'authentification utilise une combinaison de domaines, de projets (locataires), d'utilisateurs et de rôles.

Pour plus d'informations sur la création d'un projet et l'exécution d'autres tâches dans OpenStack, consultez la documentation OpenStack à l'adresse `<http://docs.openstack.org/>`.

Ajout de locataires OpenStack

1. Dans NetScaler Console, accédez à **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Locataires OpenStack**, puis cliquez sur **Ajouter**.
2. Dans la page **Ajouter des locataires OpenStack**, cliquez sur **+Ajouter**, puis sélectionnez le locataire OpenStack.
3. Cliquez sur **OK**.

Selon que vous utilisez une instance pré-provisionnée ou que vous provisionnez automatiquement l'instance lors de l'intégration d'OpenStack, suivez l'une de ces deux tâches :

- Pré-provisionner les appliances NetScaler
- Provisionner automatiquement les appliances NetScaler VPX sur OpenStack

Provisionnement des appliances NetScaler

Selon que vous utilisez une instance pré-provisionnée ou que vous provisionnez automatiquement l'instance lors de l'intégration d'OpenStack, suivez l'une de ces deux tâches :

- Pré-provisionner les appliances NetScaler
- Provisionner automatiquement les appliances NetScaler VPX sur OpenStack

PRÉ-PROVISIONNEMENT DES APPLIANCES NETSCALER

Installez l'appliance NetScaler sur l'une des plateformes d'hyperviseur telles que Citrix Hypervisor, KVM ou ESX, et ajoutez l'instance à NetScaler Console. NetScaler Console gère ensuite cette appliance qui équilibre la charge du trafic sur les serveurs.

Pour ajouter une instance NetScaler VPX existante dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure** \> **Instances** \> **NetScaler VPX**, puis cliquez sur **Ajouter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sur la page **Ajouter NetScaler VPX**, spécifiez l'adresse IP de l'instance NetScaler VPX et sélectionnez un profil d'instance dans la liste **Nom du profil**. Le profil d'instance contient les informations d'identification utilisées pour se connecter au NetScaler VPX. Vous pouvez également créer un nouveau profil d'instance en cliquant sur l'icône +. Cliquez sur **OK**.

PROVISIONNEMENT AUTOMATIQUE DES APPLIANCES NETSCALER

Téléchargez l'image d'instance NetScaler requise depuis la page de téléchargement NetScaler, et téléchargez-la sur Glance, le service d'imagerie OpenStack. La disponibilité d'une image sur Glance vous permet de configurer une instance NetScaler à la demande lors de l'affectation de l'instance au locataire.

Pour provisionner automatiquement les appliances NetScaler VPX sur OpenStack :

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration cloud** \> **OpenStack**.
2. Cliquez sur **Paramètres de déploiement**.
3. Définissez les paramètres suivants :

    a. Réseau de gestion - sélectionnez le réseau de gestion sur OpenStack, auquel le NetScaler VPX auto-provisionné est connecté.

    b. Nom du profil - sélectionnez le profil dans la liste déroulante. La console NetScaler utilise le mot de passe contenu dans ce profil pour configurer les nouvelles instances NetScaler VPX auto-provisionnées.

    c. Licences - fournissez les codes d'accès de licence de la console NetScaler utilisés pour licencier les nouvelles instances NetScaler auto-provisionnées. La console NetScaler provisionne les instances NetScaler sur le calcul OpenStack dans le réseau de gestion, puis déclenche l'installation de la licence sur celles-ci à l'aide du code de licence spécifié. L'instance NetScaler télécharge ensuite les fichiers de licence depuis le site Web de Citrix à l'aide du code d'accès de licence spécifié ici.

    d. Image NetScaler VPX dans Glance - sélectionnez l'image NetScaler VPX disponible dans OpenStack Glance qui est utilisée pour créer une instance NetScaler VPX.

    e. Paramètres du proxy - fournissez les détails du serveur proxy NetScaler pour l'installation des licences. Cela peut être nécessaire lorsque NetScaler n'a pas d'accès direct à Internet via le réseau de gestion.

4. Cliquez sur **OK**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Création d'un package de services dans NetScaler Console

Pour créer des packages de services pour un locataire dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Packages de services**, puis cliquez sur **Ajouter**.
2. Sur la page **Package de services**, spécifiez les paramètres suivants :
   a. Nom - nom du package de services. Par exemple, entrez SVC-PKG-GOLD.
   b. Allocation d'instances NetScaler - le type d'allocation d'instances défini dans le package de services en fonction duquel les ressources d'instances NetScaler sont allouées à un locataire. Sélectionnez **Dédié**. Pour plus d'informations sur les stratégies, consultez Stratégies d'isolation des packages de services.
   c. Provisionnement d'instances NetScaler - sélectionnez **Instance existante** pour allouer une instance NetScaler existante à un locataire. Si vous souhaitez créer des instances NetScaler pendant la configuration elle-même, sélectionnez **Créer une instance à la demande**.
   d. Type d'instance NetScaler - sélectionnez **NetScaler VPX**.

   REMARQUE

   Sélectionnez NetScaler VPX pour allouer des instances NetScaler pré-provisionnées hébergées sur la plateforme SDX.

3. Cliquez sur **Continuer** pour associer un locataire à un package de services.

   REMARQUE

   Activez **Provisionner une paire d'instances NetScaler pour la haute disponibilité**, si vous déployez les instances NetScaler en mode haute disponibilité.

4. Dans la section **Attribuer des instances**, cliquez sur **Ajouter**, puis sélectionnez l'instance NetScaler que vous souhaitez attribuer au locataire, et cliquez sur **Continuer**.
5. Dans la section **Attribuer des locataires/stratégies de placement OpenStack**, sous **Locataires OpenStack**, cliquez sur **Ajouter,** et sélectionnez le locataire.
6. Cliquez sur **Continuer**, puis cliquez sur **Terminé**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si la stratégie n'est pas trouvée, le mécanisme de secours est réactivé, et la console NetScaler attribue des instances NetScaler en fonction des locataires. Si le locataire ne fait partie d'aucun package de services, la console NetScaler affiche un message d'erreur indiquant : "Le locataire \<admin\> ne fait partie d'aucun package de services et il n'y a pas de package de services par défaut."

Création de stratégies de placement (facultatif)

Les stratégies d'isolation ne sont pas uniquement basées sur le locataire. Vous pouvez créer des stratégies de placement flexibles, où les stratégies ne sont pas seulement basées sur le nom ou l'ID du locataire, mais aussi sur d'autres attributs personnalisés.

Pour créer des stratégies de placement pour un locataire dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration cloud** \> **OpenStack** \> **Stratégie de placement**, puis cliquez sur **Ajouter**.
2. Sur la page **Ajouter une stratégie de placement**, définissez les paramètres suivants :
    a. Nom - saisissez un nom pour la stratégie de placement
    b. Exemples d'expressions - sélectionnez un exemple d'expression dans la liste. Ces exemples sont utiles pour construire la stratégie de placement.
    c. Expression - une expression booléenne est renseignée dans ce champ en fonction de l'exemple d'expression que vous avez sélectionné dans le champ précédent. Modifiez les noms de champ si nécessaire.
3. Cliquez sur **OK**.

Activation du trafic des instances NetScaler vers les serveurs back-end via le réseau client

Par défaut, dans le workflow d'orchestration OpenStack, les instances NetScaler sont liées dynamiquement à l'équilibreur de charge ou aux réseaux clients et aux réseaux membres ou serveurs.

Dans certains déploiements, les serveurs sont également accessibles via les réseaux clients et peuvent être acheminés via la passerelle client. Dans de tels cas, les instances NetScaler n'ont pas besoin d'être liées aux réseaux de serveurs, mais elles doivent être liées uniquement aux réseaux clients.

Effectuez le réglage suivant pour configurer le trafic via la passerelle client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Deployment Settings**, puis sélectionnez l'option **Provision only VIP network and route pool traffic through VIP network**.

NetScaler Console configure ensuite l'instance NetScaler sur les réseaux clients en ajoutant un SNIP dans ce réseau, et ajoutera ensuite une route par défaut vers la passerelle du réseau client. Cela permet à l'instance d'atteindre les serveurs via la passerelle client.

Provisionnement automatique des dispositifs NetScaler VPX déployés sur la plateforme NetScaler SDX

Ajoutez la plateforme NetScaler SDX dans NetScaler Console, afin que NetScaler Console provisionne les instances sur cette plateforme à la demande.

Pour provisionner automatiquement les instances NetScaler déployées sur la plateforme NetScaler SDX :

1. Dans l'interface graphique de NetScaler Console, accédez à **Infrastructure > Instances** \> **NetScaler SDX**, puis cliquez sur **Add** pour ajouter une plateforme NetScaler SDX.
2. Accédez à **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Deployment Settings.**
3. Dans la section **Réseau de gestion**, sélectionnez le réseau de gestion sur OpenStack auquel le NetScaler SDX auto-provisionné est connecté.
    a. Dans **Nom du profil**, sélectionnez le profil dans la liste déroulante. La console NetScaler utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances NetScaler VPX auto-provisionnées.
    b. Cliquez sur **OK**.
4. Pour provisionner la plate-forme NetScaler SDX dans OpenStack, accédez à **Orchestration** \> **Orchestration cloud** \> **OpenStack**\> **Package de services**.
    a. Cliquez sur **Ajouter** pour créer un nouveau package de services.
    b. Saisissez le nom du package de services.
    c. Dans le champ **Allocation d'instance NetScaler**, sélectionnez **Dédié**.
    d. Dans le champ **Provisionnement d'instance NetScaler**, sélectionnez **Créer une instance à la demande**, et dans le champ **Plate-forme de provisionnement automatique**, sélectionnez **NetScaler SDX**.
    e. Par défaut, seules les instances NetScaler VPX sont provisionnées sur la plate-forme NetScaler SDX.
    f. Cliquez sur **Continuer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. Dans la section **Paramètres de provisionnement automatique**, définissez les propriétés des **Ressources**.

   i. Champ **Débit**. Saisissez 1000 Mbps.

   ii. Champ **Version de NetScaler**. Dans la liste, sélectionnez la version appropriée de l'image NetScaler VPX présente sur la plate-forme NetScaler SDX.

h. Dans la section **Plates-formes NetScaler SDX**, cliquez sur **Ajouter** pour ajouter la plate-forme SDX au package de services.

i. Cliquez sur **Continuer**.

j. Dans la section **Configurer les locataires OpenStack**, cliquez sur **Ajouter** pour ajouter les locataires. Vous pouvez également ajouter de nouveaux locataires en cliquant sur **Nouveau**.

k. Cliquez sur **Terminé**.

5. Les implémentations de l'API LBaaS V2 sont effectuées via les commandes Neutron LBaaS. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur l'exécution des commandes de configuration, consultez Configuration de LBaaS V2 à l'aide de la ligne de commande.

Configurer LBaaS V1 à l'aide de Horizon

Vous pouvez vous connecter au portail OpenStack Horizon pour créer un pool LBaaS et sélectionner un sous-réseau. Tous les membres de ce pool se trouvent dans le sous-réseau. Pour configurer :

- Ajoutez une adresse IP virtuelle (VIP) et attribuez cette VIP au pool créé.
- Vous pouvez également effectuer cette action sur la ligne de commande ou via des API.
- Les clients externes de vos serveurs peuvent se connecter à cette adresse VIP hébergée sur le NetScaler attribué.
- NetScaler distribue toutes les requêtes aux membres du pool sur les ports configurés.
- Les membres du pool LBaaS sont les serveurs à charge équilibrée qui sont ajoutés au pool sélectionné.
- Attribuez un poids et un port à chacun de ces membres.

Les moniteurs de santé sont utilisés pour surveiller la santé et le bon fonctionnement de tous les membres du pool. Vous pouvez créer un modèle de surveillance de santé dans OpenStack en définissant des paramètres tels que le délai, le délai d'expiration, les limites de nouvelle tentative,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

la méthode, le chemin d'URL et les codes de succès HTTP attendus. Après avoir créé un moniteur, vous devez l'associer au pool qui a été créé précédemment.

Pour plus d'informations sur la création de pools et d'autres tâches de configuration LBaaS dans OpenStack, consultez la documentation OpenStack.

IMPORTANT

LBaaS V1 n'est pas pris en charge dans la version Liberty d'OpenStack. Pour plus d'informations, consultez les notes de publication d'OpenStack.

Configurer LBaaS V2 à l'aide de la ligne de commande

LBaaS V2 prend en charge le déchargement SSL avec des certificats gérés par **Barbican**, des bundles de certificats (incluant les autorités de certification intermédiaires), la prise en charge SNI ainsi que les fonctionnalités d'équilibrage de charge classiques. LBaaS V2 ne prend en charge que l'interface de ligne de commande pour exécuter les tâches de configuration. Les implémentations de l'API LBaaS V2 sont effectuées via les commandes Neutron LBaaS.

REMARQUE

Téléchargez le certificat et la clé vers le service **Barbican** lorsque vous avez besoin de la fonction de déchargement SSL. Effectuez les étapes 1, 2 et 3 si le déchargement SSL est pris en charge, sinon continuez à partir de l'(/fr-fr/netscaler-application-delivery-management-software/current-release/orchestration/integrate-with-openstack-platform/openstack-configuring-lbaasv2-using-command-line.html) pour créer un équilibreur de charge, un écouteur, un pool et un membre.

1. Téléchargez le certificat vers le service **Barbican** à l'aide de la commande suivante :

   ```
   barbican secret store --payload-content-type <content_type> --name
   <certificate_name> --payload<certificate_location>
   ```

   Exemple :

   ```
   barbican secret store --payload-content-type='text/plain' --
   name='hp_server_certificate' --payload=" hp_server/tmp/
   server_certificate"
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Téléchargez la clé vers le service **Barbican** à l'aide de la commande suivante :

```
barbican secret store --payload-content-type <content_type> --name
<key_name> --payload<key_location>
```

Exemple :

```
barbican secret store -- payload-content-type='text/plain' --
name='shp_server_key' --payload="hp-server/tmp/server_key"
```

REMARQUE

Lorsque vous exécutez ces deux commandes **Barbican** pour charger le certificat et la clé, les champs Secret href fournissent un emplacement ou une URL. C'est là que le certificat et la clé sont stockés sur le système où OpenStack est installé. Copiez ces liens et fournissez-les comme paramètres lorsque vous créez le conteneur sur le service **Barbican** à l'étape 3.

3. Créez un conteneur dans le service **Barbican** pour stocker le certificat et la clé à l'aide de la commande suivante :

   Dans la commande, remplacez <certificate_url> par l'URL que vous avez obtenue du champ Secret href lorsque vous avez téléchargé le certificat. De même, remplacez <key_url> par l'URL que vous avez obtenue du champ Secret href lorsque vous avez téléchargé la clé.

```
barbican secret container create --name<container_name> --
type<container_type> --secret<certificate_url> --secret<key_url>
```

Exemple :

```
barbican secret container create --name='hp_container' --
type='certificate' --secret="`certificate=http://localhost:9311/v1/
secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --
secret="private_key=http://localhost:9311/v1/secrets/
1b9e1a93-2aeb-4101-8002-e52acab987b0`"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Copiez la valeur href du conteneur. Vous devez fournir le lien vers le conteneur lors de la création de l'écouteur à l'étape 6.

4. Définissez les variables d'environnement dans OpenStack. Les variables permettent aux commandes client OpenStack de communiquer avec les services OpenStack.

   Exemple :

   Exportez OS_PASSWORD-hp

   Exportez OS_AUTH_URL=`http://10.106.43.15:35357/v2.0/`

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

   exporter OS_IDENTITY_API_VERSION=2.0

   exporter BARBICAN_ENDPOINT="`http://10.106.43.15:9311/`"

   REMARQUE

   Définissez ces variables pour chaque session SSH avant d'exécuter d'autres commandes. Pour plus d'informations sur les variables d'environnement OpenStack, consultez variables d'environnement OpenStack.

5. Créez un équilibreur de charge à l'aide de la commande suivante :

   ```
   neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <subnet-name> --provider <netscaler>
   ```

   Exemple :

   ```
   neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
   ```

   Le statut passe de PENDING_CREATE à ACTIVE une fois l'équilibreur de charge créé avec succès.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Créez un écouteur à l'aide de la commande suivante :

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name
<listener-name> --protocol <protocol_type> --protocol-port
<port_number> --default-tls-container-id<container_url>
```

Exemple :

```
neutron lbaas-listener-create --name hp-lb-test-list  --loadbalancer
hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-
tls-container-id `http://10.106.43.15:9311/v1/containers/d688676f-
c256-4a0d-b84d-a310419dc0aa`
```

REMARQUE

Si vous créez un écouteur sans prise en charge du déchargement SSL, exécutez la commande suivante sans fournir d'emplacements au conteneur :

`neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

7. Créez un pool à l'aide de la commande suivante :

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener
<listener-name> --protocol <protocol_type> --name <pool-name>
```

Exemple :

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener
demolistener --protocol http --name demopool
```

8. Créez un membre à l'aide de la commande suivante :

```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-
address of the web server> --protocol-port <port_number>  <pool-name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple :

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --
protocol-port 80 hp-lb-test-pool
```

Supervision des applications OpenStack dans NetScaler Console

Vos locataires peuvent se connecter à NetScaler Console à l'aide de leurs informations d'identification OpenStack pour surveiller les VIP et les pools créés à partir d'OpenStack depuis n'importe quel navigateur. L'URL doit être au format suivant :

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

Où, `mas-ip-address`, est l'adresse IP de NetScaler Console qui est enregistrée auprès d'OpenStack.

REMARQUE

- Les VIP OpenStack correspondent à des serveurs virtuels dans NetScaler Console.
- Les pools OpenStack correspondent à des groupes de services dans NetScaler Console.
- Les membres du pool OpenStack correspondent à des membres de groupe de services dans NetScaler Console.

Configurer la commutation de contenu de couche 7

NetScaler Console s'intègre à OpenStack pour configurer les fonctionnalités de commutation de couche 7 (L7) ou de commutation basée sur le contenu sur les instances NetScaler. La commutation de contenu diffère de la simple répartition de charge en ce sens que des types spécifiques de requêtes peuvent être dirigés vers des serveurs spécifiques. Lorsque les configurations L7 sont créées dans OpenStack avec une instance NetScaler comme fournisseur, NetScaler Console alloue une instance NetScaler et déploie des configurations de commutation de contenu et de répondeur correspondant aux configurations L7. Les instances NetScaler peuvent alors distribuer et équilibrer la charge des requêtes utilisateur en fonction des caractéristiques de la couche application des requêtes.

La fonctionnalité d'équilibrage de charge de couche 7 (L7) d'OpenStack combine l'équilibrage de charge et la commutation de contenu pour fournir une diffusion optimisée de types de contenu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

spécifiques. Cela améliore les performances de l'équilibreur de charge en exécutant uniquement les politiques applicables au contenu. L'équilibrage de charge de couche 7 facilite également l'augmentation de l'efficacité de l'infrastructure d'application. La capacité à séparer le contenu en fonction du type, de l'URI ou des données permet une meilleure allocation des ressources physiques dans l'infrastructure d'application. Par exemple, un utilisateur final naviguant vers `http://example-sports.com/about-us` est servi par un pool de serveurs hébergeant du contenu sur l'entreprise et les services, tandis qu'un utilisateur naviguant vers `http://example-sports.com/shopping-cart-football` est servi par un pool de serveurs différent qui permet aux utilisateurs d'effectuer des achats en ligne.

Dans la commutation L7, un équilibreur de charge est implémenté comme un serveur virtuel de commutation de contenu qui accepte les requêtes HTTP des utilisateurs et distribue ces requêtes aux serveurs d'applications. La commutation L7 ou la commutation de contenu vous permet d'avoir un point d'entrée unique pour accéder à une variété de services back-end (par exemple, pas seulement des applications web, des portails de services web, des courriers web, mais aussi la gestion mobile, du contenu dans différentes langues, etc.). Autrement dit, vous pouvez fournir une seule adresse IP publique pour tous les services que vous proposez à vos utilisateurs.

Contrairement à l'équilibrage de charge de niveau inférieur, la commutation de couche 7 n'exige pas que tous les serveurs du pool aient le même contenu. Une configuration d'équilibreur de charge utilisant la commutation L7 s'attend à ce que les serveurs d'applications ou back-end de différents pools aient un contenu différent. Les commutateurs L7 peuvent diriger les requêtes en fonction de l'URI, de l'hôte, des en-têtes HTTP ou de tout autre élément du message d'application. Les serveurs d'applications servent essentiellement des types de contenu spécifiques. Par exemple, un serveur peut servir uniquement des images, un autre peut exécuter des langages de script côté serveur, tels que PHP et ASP, et un autre peut servir du contenu statique tel que HTML, CSS et JavaScript.

Règles L7

Les attributs suivants sont définis dans une règle pour évaluer le trafic et sont comparés aux valeurs définies dans la règle :

- Nom d'hôte : Le nom d'hôte dans la requête HTTP est comparé au paramètre de valeur dans la règle. Par exemple, <www.example-sports.com>.
- chemin : La partie chemin de l'URI HTTP est comparée au paramètre de valeur dans la règle. Par exemple, <www.example-sports.com/shopping-cart/football_pump.html>
- type_de_fichier : La dernière partie de l'URI est comparée au paramètre de valeur dans la règle. Par exemple, txt, html, jpg, PNG, xls, et autres.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- en-tête : L'en-tête défini dans le paramètre clé est comparé au paramètre de valeur dans la règle.
- cookie : Le cookie nommé par le paramètre clé est comparé au paramètre de valeur dans la règle. La valeur du champ d'en-tête de requête de cookie contient une paire nom-valeur d'informations stockées pour cette URL ; la syntaxe générale est la suivante : Cookie: nom=valeur. Par exemple, une règle qui recherche un cookie nommé « stores » avec la valeur commençant par « football- » ressemblera à : type = Cookie, compare_type=StartsWith, key = stores value = football-.

Types de comparaison

Lors de l'évaluation du trafic, la politique L7 compare les expressions suivantes aux attributs définis dans la règle.

- regex : Correspondance d'expressions régulières de type Perl
- starts_with: Chaîne commence par
- ends_with: Chaîne se termine par
- contains: Chaîne contient
- equal_to: Chaîne est égale à

REMARQUE

Les attributs de nom d'hôte, de chemin, d'en-tête et de cookie prennent en charge tous les types de comparaison, mais l'attribut file_type ne prend en charge que les regex et equal_to.

Stratégies L7

Une stratégie L7 traite le trafic HTTP entrant et renvoie une valeur "true" lorsque toutes les règles définies dans la stratégie sont respectées.

Dans toute stratégie L7, toutes les règles sont logiquement jointes par un opérateur ET. Une requête doit correspondre à toutes les règles pour que la stratégie renvoie une valeur "true". L'action entreprise par l'équilibreur de charge est basée sur la valeur renvoyée par la stratégie. Vous pouvez créer une deuxième stratégie avec la même action pour réaliser une opération OU logique entre les règles.

Par exemple, vous pouvez créer une stratégie où la requête HTTP entrante peut contenir les mots "EXAMPLE-SPORTS", "SPORTS-FOOTBALL" ou "EXAMPLE-FOOTBALL", afin que l'équilibreur de charge prenne l'action appropriée de transférer ces requêtes vers le pool de serveurs de la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

société de commerce électronique Example-sports pour servir le contenu demandé. Vous pouvez créer une autre stratégie qui effectue la même action mais correspond à "example-sports", "example-sports-football" ou "example-football". Lorsqu'un utilisateur envoie une requête HTTP avec l'un de ces six mots-clés, l'équilibreur de charge transfère la requête au serveur Example-Sports.

Selon les règles définies dans la stratégie, une stratégie L7 peut effectuer l'une des actions suivantes :

- Rediriger vers le pool - Transférer la requête vers le pool de serveurs d'applications identifié par les règles associées à la stratégie L7. Autrement dit, vous pouvez créer une règle d'application pour diriger les requêtes vers un pool d'équilibrage de charge spécifique en fonction du nom de domaine. Par exemple, vous pouvez créer une règle qui dirige certaines requêtes vers example-football.com vers pool_1, et d'autres requêtes vers example-sports-online_purchase.com vers pool_2.
- Rediriger vers l'URL - Envoyer au client une réponse HTTP de redirection dans laquelle l'en-tête de réponse de localisation contient le nouvel emplacement. Le navigateur mettra à jour la barre d'adresse avec le nouvel emplacement et émettra une nouvelle requête. Les cas d'utilisation sont nombreux. Par exemple, si l'adresse d'un site web a changé, vous pouvez rediriger les requêtes vers la nouvelle adresse au lieu de les abandonner. Ou, pendant la maintenance du site web, vous pouvez rediriger les utilisateurs vers un site en lecture seule.
- Rejeter - Rejette la requête et ne prend aucune autre mesure. Par exemple, vous pouvez renvoyer une réponse 401 Non autorisé pour refuser l'accès aux utilisateurs pour les pages web restreintes.

Une configuration de commutation de contenu se compose d'un serveur virtuel de commutation de contenu, d'une configuration d'équilibrage de charge (comprenant des serveurs virtuels et des services d'équilibrage de charge) et de stratégies de commutation de contenu. Après avoir créé le serveur virtuel de commutation et les stratégies, vous liez chaque stratégie à ce serveur. Lors de la liaison de la stratégie à ce dernier, vous spécifiez le serveur virtuel d'équilibrage de charge cible. Lorsqu'une requête atteint le serveur virtuel de commutation, celui-ci applique les stratégies de commutation associées à cette requête. La priorité de la stratégie définit l'ordre d'évaluation des stratégies liées au serveur virtuel de commutation.

Tout pool ayant l'ID d'écouteur peut être attribué comme pool par défaut de serveurs virtuels vers lesquels le trafic est redirigé. Le pool est lié de manière lâche à un écouteur et n'est associé à un écouteur que par la mise en œuvre d'une politique L7. Un pool peut également être créé directement sous un équilibreur de charge sans être nécessairement lié à un écouteur. Dans un tel cas, le pool est créé dans un état "pending_create". Étant donné que les politiques L7 sont

© 1997–2026 Citrix Systems, Inc. All rights reserved.

étroitement liées aux écouteurs, une politique L7 contenant l'ID du pool doit être créée et mise en œuvre pour que le pool devienne "actif" et commence à recevoir des requêtes de trafic.

Un pool peut être desservi par plusieurs politiques L7, mais reste à l'état "actif" si au moins une politique lui est attachée. Lorsque la dernière politique est supprimée, le pool retourne à l'état "pending_create" jusqu'à ce qu'une autre politique soit créée et lui soit associée. Si le pool lui-même est supprimé, toutes les requêtes HTTP qu'il aurait autrement reçues sont redirigées vers le pool par défaut.

MAPPAGE ENTRE LES POLITIQUES L7 OPENSTACK ET LES ENTITÉS NETSCALER

OpenStack	Entité NetScaler	Description
Politique L7 avec action REDIRECT_TO_POOL	Politique de commutation de contenu > Action de commutation de contenu	NetScaler Console crée une politique de commutation de contenu qui est liée au serveur virtuel de commutation de contenu et associée à une action de commutation de contenu qui spécifie le pool cible de serveurs d'applications pour la récupération et la présentation du contenu à l'utilisateur.
Politique L7 avec action REDIRECT_TO_URL	Politique de répondeur > Action de répondeur	NetScaler Console crée une politique de répondeur qui est liée au serveur virtuel de commutation de contenu et associée à une action de répondeur qui spécifie l'URL cible à présenter aux utilisateurs.
Politique L7 avec action REJECT	Politique de répondeur > Rejeter la requête	NetScaler Console crée une politique de répondeur qui est liée au serveur virtuel de commutation de contenu et associée à une action de répondeur qui rejette la requête.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si l'action d'une politique L7 qui évalue à "true" redirige le trafic vers un pool en état "create_pending", NetScaler Console implémente le pool spécifié ainsi qu'un serveur virtuel d'équilibrage de charge. NetScaler Console crée une politique de commutation de contenu à partir de la politique L7 et utilise l'action de commutation de contenu correspondante pour rediriger les requêtes vers le serveur virtuel d'équilibrage de charge associé à ce pool. Si une deuxième politique L7 redirige vers le même pool, NetScaler Console crée une politique de commutation de contenu et une action de commutation de contenu pour rediriger le trafic vers le serveur virtuel d'équilibrage de charge existant associé à ce pool.

POSITIONNEMENT DES POLITIQUES

L'évaluation des politiques L7 dans OpenStack est déterminée par leurs priorités. Dans OpenStack, par défaut, les politiques se voient attribuer des priorités dans l'ordre de leur création. La politique créée en premier est numérotée "1", et les politiques créées ultérieurement sont numérotées consécutivement. Cependant, vous pouvez modifier les priorités des politiques et leur attribuer des priorités différentes. Les politiques sont toujours évaluées dans l'ordre de leurs priorités. La première politique qui correspond à une requête spécifique est toujours exécutée en premier.

Lors de la création de politiques, notez les points suivants :

- Si vous attribuez à une nouvelle politique la même priorité qu'une politique existante, la nouvelle politique prend cette priorité. La priorité de la politique existante est abaissée. Si nécessaire, les priorités des autres politiques sont également abaissées pour conserver l'ordre dans lequel les politiques sont évaluées.
- Si vous créez une nouvelle politique sans spécifier de position, la nouvelle politique sera simplement ajoutée à la liste.
- Si vous créez une nouvelle politique et lui attribuez une position supérieure au nombre de politiques déjà présentes dans la liste, la nouvelle politique sera ajoutée à la liste, c'est-à-dire que la nouvelle politique prendra toujours la prochaine priorité disponible. Par exemple, s'il existe trois politiques A, B et C avec les priorités 1, 2 et 3, et si vous créez une politique et lui attribuez une priorité de 8, la priorité de la nouvelle politique devient 4.
- Si vous ajoutez une politique à la liste ou en supprimez une, les valeurs de position des politiques sont réordonnées à partir de 1 sans sauter de numéros. Par exemple, si les politiques A, B, C et D ont des valeurs de position de 1, 2, 3 et 4, et si vous supprimez la politique B de la liste, la politique C prend alors la deuxième position et la politique D prend la troisième position.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans NetScaler Console, il existe toujours une politique par défaut associée à un `csvserver` avec une priorité de 1. Cette politique par défaut spécifie le nombre de connexions TCP qu'un `lbvserver` traite à un moment donné. Par conséquent, lorsque les politiques de répondeur et les politiques de commutation de contenu correspondantes sont créées dans NetScaler, elles se voient toujours attribuer une priorité supérieure de 1 à la priorité de la politique L7 correspondante. Par exemple, lorsqu'une politique L7 avec une priorité de 1 est évaluée et qu'une politique de commutation de contenu est créée avec une priorité de 2. De même, lorsqu'une politique L7 avec une priorité de 2 est évaluée et qu'une politique de répondeur est créée avec une priorité de 3.

Dans OpenStack, la politique "reject" ou "redirect_to_url" est évaluée en premier, puis la politique "redirect_to_pool" est évaluée. Dans une instance NetScaler, les politiques de répondeur sont toujours évaluées en premier pour soit abandonner la requête, soit présenter à l'utilisateur une adresse web redirigée, et les politiques de commutation de contenu sont évaluées en dernier. Cet ordre d'évaluation ne cause généralement aucun conflit si les politiques de commutation de contenu et de répondeur sont mutuellement exclusives. C'est-à-dire que deux politiques L7 ne doivent pas avoir des expressions identiques. Les expressions dérivées sont ajoutées dans les politiques de répondeur et de commutation de contenu pour éviter de tels conflits. Par exemple, écrivez une expression pour rejeter toutes les requêtes vers "sports-football.com" et une autre expression pour autoriser les requêtes vers "example-sports-football.com". Créez les politiques L7 de manière à ce que toutes les politiques de répondeur pour rejeter la requête soient placées en haut de la liste d'évaluation, suivies des politiques de répondeur pour la redirection web, suivies des politiques de commutation de contenu.

Dans NetScaler Console, il existe toujours une politique par défaut associée à un `csvserver` avec une priorité de 1. Cette politique par défaut spécifie le nombre de connexions TCP qu'un `lbvserver` traite à un moment donné. Par conséquent, lorsque les politiques de répondeur et les politiques de commutation de contenu correspondantes sont créées dans NetScaler, elles se voient toujours attribuer une priorité supérieure de 1 à la priorité de la politique L7 correspondante. Par exemple, lorsqu'une politique L7 avec une priorité de 1 est évaluée et qu'une politique de commutation de contenu est créée avec une priorité de 2. De même, lorsqu'une politique L7 avec une priorité de 2 est évaluée et qu'une politique de répondeur est créée avec une priorité de 3.

Dans OpenStack, la politique "reject" ou "redirect_to_url" est évaluée en premier, puis la politique "redirect_to_pool" est évaluée. Dans NetScaler, les politiques de répondeur sont toujours évaluées en premier pour soit abandonner la requête, soit présenter à l'utilisateur une adresse web redirigée, et les politiques de commutation de contenu sont évaluées en dernier. Cet ordre d'évaluation ne cause généralement aucun conflit si les politiques de commutation de contenu et de répondeur sont mutuellement exclusives. C'est-à-dire qu'aucune deux politiques L7 n'ont d'expressions similaires. Des expressions dérivées similaires sont ajoutées dans les politiques de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

répondeur et de commutation de contenu pour éviter de tels conflits. Par exemple, écrivez une expression pour rejeter toutes les requêtes vers "sports-football.com" et une autre expression pour autoriser les requêtes vers "example-sports-football.com". Créez les politiques L7 de manière à ce que toutes les politiques de répondeur pour rejeter la requête soient placées en haut de la liste d'évaluation, suivies des politiques de répondeur pour la redirection web, suivies des politiques de commutation de contenu.

TÂCHES DE CONFIGURATION

Les implémentations des politiques et actions L7 sont effectuées via les commandes Neutron LBaaS.

Définissez les variables d'environnement dans OpenStack et créez l'équilibreur de charge (par exemple, LB1). Une fois l'équilibreur de charge créé avec succès, créez l'écouteur et les pools (par exemple, L1, P1 et P2), et ajoutez des membres et des moniteurs aux pools. Par exemple, P1 est le pool par défaut pour L1, tandis que P2 est le pool lié à LB1 et gérant les serveurs d'applications.

Pour plus d'informations sur la configuration de LBaaS V2 à l'aide de la ligne de commande, consultez (/fr-fr/netscaler-application-delivery-management-software/current-release/orchestration/integrate-with-openstack-platform/openstack-configuring-lbaasv2-using-command-line.html).

Les commandes suivantes créent les stratégies et définissent les actions spécifiques :
Créer une stratégie L7 pour rejeter les requêtes

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action&lt;action-name>
```

Exemple :

neutron lbaas-l7policy-create --name policy11 --action REJETER --listener L1

La commande ci-dessus crée et lie policy11, une stratégie de répondeur, au serveur de commutation de contenu pour rejeter les requêtes. Comme aucune règle n'a été créée pour cette stratégie, la stratégie est évaluée à « faux » et la requête est rejetée.
Créer une stratégie L7 pour rediriger les requêtes vers une URL particulière

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-url &lt;redirect-
url>
```

Exemple :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

neutron lbaas-l7policy-create --name policy12 --action REDIRECTION_VERS_URL --listener admin-list1 --redirect-url `http://example-sports/about-us.html`

La commande ci-dessus crée une action de répondeur pour rediriger les requêtes vers une URL, crée une stratégie de répondeur avec action et lie cette stratégie au serveur virtuel de commutation de contenu.

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
value &lt;value-string> &lt;L7 policy name>



neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
&lt;value-string> &lt;L7 policy name>
```

Les deux règles ci-dessus peuvent être connectées avec un opérateur ET pour dériver l'expression de la stratégie de répondeur.
Créer une stratégie L7 pour rediriger les requêtes vers un pool

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-pool &lt;redirect-
pool>
```

Exemple :

neutron lbaas-l7policy-create --name policy13 --action REDIRECT_TO_POOL --listener admin-list1 --redirect-pool admin-pool2

S'il s'agit de la première stratégie L7, la commande ci-dessus implémente P2 avec LB1, crée l'action de redirection de commutation de contenu et redirige les requêtes vers LB1. Si P2 existe déjà, la commande crée l'action de redirection de commutation de contenu et redirige les requêtes vers LB1.

Provisionnement manuel d'une instance NetScaler VPX sur OpenStack

Dans certains réseaux d'entreprise, les instances NetScaler VPX ne peuvent pas se connecter au serveur de licences NetScaler pour télécharger automatiquement les licences, pour des raisons de sécurité. Dans un tel scénario, vous devez déployer manuellement les instances NetScaler VPX sur la plateforme OpenStack. À l'aide du code d'accès à la licence que vous avez reçu de Citrix, téléchargez la licence NetScaler VPX appropriée et enregistrez-la sur votre système local.

Pour provisionner manuellement une instance NetScaler VPX sur OpenStack :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Installez le logiciel du pilote NetScaler et enregistrez NetScaler Console sur OpenStack

    a. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration cloud** \> **OpenStack**.

    b. Cliquez sur **Configurer les paramètres OpenStack**. Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack dans NetScaler Console. Vous avez deux options ici : **Par défaut** et **Personnalisé**.

    c. Sélectionnez **Par défaut**, si les services OpenStack s'exécutent sur les ports par défaut.

2. Accédez à **Orchestration** \> **Orchestration cloud** \> **OpenStack**, puis cliquez sur **Paramètres de déploiement**.

    a. **Réseau de gestion** - sélectionnez le réseau de gestion sur OpenStack, auquel le NetScaler VPX auto-provisionné est connecté.

    b. **Nom du profil** - sélectionnez le profil dans la liste déroulante. NetScaler Console utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances NetScaler VPX auto-provisionnées.

    c. Image NetScaler VPX dans Glance - sélectionnez l'image NetScaler VPX disponible dans OpenStack Glance qui est utilisée pour créer une instance NetScaler VPX. La liste déroulante affichera uniquement les images présentes sur OpenStack Glance.

3. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration cloud** \> **OpenStack** \> **Packages de services**, puis cliquez sur **Ajouter**.

4. Sur la page **Package de services**, spécifiez les paramètres suivants :

    a. **Nom** - nom du package de services. Par exemple, entrez SVC-PKG-GOLD.

    b. **Allocation d'instance NetScaler** - sélectionnez **Dédié** ou **Partitionné** comme type d'allocation d'instance défini dans le package de services.

    c. **Provisionnement d'instances NetScaler** - sélectionnez **Créer une instance à la demande** pour créer des instances NetScaler pendant la configuration elle-même.

    d. **Plateforme de provisionnement automatique** - sélectionnez **OpenStack Compute**. Par défaut, NetScaler VPX sera sélectionné comme type d'instance.

    e. **Attribuer des locataires/stratégies de placement OpenStack** - section, sous Locataires OpenStack, cliquez sur **Ajouter**, et sélectionnez le locataire.

    f. Cliquez sur **Continuer**, puis cliquez sur **Terminé**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Accédez à **Système** \> **Administration du système** \> **Modifier les paramètres système** et sélectionnez **http** dans la liste déroulante.
6. Accédez à **Infrastructure > Instances > NetScaler VPX**.
7. Dans la page **NetScaler VPX**, cliquez sur la liste déroulante **Admin** et sélectionnez **Provisionner le périphérique**.

   a. Sur la page **Provisionnement du périphérique**, saisissez le nom du périphérique, et sélectionnez le package de services que vous avez créé à l'étape précédente.

   b. Cliquez sur **OK**.

8. Accédez à l'onglet **Orchestration** \> **Orchestration cloud** \> **OpenStack** \> **Requêtes**. Sélectionnez la requête et cliquez sur **Tâches** pour afficher les tâches. Lorsque le statut de la tâche passe à **Terminé**, cela signifie que le NetScaler VPX est provisionné dans NetScaler Console.
9. Accédez à **Infrastructure > Instances** \> **NetScaler VPX** pour vérifier que l'instance NetScaler VPX apparaît dans la page NetScaler VPX.
10. Cliquez sur l'instance NetScaler VPX. Lorsque l'instance NetScaler VPX s'ouvre dans la fenêtre de votre navigateur, connectez-vous à l'instance. Accédez à **Configuration** \> **Système** \> **Licences**, et ajoutez manuellement la nouvelle licence. Pour plus d'informations sur l'ajout d'une nouvelle licence, consultez Présentation des licences NetScaler.
11. Redémarrez l'instance NetScaler VPX.
12. Après quelques minutes, vous pouvez vous connecter à OpenStack et, dans **Système** \> **Instances**, vous pouvez voir que l'instance NetScaler VPX est déployée sur OpenStack.
13. Les implémentations de l'API LBaaS V2 sont effectuées via les commandes Neutron LBaaS. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur l'exécution des commandes de configuration, consultez Configuration de LBaaS V2 à l'aide de la ligne de commande.

Provisionnement d'une instance NetScaler VPX sur OpenStack à l'aide de StyleBook

Dans le flux de travail d'orchestration OpenStack, NetScaler Console utilise désormais le StyleBook `os-cs-lb-mon` pour déployer les configurations LBaaS sur les instances NetScaler allouées au locataire OpenStack. Un pack de configuration est créé pour chaque équilibreur de charge créé par l'utilisateur OpenStack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L'utilisation de StyleBooks pour la configuration dans un flux de travail OpenStack offre les avantages suivants :

- Meilleure visualisation en affichant tous les objets de configuration.
- Fiabilité grâce à la restauration.
- Prise en charge de divers types d'instances NetScaler (NetScaler HA, partitions, VPX, CPX, MPX et autres).
- Personnalisation en utilisant vos propres StyleBooks pour déployer la configuration pour les locataires OpenStack.

En tant qu'administrateur de NetScaler Console, accédez à **Applications** > **Configurations** pour afficher le pack de configuration déployé sur l'instance NetScaler. Vous pouvez effectuer les tâches suivantes :

- Faites défiler pour afficher le pack de configuration `os-cs-lb-mon` déployé pour l'équilibreur de charge.
- Cliquez sur **Afficher la définition** dans le panneau StyleBook `os-cs-lb-mon` pour vérifier la configuration déployée sur les instances.
- Cliquez sur **Afficher l'objet** pour afficher la liste des objets ou entités NetScaler déployés sur les instances.

Points à noter avant de provisionner des instances à l'aide de StyleBooks

À partir de NetScaler Console 12.1 build 49.23, l'architecture d'un flux de travail d'orchestration OpenStack a été mise à jour. Le flux de travail utilise désormais les StyleBooks de NetScaler Console pour configurer les instances NetScaler. Si vous effectuez une mise à niveau vers NetScaler Console 12.1 build 49.23 à partir de la version 12.0 ou de la version 12.1 build 48.18, vous devez exécuter le script de migration suivant :

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

- L'exécution du script de migration crée des packs de configuration du StyleBook `os-cs-lb-mon` correspondant aux configurations OpenStack existantes.
- L'exécution de ce script de migration est obligatoire si vous aviez des configurations OpenStack déployées à partir de ces versions antérieures.
- Vous pouvez déployer de nouvelles configurations sur les instances à l'aide du StyleBook `os-cs-lb-mon` seulement après avoir exécuté le script de migration à partir de la version 12.1 build 49.23.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Toutes les configurations tentées depuis OpenStack échouent jusqu'à ce que le script de migration soit exécuté.

REMARQUE

- Une fois que vous avez exécuté le script de migration, vous ne pouvez pas revenir à la version précédente de NetScaler Console.
- Assurez-vous d'avoir mis à niveau les pilotes NetScaler pour OpenStack LBaaS V2 vers la dernière version. Utilisez les fichiers de bundle NetScaler fournis avec la dernière version de NetScaler Console 13.0.

Les implémentations de l'API LBaaS V2 sont effectuées via les commandes Neutron LBaaS. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur l'exécution des commandes de configuration, consultez Configuration de LBaaS V2 à l'aide de la ligne de commande.

Prise en charge des licences VPX d'enregistrement et de retrait et des licences en pool pour l'environnement OpenStack

Dans le workflow d'orchestration OpenStack, NetScaler Console crée des instances NetScaler VPX à la demande lorsque vous sélectionnez un package de services avec **OpenStack Compute**. Désormais, la page des packages de services de la fonctionnalité d'orchestration dans NetScaler Console est améliorée pour fournir la licence qui doit être installée sur les instances NetScaler VPX créées à la demande. Les licences fournies peuvent être des licences VPX d'enregistrement et de retrait ou des licences en pool.

Pour utiliser cette fonctionnalité, vous devez d'abord télécharger les licences dans NetScaler Console, puis créer des packages de services qui utilisent OpenStack compute.

- S'il s'agit d'une licence d'enregistrement et de retrait, vous pouvez choisir la licence à installer parmi les différentes licences disponibles.

  

- S'il s'agit d'une licence en pool, vous pouvez sélectionner à la fois la bande passante et le type d'édition de licence à installer.

  

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Chaque fois que vous déployez votre premier équilibreur de charge avec NetScaler Console en tant que fournisseur, NetScaler Console crée l'instance NetScaler VPX et installe la licence spécifiée dans le package de services sur l'instance nouvellement créée.

De plus, lorsque vous supprimez une instance d'équilibrage de charge existante, cette instance n'est plus nécessaire. L'instance est désactivée et la licence est renvoyée à NetScaler Console. Cela permet une utilisation optimale des licences disponibles dans NetScaler Console.

REMARQUE

Lorsque NetScaler Console est déployé en mode haute disponibilité, considérez que les licences sont téléchargées sur la NetScaler Console active ou principale actuelle, MAS-HA-1. Lorsque vous déployez la première requête et que NetScaler Console crée les instances NetScaler VPX, l'instance extrait les licences requises de MAS-HA-1. Plus tard, supposons que la NetScaler Console secondaire, MAS-HA-2, qui ne possède pas les licences, est maintenant active. L'instance NetScaler VPX ne peut pas extraire la licence de MAS-HA-2 maintenant et, par conséquent, l'instance ne peut pas être créée pour les nouveaux utilisateurs.

Dans un tel cas, assurez-vous que MAS-HA-1 est opérationnel et est maintenant le nœud principal actuel. C'est-à-dire, basculez manuellement la NetScaler Console de MAS-HA-2 vers MAS-HA-1. Après cela, vous devez retenter la configuration depuis OpenStack et les instances seront recréées avec les licences appropriées. Pour plus d'informations sur la prise en charge des licences dans le déploiement haute disponibilité de NetScaler Console, consultez Haute disponibilité.

Prise en charge du VLAN partagé pour les partitions d'administration

Pour les locataires se connectant à partir de réseaux privés, NetScaler Console prend en charge une politique d'isolation afin que chaque locataire dispose de sa propre partition dédiée, d'un VLAN dédié et de serveurs dédiés. Pour les locataires se connectant à partir de réseaux publics, un VLAN dédié nécessiterait l'utilisation de trop d'adresses IP. Un VLAN partagé contourne ce problème en créant une adresse IP virtuelle sur chaque partition, créant ainsi un seul sous-réseau IP.

Lorsqu'un locataire configure une VIP ou un écouteur, une partition d'administration est créée dans l'appliance NetScaler pour ce locataire. Toute la configuration de l'équilibreur de charge est poussée vers cette partition d'administration créée. Si le locataire utilise un réseau partagé ou un réseau externe pour créer un équilibreur de charge, le VLAN de ce réseau est ajouté et la fonction

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de partage est activée. Lorsqu'un autre locataire utilise le même réseau partagé pour créer son équilibreur de charge, le VLAN n'est pas ajouté à nouveau au NetScaler, mais le VLAN sera également lié à la deuxième partition. Ainsi, tout locataire qui utilise le même réseau partagé obtient une partition liée au même VLAN.

NetScaler Console prend en charge l'adresse MAC de destination virtuelle. Lorsque les locataires partagent un VLAN, NetScaler Console attribue différentes adresses MAC à la partition sur l'appliance NetScaler. Cela permet de partager un VLAN entre les partitions ou entre tous les locataires et tous les domaines de trafic.

Configuration du VLAN partagé à partir d'une instance NetScaler

1. Dans une instance NetScaler, accédez à **Configuration** \> **Système** \> **Réseau** \> **VLANs**, sélectionnez un profil VLAN, puis cliquez sur **Modifier** pour définir le paramètre de partage de partition.
2. Sur la page **Configurer le VLAN**, cochez la case **Partage de partitions**.
3. Cliquez sur **OK**.



Configuration du VLAN partagé à partir de l'orchestration OpenStack

1. Dans OpenStack, accédez à **Admin** \> **Système** \> **Réseaux**, puis cliquez sur **Créer un réseau**.
2. Dans **Créer un réseau**, définissez les paramètres suivants :
   a. Nom - entrez le nom du réseau
   b. Projet - sélectionnez un projet dans la liste déroulante
   c. Type de réseau fournisseur - sélectionnez **VLAN** dans la liste déroulante. Cela définit que le réseau virtuel est établi en tant que VLAN.
   d. Réseau physique - le réseau physique par défaut est sélectionné ici. Vous pouvez le modifier.
   e. État d'administration - par défaut, l'état administratif du réseau est ACTIF
   f. Sélectionnez **Partagé** et **Externe** pour le réseau afin de définir que le VLAN est partagé et utilise un réseau externe.
3. Cliquez sur **Créer un réseau**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Flux de travail de la licence d'essai

Lors du provisionnement automatique de l'instance NetScaler VPX à l'aide de l'orchestration OpenStack, la console NetScaler utilise OpenStack Compute pour lancer une instance NetScaler VPX. L'instance NetScaler VPX nouvellement provisionnée contacte le portail de licences Citrix lors de la configuration et utilise le code d'accès à la licence pour télécharger et installer automatiquement les fichiers de licence.

Licences d'essai

Le personnel du support technique utilise des licences d'essai lors de l'installation des dispositifs NetScaler Console et NetScaler VPX sur le terrain. Une licence d'essai ou d'évaluation pour NetScaler VPX est valide pendant 90 jours. S'il est nécessaire d'évaluer plus d'un NetScaler ou de prolonger les tests après 90 jours, une nouvelle licence d'évaluation doit être demandée. Au lieu de l'installation automatique des fichiers de licence d'essai, NetScaler Console vous offre une solution alternative. Vous pouvez télécharger manuellement les fichiers de licence et les installer sur NetScaler VPX pour terminer l'installation de l'instance.

Si le NetScaler VPX ne peut pas se connecter à Internet, configurez la console NetScaler pour qu'elle agisse comme un serveur proxy pour le portail de licences Citrix et installez les fichiers de licence.

Les instances NetScaler VPX disposant d'une licence d'essai peuvent communiquer avec NetScaler Console uniquement via HTTP. Pour configurer la communication HTTP dans NetScaler Console, accédez à **System** \> **System Administration**, puis cliquez sur **Change System Settings**. Sélectionnez **http** dans la liste déroulante pour définir la méthode de communication, puis cliquez sur **OK**.



Intégrer avec les services OpenStack Heat

Le service OpenStack Neutron LBaaS permet des services d'équilibrage de charge essentiels, tels que l'équilibrage de charge, le déchargement SSL et la commutation de contenu, pour les applications. LBaaS est géré via une API REST, et l'API permet aux locataires d'effectuer des appels REST pour créer, mettre à jour et supprimer des objets LBaaS. Étant donné que LBaaS fournit des services d'équilibrage de charge, il ne permet pas l'utilisation des fonctionnalités NetScaler plus avancées pendant le processus d'orchestration. Le plug-in NetScaler Heat surmonte cette limitation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service d'orchestration Heat

Le service d'orchestration OpenStack Heat permet le déploiement d'applications cloud complexes basées sur des modèles. Le modèle d'orchestration Heat (HOT) décrit l'infrastructure d'une application cloud dans des fichiers texte lisibles et modifiables par l'homme, et pouvant être gérés par des outils de contrôle de version. YAML, un langage structuré, est utilisé pour écrire ces modèles. Le modèle HOT vous permet de créer la plupart des types de ressources OpenStack et spécifie les relations entre les ressources qui y sont définies. Le plug-in NetScaler Heat vous permet de configurer des fonctionnalités NetScaler avancées sur n'importe quelle instance NetScaler.

StyleBooks NetScaler

Les StyleBooks de NetScaler Console peuvent être utilisés pour créer et configurer des fonctionnalités NetScaler. Tout comme les modèles Heat, les StyleBooks sont également écrits en YAML. Un StyleBook distinct peut être créé pour chaque fonctionnalité, et un seul StyleBook peut être utilisé pour déployer des configurations sur plusieurs instances NetScaler.

Lors de l'intégration de NetScaler avec OpenStack, NetScaler Console publie tous les StyleBooks de NetScaler Console en tant que ressource dans le service Heat. Cela inclut à la fois les StyleBooks fournis avec NetScaler Console et les StyleBooks créés par l'utilisateur ultérieurement. Le modèle Heat vous permet de configurer les fonctionnalités avancées des NetScalers à l'aide de ces ressources StyleBooks.

Flux de travail pour configurer les instances NetScaler à l'aide de Heat

L'organigramme suivant illustre le flux de travail pour le déploiement de la pile Heat :



Effectuez les tâches suivantes en tant qu'administrateur cloud :

Pour configurer les services Heat dans OpenStack :

1. Télécharger les bundles NetScaler pour OpenStack

   Installez les bundles NetScaler dans OpenStack. Dans NetScaler Console, accédez à **Téléchargements** et téléchargez les bundles de pilotes NetScaler, décompressez les bundles et copiez le contenu du dossier Heat du bundle dans le répertoire des ressources du moteur Heat dans OpenStack. Le chemin du répertoire est le suivant : /opt/stack/heat/heat/engine/resources/netscaler_resources
2. Créez une section « netscaler_plugin » dans le fichier heat.conf et mettez à jour les paramètres suivants dans cette section :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Lorsque la communication est HTTP, les paramètres sont mis à jour comme suit :

   NMAS_BASE_URI=< `http://10.146.103.45:80` >

   NMAS_USERNAME=<openstack_driver_username>

   NMAS_PASSWORD=<openstack_driver_password>

b. Lorsque la communication est HTTPS, les paramètres sont mis à jour comme suit :

   NMAS_BASE_URI= `https://common_name_used_in_certificate`

   NMAS_USERNAME=\<openstack_driver_username

   NMAS_PASSWORD=\<openstack_driver_password\>

   SSL_CERT_VERIFY=\<True_or_False\>

   CERT_FILE_PATH=\<path_of_the_certificate_file\>

   Si l'utilisateur définit ssl_cert_verify sur « False », NetScaler Console envoie verify=False dans les appels de requête, ce qui désactive la validation du certificat SSL. Si ssl_cert_verify est défini sur « True » et que l'entrée cert_file_path est présente, NetScaler Console envoie ce chemin dans le paramètre de vérification de la requête, sinon NetScaler Console envoie verify=True.

   REMARQUE

   Pour déployer NetScaler Console en mode « Haute disponibilité », mettez à jour les paramètres suivants dans le fichier heat.conf :

   NMAS_BASE_URI=\<adresse IP du serveur virtuel frontal\>

3. Redémarrez le service Heat dans OpenStack.

   Lorsque vous redémarrez les services NetScaler Heat dans OpenStack, tous les StyleBooks NetScaler Console définis sont importés dans Heat en tant que ressources. De plus, la ressource réseau NetScaler et la ressource de certificat sont importées dans OpenStack en tant que ressources NetScaler Heat.

4. Enregistrez NetScaler Console auprès d'OpenStack.

   a. Dans NetScaler Console, accédez à **Orchestration** \> **Cloud Orchestration** \> **OpenStack**, puis cliquez sur **Configure OpenStack Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Dans la page **Configure OpenStack Settings**, vous pouvez définir les paramètres de configuration d'OpenStack. Vous avez deux options ici : Default et Customized.

c. Sélectionnez **Default** si les services OpenStack s'exécutent sur les ports par défaut. Saisissez les paramètres suivants :

   i. Adresse IP du contrôleur OpenStack

   ii. Nom d'utilisateur administrateur

   iii. Mot de passe

   iv. Locataire administrateur OpenStack

   v. Mot de passe du pilote NetScaler et de Heat

REMARQUE

Il s'agit du même mot de passe (NMAS_PASSWORD) que celui que vous avez saisi dans le fichier heat.conf.

5. Créez des packages de services et définissez les SLA avec votre locataire.

   Un locataire est créé dans NetScaler Console pour chaque utilisateur lors de l'enregistrement OpenStack, et les informations du locataire sont utilisées à la fois par le pilote LBaaS et le plug-in Heat. Le plug-in Heat utilise ces informations pour contacter NetScaler Console afin d'importer les StyleBooks en tant que ressources Heat dans OpenStack.

   REMARQUE

   Pour plus d'informations sur la création de packages de services et d'autres tâches de pré-configuration dans NetScaler Console et OpenStack, consultez Intégration de NetScaler Console à la plate-forme OpenStack.

6. Notez que tous les StyleBooks pertinents dans NetScaler Console sont importés dans OpenStack Heat en tant que ressources. Notez également que la ressource réseau NetScaler et la ressource de certificat NetScaler sont importées dans OpenStack Heat en tant que ressources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Actuellement, vous ne pouvez utiliser que les StyleBooks fournis avec NetScaler Console.

Votre locataire peut maintenant créer le modèle Heat dans OpenStack, saisir les valeurs des paramètres Heat requis et déployer la pile Heat. Lorsque la pile Heat est déployée, la configuration est transmise à NetScaler Console et les instances NetScaler requises sont configurées.

Pour préparer le modèle Heat et lancer la pile Heat :

1. Dans OpenStack, le locataire peut créer un modèle d'orchestration Heat (HOT) en utilisant les ressources Heat.
2. Dans OpenStack Horizon, l'administrateur du locataire peut accéder à **Project** \> **Orchestration** \> **Stacks** pour créer le modèle Heat et lancer la pile Heat. Il existe deux façons de créer un HOT :

   - **Fichier** - Sélectionnez le modèle mis à jour à partir du répertoire local
   - **Saisie directe** - Copiez et collez le contenu YAML du modèle dans la fenêtre

   REMARQUE

   Après avoir déployé la pile avec succès, le locataire peut la mettre à jour en utilisant le modèle de modification de pile (Change Stack Template). Cependant, les informations de sous-réseau et l'adresse IP virtuelle (VIP) fournies initialement lors de la création de la pile ne peuvent pas être modifiées.

   Une fois que le locataire a déployé la pile, accédez à **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Requests** dans NetScaler Console pour consulter les listes de tâches. Accédez également à **Applications** \> **Configuration** dans NetScaler Console pour vérifier que les instances NetScaler sont configurées avec succès sous forme de packs de configuration StyleBooks.

Exemple de StyleBooks NetScaler Console :

L'image suivante montre un exemple de la façon dont un StyleBook NetScaler Console est construit et explique brièvement les composants. Pour plus d'informations sur les StyleBooks NetScaler Console et sur la façon d'utiliser les StyleBooks fournis, consultez StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple de modèle Heat :

L'image suivante montre la structure d'un modèle Heat défini en YAML, et indique les ressources StyleBooks et les ressources réseau NetScaler qui sont importées en tant que ressources Heat.

Pour plus d'informations sur les services Heat et sur la création de modèles, consultez la documentation OpenStack Heat.

Stratégies d'isolation des packages de services

Stratégie d'isolation dédiée

Chaque locataire associé au package de services NetScaler Console d'une stratégie dédiée se voit attribuer une instance NetScaler parmi les instances faisant partie de ce package de services. Cette instance NetScaler attribuée n'est pas partagée avec d'autres locataires.

Stratégie d'isolation de partition

Chaque locataire associé au package de services de la stratégie de partition se voit attribuer une partition d'administration logique dédiée d'une instance NetScaler faisant partie du package de services.

Stratégie d'isolation partagée

Les locataires associés au package de services partagent les instances NetScaler qui font partie du package de services. Toutes les configurations d'un locataire sont attribuées à une seule instance NetScaler. Dans ce mode, les configurations de plusieurs locataires peuvent être hébergées sur la même instance NetScaler. Vous pouvez sélectionner **NetScaler VPX** ou **NetScaler MPX** comme type de périphérique. Vous pouvez choisir d'allouer une seule instance NetScaler ou plusieurs instances au package de services. Autrement dit, plusieurs locataires peuvent partager une ou plusieurs instances virtuelles du périphérique NetScaler.

REMARQUE

Ajoutez les instances NetScaler SDX dans les packages de services uniquement en tant qu'instances NetScaler VPX, car un NetScaler SDX dispose d'un NetScaler VPX provisionné sur celui-ci.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous pouvez également créer des stratégies de placement flexibles, où les stratégies ne sont pas basées uniquement sur le nom ou l'ID du locataire, mais sur d'autres attributs personnalisés. Pour plus d'informations sur les stratégies de placement flexibles, consultez Allocation de périphériques basée sur une stratégie flexible.

Allocation flexible de périphériques basée sur des politiques

NetScaler Console attribue des instances virtuelles NetScaler aux locataires, en fonction des SLA convenus avec les locataires. L'attribution d'instances virtuelles aux locataires crée une relation un-à-un entre l'instance et le locataire, où un locataire ne peut être attribué qu'à un seul package de services dans le centre de données.

Dans certaines situations, les locataires peuvent nécessiter plus d'une instance, ou l'attribution d'instances peut ne pas être basée sur les locataires comme critère, mais sur d'autres facteurs tels que l'ID réseau ou l'application. Dans de tels cas, NetScaler Console vous permet de définir précisément des politiques de placement basées sur des expressions définies par l'utilisateur afin d'attribuer une configuration d'équilibreur de charge à l'une des instances gérées.

Les politiques de placement offrent la flexibilité de décider de l'instance NetScaler utilisée dans chaque configuration d'équilibreur de charge créée par les utilisateurs. Les politiques de placement flexibles dans NetScaler Console offrent une option supplémentaire à la méthode existante d'attribution d'instances NetScaler basée sur les locataires.

REMARQUE

Vous pouvez attribuer des instances aux locataires manuellement ou utiliser des politiques de placement pour attribuer des instances basées sur les expressions créées. Vous ne pouvez pas utiliser ces deux méthodes simultanément sur un seul package de services.

Les politiques de placement sont basées sur des expressions booléennes définies sur les propriétés des principaux objets de configuration LBaaS, tels que les pools et les équilibreurs de charge. L'interface utilisateur de la politique de placement dans NetScaler Console fournit des expressions prédéfinies que vous pouvez choisir pour définir une politique personnalisée. Vous pouvez créer plusieurs politiques de placement pour différentes expressions. Ainsi, chaque locataire peut avoir plusieurs périphériques définis par ses exigences.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous devez d'abord sélectionner une expression pour faire correspondre un objet racine qui devra être configuré ultérieurement. L'objet racine peut être un objet pool dans le cas de LBaaS V1, et un objet équilibreur de charge dans le cas de LBaaS V2. Ainsi, les placements basés sur les politiques de NetScaler Console sont pris en charge pour les API LBaaS V1 et V2. Ces politiques de placement sont ensuite associées à des packages de services. Une fois l'objet racine placé dans une instance, les objets successifs du modèle sont ajoutés dans l'instance.

Par exemple, l'objet de configuration du pool peut avoir les propriétés suivantes :

- tenant_id
- nom
- Description
- protocole
- lb_method
- subnet_id
- subname_name
- admin_state_up
- état
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

Voici des exemples qui montrent certaines des expressions utilisant les propriétés de pool pour définir une expression pour la politique :

1. Expression de politique basée sur le nom du pool

   ```
   config["pools"]["name"] =="high-end-pool"
   ```

2. Expression de politique basée sur le nom du sous-réseau du pool

   ```
   config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
   ```

3. Expression de politique basée sur le nom du sous-réseau de l'équilibreur de charge

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
config["loadbalancers"]["subnet_name"] == "mas-subnet"
```

Ajout d'une politique de placement

1. Depuis la page d'accueil de NetScaler Console, accédez à **Orchestration** > **Cloud Orchestration** > **Placement Policy**, puis cliquez sur **Ajouter**.
2. Sur la page **Ajouter une politique de placement**, définissez les paramètres suivants :

   a. Nom - tapez un nom pour la politique de placement

   b. Expressions fréquemment utilisées - sélectionnez une expression dans la liste déroulante.

   c. Expression - une expression logique (booléenne) est renseignée dans ce champ en fonction de l'expression que vous avez sélectionnée dans le champ précédent. Modifiez les noms de champ si nécessaire.

   REMARQUE

   Lorsque vous créez plusieurs politiques, assurez-vous qu'elles sont exclusives les unes aux autres.

3. Cliquez sur **OK**.
4. Accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages**, puis cliquez sur **Ajouter**.
5. Sur la page **Service Package**, définissez les paramètres suivants :

   a. Nom - tapez un nom pour le package de service

   b. Politique d'isolation - sélectionnez la politique **Partagée**

   Dans une politique d'isolation partagée, la configuration de l'équilibreur de charge d'un locataire coexiste avec la configuration de l'équilibreur de charge d'autres locataires dans l'appareil alloué au locataire.

   c. Type d'appareil - sélectionnez un **NetScaler VPX** ou **NetScaler MPX** pré-provisionné

   Sélectionnez **Allouer un appareil** si vous souhaitez que toutes les configurations d'équilibreur de charge d'un locataire soient liées à un seul appareil. Sélectionnez **Allouer plusieurs appareils** si vous souhaitez que chaque configuration d'équilibreur de charge

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d'un locataire soit distribuée sur plusieurs appareils en fonction des politiques de placement.

REMARQUE

NetScaler SDX doit être ajouté dans les packages de services uniquement en tant qu'instances NetScaler VPX, car un NetScaler SDX a un NetScaler VPX provisionné dessus.

d. Méthode de placement - sélectionnez **Moins configuré**

Lorsque Moins configuré est sélectionné, l'instance NetScaler qui a le moins de membres de pool configurés à ce moment-là est choisie comme périphérique pour le locataire.



6. Cliquez sur **Continuer**.
7. Dans la section **Attribuer des périphériques**, ajoutez les périphériques NetScaler disponibles à la liste des périphériques configurés.



8. Cliquez sur **Continuer**.
9. Dans la section **Attribuer des stratégies de placement/locataires OpenStack**, ajoutez la stratégie de placement que vous avez créée précédemment.



REMARQUE

Si la stratégie n'est pas trouvée, le mécanisme de secours est réactivé et NetScaler Console attribue les instances NetScaler en fonction des locataires. Si le locataire ne fait partie d'aucun package de services, NetScaler Console affiche un message d'erreur indiquant :

"Le locataire `admin` ne fait partie d'aucun package de services et il n'y a pas de package de services par défaut".

10. Cliquez sur **Continuer**, puis sur **Terminé**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NSX Manager : provisionnement manuel des instances NetScaler

NetScaler Console s'intègre à la plateforme de virtualisation de réseau VMware pour automatiser le déploiement, la configuration et la gestion des services NetScaler. Cette intégration élimine les complexités traditionnelles associées à la topologie de réseau physique, permettant aux administrateurs vSphere/vCenter de déployer les services NetScaler plus rapidement et de manière programmatique.

Cet article vous fournit une liste de tâches que vous devez effectuer à la fois sur VMware NSX Manager et sur NetScaler Console.

REMARQUE

Assurez-vous que VMware NSX pour vSphere 6.2 et versions ultérieures est installé et configuré, et que les passerelles de périphérie, le DLR et les machines virtuelles qui doivent être équilibrées en charge sont déjà créés.

Prérequis

- Installez VMware ESXi version 4.1 ou ultérieure avec un matériel qui répond aux exigences minimales.
- Installez VMware Client sur un poste de travail de gestion qui répond aux exigences minimales du système.
- Installez VMware OVF Tool (requis pour VMware ESXi version 4.1) sur un poste de travail de gestion qui répond aux exigences minimales du système.
- Installez NetScaler Console sur l'un des hyperviseurs pris en charge.

  Pour les tâches d'installation de NetScaler Console build 13.1, sur l'un des hyperviseurs pris en charge, consultez Déploiement de NetScaler Console.

Exigences matérielles de VMware ESXi

Le tableau suivant répertorie les ressources de calcul virtuelles dont vous avez besoin sur votre serveur VMware ESXi pour installer une appliance virtuelle NetScaler Console.

Composant	Exigence
RAM	8 Go

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Processeur virtuel	8
Espace de stockage	500 Go
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

REMARQUE

Les exigences en matière de mémoire et de disque dur spécifiées ci-dessus concernent le déploiement de NetScaler Console sur un serveur VMware ESXi, en considérant qu'aucune autre machine virtuelle n'est exécutée sur l'hôte. Les exigences matérielles pour le serveur VMware ESXi dépendent du nombre de machines virtuelles qui y sont exécutées.

Configuration de VMware NSX

- Créez un pool d'instances NetScaler VPX de différentes capacités, qui sont ajoutées aux différents packages de services.

Par exemple :

- Créez cinq instances NetScaler VPX de VPX1000 (1 Gbit/s). Ces instances sont ajoutées au package de services Gold.
- Créez cinq instances NetScaler VPX de VPX10 (10 Mbit/s). Ces instances sont ajoutées au package de services Bronze.

1. Dans le client vSphere, accédez à **Mise en réseau** et créez un groupe de ports de type trunking VLAN avec une plage, par exemple, 101-105 (vous pouvez même fournir la plage complète, mais créez un groupe de ports de type VLAN uniquement pour les VLAN requis).

   

2. Créez une nouvelle interface pour chaque instance NetScaler VPX et attachez-la au groupe de ports trunk de la plage VLAN qui a été créé ci-dessus.

   

3. Dans le client vSphere, accédez à **Mise en réseau** et créez un groupe de ports de type VLAN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Par exemple, si le groupe de ports trunk initial a été créé avec la plage 101-105, créez cinq groupes de ports VLAN, un par VLAN, c'est-à-dire un groupe de ports avec le VLAN 101, un autre avec le VLAN 102, et ainsi de suite, jusqu'au VLAN 105.



Ajout d'une instance NetScaler VPX dans NetScaler Console

Ajoutez des instances NetScaler VPX dans NetScaler Console et spécifiez la plage VLAN du groupe trunk pour chaque appareil.

1. Dans NetScaler Console, accédez à **Infrastructure** \> **Instances** \> **NetScaler VPX**, puis cliquez sur **Ajouter**.
2. Sur la page **Ajouter NetScaler VPX**, spécifiez soit les noms d'hôte des instances, l'adresse IP de chaque instance, ou une plage d'adresses IP, puis sélectionnez un profil d'instance dans la liste **Nom du profil**. Vous pouvez également créer un nouveau profil d'instance en cliquant sur l'icône +.
3. Cliquez sur **OK**.
4. Sélectionnez l'instance NetScaler VPX nouvellement ajoutée dans la liste de la page **NetScaler VPX**, puis cliquez sur le bouton flèche vers le bas dans le champ **Action**. Sélectionnez **Configurer les interfaces pour l'orchestration**.



5. Sur la page **Interfaces**, sélectionnez l'interface de gestion, et cliquez sur **Désactiver** pour empêcher le VLAN de se lier à l'interface de gestion.



6. Sur la page **Interfaces**, sélectionnez l'interface requise, et cliquez sur **Configurer la plage de VLAN**.
7. Saisissez la plage de VLAN configurée dans NSX Manager, cliquez sur **OK**, puis cliquez sur **Fermer**.



Enregistrement de VMware NSX Manager auprès de NetScaler Console

Enregistrez VMware NSX Manager auprès de NetScaler Console pour créer un canal de communication entre eux.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **VMware NSX Manager** dans la liste déroulante, et cliquez sur **Configurer les paramètres de NSX Manager**.
2. Sur la page **Configurer les paramètres de NSX Manager**, définissez les paramètres suivants :

   a. Adresse IP de NSX Manager - Adresse IP de NSX Manager.

   b. Nom d'utilisateur de NSX Manager - Nom d'utilisateur administratif de NSX Manager.

   c. Mot de passe - Mot de passe de l'utilisateur administratif de NSX Manager.

3. Dans la section **Compte NetScaler Console utilisé par NSX Manager**, définissez le nom d'utilisateur et le mot de passe du pilote NetScaler pour NSX Manager. NetScaler Console authentifie les requêtes de configuration de l'équilibreur de charge provenant de NSX Manager à l'aide de ces informations d'identification.
4. Cliquez sur **OK**.
5. Accédez à **Orchestration** \> **Système** \> **Paramètres de déploiement**. Fournissez la plage VLAN qui a été configurée dans le groupe de ports agrégés.

   

6. Connectez-vous à NSX Manager sur vSphere Web Client, et accédez à **Définitions de service** \> **Gestionnaires de service**.

   Vous pouvez voir Citrix NetScaler Console comme l'un des gestionnaires de service. Cela indique que l'enregistrement est réussi et qu'un canal de communication est établi entre le gestionnaire NSX et NetScaler Console.

   

Création d'un package de service dans NetScaler Console

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **VMware NSX Manager** \> **Packages de service**, et cliquez sur **Ajouter** pour ajouter un nouveau package de service.
2. Sur la page **Package de service**, dans la section **Paramètres de base**, définissez les paramètres suivants :

   a. Nom – saisissez le nom d'un package de service

   b. Stratégie d'isolation – par défaut, la stratégie d'isolation est définie sur Dédié

   c. Type de périphérique – par défaut, le type de périphérique est défini sur NetScaler VPX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Ces valeurs sont définies par défaut dans cette version, et vous ne pouvez pas les modifier.

d. Cliquez sur **Continuer**.



3. Dans la section **Attribuer des périphériques**, sélectionnez le VPX pré-provisionné pour ce package, puis cliquez sur **Continuer**.
4. Dans la section **Publier le package de services**, cliquez sur **Continuer** pour publier le package de services sur VMware NSX, puis cliquez sur **Terminé**.



Cette procédure configure un package de services dans le NSX Manager. Un service peut avoir plusieurs périphériques qui lui sont ajoutés et plusieurs périphériques Edge peuvent utiliser le même package de services pour décharger l'instance NetScaler VPX vers NetScaler Console.

5. Connectez-vous au NSX Manager sur vSphere Web Client, et accédez à **Définitions de services** \> **Services**.

   Vous pouvez voir que le package de services NetScaler Console est enregistré.



Exécution de l'insertion de service d'équilibrage de charge pour Edge

Effectuez l'insertion de service d'équilibrage de charge sur la passerelle NSX Edge précédemment créée (déchargez la fonction d'équilibrage de charge de NSX LB vers NetScaler).

1. Dans NSX Manager, accédez à **Accueil** \> **NSX Edges**, et sélectionnez la passerelle Edge que vous avez configurée.



2. Cliquez sur **Gérer**, et sous l'onglet **Équilibrage de charge**, sélectionnez **Configuration globale**, puis cliquez sur **Modifier**.



3. Sélectionnez **Activer l'équilibrage de charge**, **Journalisation**, **Activer l'insertion de service** pour les activer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Dans **Définition du service,** sélectionnez le package de service qui a été créé dans NetScaler Console et publié sur NSX Manager.



4. Sélectionnez les cartes réseau d'exécution existantes et cliquez sur l'icône Modifier pour modifier les cartes réseau d'exécution qui doivent être connectées lorsque NetScaler VPX est alloué.



5. Modifiez le nom de la carte réseau, spécifiez le type de connectivité comme **Données**, et cliquez sur **Modifier**.



6. Sélectionnez le commutateur logique web approprié.



7. Dans **Mode d'allocation IP principal**, sélectionnez Pool d'adresses IP dans la liste déroulante, et cliquez sur le bouton flèche vers le bas dans le champ Pool d'adresses IP.



8. Dans la fenêtre **Sélectionner le pool d'adresses IP**, sélectionnez le pool d'adresses IP approprié, et cliquez sur **OK**.



L'adresse IP est acquise et est définie comme adresse IP source du réseau dans l'appliance NetScaler VPX. Une passerelle L2 est créée dans NSX Manager pour mapper le VXLAN au VLAN.

REMARQUE

Toutes les interfaces de données sont connectées en tant que cartes réseau d'exécution, et elles font partie des interfaces pour DLR.

9. Actualisez la vue pour voir la création de l'exécution.



10. Une fois la VM démarrée, la valeur de Statut passe à **En service** et celle de l'état d'installation passe à **Activé**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Dans NetScaler Console, accédez à **Orchestration** \> **Requests** pour afficher les détails de progression de l'insertion du service d'équilibrage de charge.

Affichage de la passerelle L2 sur NSX Manager

1. Connectez-vous à NSX Manager sur vSphere Web Client, accédez à **NSX Edges**, et sélectionnez le DLR créé.

   

2. Dans la page DLR, accédez à **Manage** \> **Bridging**. Vous pouvez voir la passerelle L2 affichée dans la liste.

   

   REMARQUE

   Une passerelle L2 est créée pour chaque interface de données.

Affichage du NetScaler alloué

1. Connectez-vous à l'instance NetScaler VPX à l'aide de l'adresse IP affichée dans NetScaler Console. Ensuite, accédez à **Configuration** \> **Système** \> **Mise en réseau**. Dans le volet de droite, vous pouvez voir que les deux adresses IP sont ajoutées. Cliquez sur l'hyperlien de l'adresse IP pour afficher les détails.

   

   L'adresse IP du sous-réseau est la même que l'adresse IP de l'interface web ajoutée dans le NSX.

   

2. Accédez à **Configuration** \> **Système** \> **Licences** pour afficher les licences appliquées à cette instance.

Configuration de l'instance NetScaler VPX à l'aide de StyleBook

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **Configurer NSX Manager** \> **Passerelles Edge**.

   Notez l'adresse IP de l'instance NetScaler qui est attribuée à la passerelle Edge respective sur laquelle la configuration d'équilibrage de charge via StyleBooks doit être appliquée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Créez un nouveau StyleBook. Accédez à **Applications** \> **Configuration**, importez le StyleBook et sélectionnez le StyleBook dans la liste.

   Pour créer un nouveau StyleBook, consultez Créez votre propre StyleBook.

3. Spécifiez les valeurs pour tous les paramètres requis.

   

4. Spécifiez l'instance NetScaler VPX sur laquelle vous souhaitez exécuter ces paramètres de configuration.

   

5. Sélectionnez l'instance IP notée précédemment, puis cliquez sur **Sélectionner**.

   

6. Cliquez sur **Créer** pour appliquer la configuration sur l'appareil sélectionné.

   

Affichage de la configuration de l'équilibreur de charge

1. Connectez-vous à l'instance NetScaler VPX, accédez à **Configuration** \> **Gestion du trafic** \> **Équilibrage de charge** pour afficher le serveur virtuel d'équilibrage de charge qui est créé.

   

   Vous pouvez également afficher les groupes de services qui sont créés.

   

2. Sélectionnez le groupe de services, puis cliquez sur **Gérer les membres**. La page **Configurer le membre du groupe de services** affiche les membres associés au groupe de services.

   

Suppression du service d'équilibrage de charge

1. Dans NetScaler Console, accédez à **Applications** \> **Configuration**, puis cliquez sur l'icône **X** pour supprimer la configuration de l'application.
2. Connectez-vous à NSX Manager sur vSphere Web Client et accédez à la passerelle Edge à laquelle l'instance NetScaler VPX est connectée.
3. Accédez à **Gérer** \> **Équilibreur de charge** \> **Configuration globale**, cliquez avec le bouton droit sur l'entrée d'exécution, puis cliquez sur **Déprovisionner**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Les passerelles Edge dans NetScaler Console correspondent aux entrées d'exécution dans le gestionnaire NSX.

- [ ] L'instance NetScaler VPX est mise hors service.

4. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **Configurer le gestionnaire NSX** \> **Passerelles Edge**. Vérifiez que le mappage respectif de la passerelle Edge à l'instance supprimée n'est pas présent.

NSX Manager : approvisionnement automatique des instances NetScaler

Présentation

NetScaler Console s'intègre à la plateforme de virtualisation de réseau VMware pour automatiser le déploiement, la configuration et la gestion des services NetScaler. Cette intégration élimine les complexités traditionnelles associées à la topologie de réseau physique, permettant aux administrateurs vSphere/vCenter de déployer les services NetScaler par programmation plus rapidement.

Lors de l'insertion et de la suppression de services d'équilibrage de charge sur VMware NSX Manager, NetScaler Console provisionne et détruit dynamiquement les instances NetScaler. Cet approvisionnement dynamique nécessite que les attributions de licences NetScaler VPX soient automatisées dans NetScaler Console. Lorsque les licences NetScaler sont téléchargées vers NetScaler Console, NetScaler Console joue le rôle de serveur de licences.

Prérequis

REMARQUE

Cette intégration est prise en charge uniquement pour **VMware NSX for vSphere 6.1 ou version antérieure**.

- NetScaler Console, version 13.0 configuré en haute disponibilité et installé sur ESX.
- NetScaler VPX, v. 13.0
- Licences NetScaler VPX pour les instances NetScaler VPX, version 13.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Installez VMware ESXi version 4.1 ou ultérieure avec un matériel qui répond aux exigences minimales.
- Installez VMware Client sur un poste de travail de gestion qui répond aux exigences minimales du système.
- Installez VMware OVF Tool (requis pour VMware ESXi version 4.1) sur un poste de travail de gestion qui répond aux exigences minimales du système.

Déploiement en haute disponibilité de NetScaler Console et des instances NetScaler

Pour provisionner la configuration HA de NetScaler Console, installez le fichier image NetScaler Console que vous avez téléchargé depuis le site NetScaler. Pour plus d'informations sur la façon de provisionner la configuration HA de NetScaler Console, consultez Déploiement de NetScaler Console en haute disponibilité.

Configuration des détails du point de terminaison HA de NetScaler Console

Pour intégrer VMware NSX Manager à NetScaler Console déployé en mode HA, vous devez d'abord saisir l'adresse IP virtuelle de l'instance NetScaler d'équilibrage de charge. Vous devez également télécharger le fichier de certificat présent sur le serveur virtuel d'équilibrage de charge NetScaler vers le système de fichiers de NetScaler Console.

Pour fournir les informations de configuration d'équilibrage de charge dans NetScaler Console :

1. Dans le nœud HA de NetScaler Console, accédez à **Système** \> **Déploiement**.
2. Cliquez sur **Paramètres HA** dans le coin supérieur droit, et sur la page **Paramètres MAS-HA**, cliquez sur **Détails du point de terminaison MAS-HA**.

   
3. Sur la page **Détails du point de terminaison MAS-HA**, téléchargez le même certificat que celui déjà présent sur l'instance NetScaler d'équilibrage de charge.
4. Saisissez l'adresse IP virtuelle de l'instance NetScaler d'équilibrage de charge et cliquez sur **OK**.

   

Enregistrement de VMware NSX Manager auprès de NetScaler Console

Lorsque vous configurez deux serveurs NetScaler Console en haute disponibilité, les deux nœuds de serveur sont en mode actif-passif. Connectez-vous au nœud de serveur NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

principal pour enregistrer VMware NSX Manager auprès de NetScaler Console en mode HA, afin de créer un canal de communication entre eux.

Pour enregistrer VMware NSX Manager auprès de NetScaler Console en mode HA :

1. Dans le nœud de serveur NetScaler Console principal, accédez à **Orchestration** \> **Orchestration SDN** \> **VMware NSX Manager**.
2. Cliquez sur **Configurer les paramètres de NSX Manager**.
3. Sur la page **Configurer les paramètres de NSX Manager**, définissez les paramètres suivants :
    a. Adresse IP de NSX Manager - Adresse IP de NSX Manager.
    b. Nom d'utilisateur de NSX Manager - Nom d'utilisateur administratif de NSX Manager.
    c. Mot de passe - Mot de passe de l'utilisateur administratif de NSX Manager.
4. Dans la section Compte NetScaler Console utilisé par NSX Manager, définissez le mot de passe du pilote NetScaler pour NSX Manager.
5. Cliquez sur **OK**.

Chargement des licences dans NetScaler Console

Chargez les licences NetScaler VPX vers NetScaler Console, afin que NetScaler Console puisse allouer automatiquement des licences aux instances lors de l'orchestration avec NSX.

Pour installer les fichiers de licence sur NetScaler Console :

1. Dans NetScaler Console, accédez à **Infrastructure > Pooled Licensing**.
2. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :
    a. **Charger les fichiers de licence depuis un ordinateur local** - Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le charger sur NetScaler Console. Pour ajouter des fichiers de licence, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.
    b. **Utiliser le code d'accès à la licence** - Citrix envoie par e-mail le code d'accès à la licence pour les licences que vous achetez. Pour ajouter des fichiers de licence, saisissez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir les licences**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

À tout moment, vous pouvez ajouter d'autres licences à NetScaler Console à partir des paramètres de licence.

Téléchargement des images NetScaler VPX dans NetScaler Console

Ajoutez les images NetScaler à NetScaler Console, afin que NetScaler Console utilise ces images telles que définies dans le package de services.

Pour télécharger des images NetScaler VPX dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **VMware NSX Manager** \> **Images ESX NSVPX**.
2. Cliquez sur **Télécharger**, puis sélectionnez le package zip NetScaler VPX dans le dossier de stockage local.

Création de packages de services dans NetScaler Console

Créez des packages de services dans NetScaler Console pour définir l'ensemble des SLA, qui indiquent comment les ressources NetScaler sont allouées.

Pour créer des packages de services dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **VMware NSX Manager** \> **Packages de services**, puis cliquez sur **Ajouter** pour ajouter un nouveau package de services.
2. Sur la page **Package de services**, dans la section **Paramètres de base**, définissez les paramètres suivants :
    a. Nom - nom d'un package de services
    b. Stratégie d'isolation - sélectionnez **Dédié**
    c. Provisionnement d'instances NetScaler - sélectionnez **Créer une instance à la demande**
    d. Plateforme de provisionnement automatique - sélectionnez **CitrixNetScaler SDX**
    e. Cliquez sur **Continuer**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Dans la section **Paramètres de provisionnement automatique**, sélectionnez le package zip NetScaler VPX récemment téléchargé pour le déployer sur la plateforme NSX, sélectionnez la licence correspondante, puis cliquez sur **Continuer**.

   REMARQUE

   Dans la section **Haute disponibilité**, cochez la case pour provisionner les instances NetScaler pour la HA.

   Paramètres de provisionnement automatique(/en-us/netscaler-application-delivery-management-software/media/nsx-autoprovisioning-mas-ha-service-package.jpg)

   REMARQUE

   Le nom de la licence affiché dans la zone de liste déroulante illustrée dans la figure ci-dessus, VPX8000_Advanced, 2 numéros, est un exemple et est expliqué ci-dessous :

   - VPX - la licence sert à déployer des instances NetScaler VPX
   - 8000 - la bande passante consommable est de 8 Go
   - Advanced - NetScaler® propose trois types de licences : Standard, Advanced et Premium
   - 2 numéros - deux instances NetScaler VPX peuvent être déployées à l'aide de cette licence

   Le nom de la licence affiché dans la zone de liste **Licence** dépend de la licence que vous avez achetée auprès de Citrix.

4. Cliquez sur **Continuer**.
5. Le package de service est publié sur NSX Manager. Dans NSX Manager, accédez à **Définitions de service** \> **Gestionnaires de service**. Vous pouvez voir NetScaler Console comme l'un des gestionnaires de service. Cela indique que l'enregistrement est réussi et qu'une communication bidirectionnelle est établie entre le gestionnaire NSX et NetScaler Console.

   REMARQUE

   Pour NetScaler Console dans un déploiement à haute disponibilité, les licences sont téléchargées uniquement sur le nœud du serveur de licences NetScaler Console. Les nœuds NetScaler Console sont en mode actif-passif.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Effectuer l'insertion de service d'équilibrage de charge pour Edge

Effectuez l'insertion du service d'équilibrage de charge sur la passerelle NSX Edge existante, c'est-à-dire déchargez la fonction d'équilibrage de charge de l'équilibreur de charge NSX vers NetScaler.

Pour insérer le service d'équilibrage de charge sur la passerelle NSX Edge :

1. Dans NSX Manager, accédez à **Accueil** \> **Mise en réseau et sécurité** \> **NSX Edges**, puis double-cliquez pour sélectionner la passerelle Edge que vous avez configurée.
2. Cliquez sur **Gérer**, puis dans l'onglet **Équilibreur de charge**, sélectionnez **Configuration globale**, et cliquez sur **Modifier**.
3. Sélectionnez **Activer l'équilibreur de charge** et **Activer l'insertion de service** pour les activer.
4. Dans **Définition du service**, sélectionnez le package de service qui a été publié sur NSX Manager.
5. Configurez une carte réseau virtuelle pour l'interface de gestion, et une ou plusieurs cartes réseau virtuelles pour les interfaces de données. Sélectionnez les réseaux pour la gestion et les données en conséquence.

   REMARQUE

   Sélectionnez l'option Pool d'adresses IP en mode d'allocation d'adresses IP primaire. NetScaler Console ne prend pas en charge l'allocation manuelle ou DHCP d'adresses IP.

6. Cliquez sur l'icône d'actualisation pour voir la création de l'exécution.

   REMARQUE

   Étant donné que vous déployez deux instances NetScaler VPX dans un déploiement HA, deux exécutions sont créées dans le gestionnaire NSX.

   Vous devrez peut-être actualiser l'écran pour afficher les exécutions affichées à l'écran.
7. Sélectionnez l'exécution, cliquez sur **Actions**, et sélectionnez **Installer** dans le menu contextuel. Pour HA, répétez cette opération pour l'autre exécution également.
8. Lorsque les deux machines virtuelles démarrent, la valeur de Statut passe à "En service" et celle de l'état d'installation passe à "Activé".

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous devrez peut-être actualiser l'écran pour afficher le changement de statut.

9. Dans NetScaler Console, accédez à **Orchestration** \> **Requêtes** pour afficher les détails de progression de l'achèvement de l'insertion de service. Vous pouvez voir qu'une requête de création et de mise à jour de l'environnement d'exécution a été reçue dans NetScaler Console. Lorsque l'environnement d'exécution a été mis à jour, sélectionnez la requête et cliquez sur le bouton **Tâches** pour vérifier que NetScaler Console a été ajouté dans NSX Manager.

   Pour la HA, il y aura deux requêtes pour créer et mettre à jour deux environnements d'exécution dans NetScaler Console. Lorsque les deux environnements d'exécution ont été mis à jour, sélectionnez les deux requêtes et cliquez sur le bouton **Tâches** pour vérifier que deux nœuds HA de NetScaler Console ont été ajoutés dans NSX Manager.

10. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration SDN** \> **VMware NSX Manager** \> **Passerelles Edge**. Dans le panneau de droite, vous pouvez voir que le NetScaler VPX a été ajouté à la passerelle NSX Edge.

    Pour la HA, vous pouvez voir que deux instances NetScaler VPX en mode HA ont été ajoutées à la passerelle NSX Edge.

11. Dans NetScaler Console, accédez à **Infrastructure > Licences en pool > Licences VPX**. Sélectionnez la licence NetScaler VPX et l'édition que vous avez installée.

    Les instances NetScaler VPX qui sont en mode HA consomment deux licences et le statut est affiché sur votre écran comme suit.

    

    Une fois l'insertion de service terminée, vous pouvez utiliser les StyleBooks pour configurer les instances NetScaler selon l'une des deux méthodes suivantes :

    - Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de VMware NSX Manager
    - Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de NetScaler Console

Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de VMware NSX Manager

Effectuez la tâche suivante pour activer la configuration des services d'équilibrage de charge sur le périphérique de passerelle NSX Edge à l'aide des StyleBooks intégrés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans NSX Manager, accédez à **Accueil** \> **Mise en réseau et sécurité** \> **NSX Edges**, puis double-cliquez pour sélectionner la passerelle Edge que vous avez configurée.

Création de pools et de membres de pool

Créez un pool de serveurs et de membres de différentes capacités.

1. Cliquez sur **Gérer**, puis dans l'onglet **Équilibreur de charge**, sélectionnez **Pools**, et cliquez sur l'icône « **+** » pour ajouter un nouveau pool, et définissez les paramètres suivants :
    a. Nom - Nom du nouveau pool
    b. Algorithme - Sélectionnez un algorithme dans la liste déroulante en fonction duquel le pool sera sélectionné.
    c. Moniteurs - Assurez-vous que le moniteur de service est défini sur default_http_monitor
    d. Membres - Cliquez sur « + » pour ajouter des membres au pool et saisissez les paramètres requis dans la fenêtre Nouveau membre.
        i. Nom - Nom du membre
        ii. Adresse IP/Conteneur VC - Cliquez sur Sélectionner pour sélectionner l'objet dans la liste disponible ou saisissez l'adresse IP de l'objet.
2. Cliquez sur **OK**.

    Ajoutez autant de membres que nécessaire.

Création de serveurs virtuels

Créez un ensemble de serveurs virtuels et attribuez un pool à chaque serveur virtuel.

1. Cliquez sur **Gérer**, puis dans l'onglet Équilibreur de charge, sélectionnez **Serveurs virtuels**, et cliquez sur l'icône « **+** » pour ajouter un serveur virtuel, et définissez les paramètres suivants :
    a. Profil d'application - Par défaut, le profil de service que vous avez créé dans NetScaler Console s'affiche.
    b. Nom - Nom du serveur virtuel.
    c. Adresse IP - Cliquez sur Sélectionner pour sélectionner un pool d'adresses IP existant ou créer un nouveau pool d'adresses IP.
    d. Pool par défaut - Sélectionnez le pool par défaut dans la liste déroulante.
2. Cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Dans NetScaler Console, accédez à **Orchestration** \> **Requêtes** pour afficher les détails de progression de la création du service sur une ou plusieurs instances NetScaler sélectionnées.
4. Dans NetScaler Console, accédez à **Applications** \> **Configuration**, et vérifiez que le pack de configuration `nsx-lb-mon` a été créé.



Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de NetScaler Console

Déployez les configurations d'équilibreur de charge sur l'instance NetScaler à l'aide des StyleBooks de NetScaler Console. Pour la haute disponibilité (HA), la configuration est déployée sur les deux instances NetScaler qui sont en HA.

Pour créer des packs de configuration via StyleBooks :

1. Dans NetScaler Console, accédez à **Applications** \> **Configuration** \> **Créer nouveau**, et sélectionnez le **StyleBook HTTP/SSL LoadBalancing (avec moniteurs)** dans la liste. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous saisissez les valeurs de tous les paramètres définis dans ce StyleBook.
2. Spécifiez les valeurs de tous les paramètres requis.
3. Sélectionnez l'instance NetScaler VPX cible provisionnée dans l'environnement NSX, puis cliquez sur **Créer** pour appliquer la configuration sur l'appareil sélectionné. Pour un déploiement HA, sélectionnez les instances qui sont en mode HA.

Vérification de la création de serveurs virtuels et de groupes de services dans les instances NetScaler VPX

Vous pouvez vérifier que les groupes de services et les serveurs virtuels sont créés en vous connectant à l'instance NetScaler VPX.

Pour afficher les groupes de services et les serveurs virtuels :

1. Connectez-vous à l'instance NetScaler VPX. Pour un déploiement HA, vous devez vous connecter aux deux instances NetScaler qui sont en HA.
2. Accédez à **Configuration** \> **Système** \> **Mise en réseau**. Dans le volet droit, vous pouvez afficher les adresses IP qui ont été ajoutées. Cliquez sur le lien hypertexte de l'adresse IP pour voir les détails. Vous pouvez constater que l'adresse IP du sous-réseau est la même que l'adresse IP de l'interface web qui a été ajoutée dans NSX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Ensuite, accédez à **Gestion du trafic** \> **Équilibrage de charge** \> **Serveurs virtuels** et affichez les détails du serveur virtuel.
4. Ensuite, accédez à **Groupes de services** et affichez les détails du groupe de services.
5. Enfin, accédez à **Configuration** \> **Système** \> **Licences** pour afficher les licences appliquées à cette instance.

Suppression des services d'équilibrage de charge

Lorsque les services d'équilibrage de charge ne sont plus nécessaires sur les instances NetScaler VPX déployées sur le gestionnaire NSX, vous pouvez supprimer les insertions de service qui ont été effectuées précédemment.

Pour supprimer la configuration et l'insertion de service :

1. Dans NetScaler Console, accédez à **Applications** \> **Configuration**, sélectionnez la configuration d'application créée, puis supprimez la configuration en cliquant sur l'icône « X ».
2. Dans NSX Manager, accédez à la passerelle Edge à laquelle l'instance NetScaler VPX est connectée. Accédez à **Gérer** \> **Équilibreur de charge** \> G**lobal Configuration**, cliquez avec le bouton droit sur l'entrée d'exécution, puis cliquez sur **Déprovisionner**. La machine virtuelle est mise hors service.
3. Dans NetScaler Console, accédez à **Orchestration** \> **Orchestration cloud** \> **Passerelles Edge**. Assurez-vous qu'il n'y a pas de mappage respectif de la passerelle Edge à l'instance supprimée.

Gérer la configuration Ingress de Kubernetes dans NetScaler Console

Kubernetes (K8s) est une plateforme d'orchestration de conteneurs open source qui automatise le déploiement, la mise à l'échelle et la gestion des applications cloud natives.

Kubernetes fournit la fonctionnalité Ingress qui permet au trafic client externe au cluster d'accéder aux microservices d'une application exécutée à l'intérieur du cluster Kubernetes. Les instances NetScaler peuvent agir comme Ingress pour les applications exécutées à l'intérieur d'un cluster Kubernetes. Les instances NetScaler peuvent équilibrer la charge et acheminer le contenu du trafic Nord-Sud des clients vers n'importe quel microservice à l'intérieur du cluster Kubernetes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- NetScaler Console prend en charge la fonctionnalité Ingress sur les clusters avec la version 1.14 à 1.21 de Kubernetes.
- NetScaler Console prend en charge les appliances NetScaler VPX et MPX en tant que périphériques Ingress.
- Dans l'environnement Kubernetes, l'instance NetScaler équilibre la charge uniquement pour le type de service « NodePort ».

Vous pouvez configurer plusieurs instances NetScaler pour agir comme périphériques Ingress sur le même cluster ou sur différents clusters ou espaces de noms. Après avoir configuré les instances, vous pouvez attribuer chaque instance à différentes applications en fonction de la politique Ingress.

Vous pouvez créer et déployer une configuration Ingress à l'aide de Kubernetes `kubectl` ou d'API. Vous pouvez également configurer et déployer un Ingress depuis NetScaler Console.

Vous pouvez spécifier les aspects suivants de l'intégration de Kubernetes dans NetScaler Console :

- **Cluster** – Vous pouvez enregistrer ou désenregistrer des clusters Kubernetes pour lesquels NetScaler Console peut déployer des configurations Ingress. Lorsque vous enregistrez un cluster dans NetScaler Console, spécifiez les informations du serveur API Kubernetes. Ensuite, sélectionnez un agent capable d'atteindre le cluster Kubernetes et de déployer des configurations Ingress.
- **Stratégies** – Les stratégies Ingress sont utilisées pour sélectionner l'instance NetScaler en fonction du cluster ou de l'espace de noms afin de déployer une configuration Ingress. Spécifiez les informations de cluster, de site et d'instance lorsque vous ajoutez une stratégie.

Avant de commencer

Pour utiliser les instances NetScaler comme périphériques Ingress sur les clusters Kubernetes, assurez-vous de disposer des éléments suivants :

- Un cluster Kubernetes en place.
- Cluster Kubernetes enregistré dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer NetScaler Console avec un jeton secret pour gérer un cluster Kubernetes

Pour que NetScaler Console puisse recevoir des événements de Kubernetes, vous devez créer un compte de service dans Kubernetes pour NetScaler Console. Ensuite, configurez le compte de service avec les autorisations RBAC nécessaires dans le cluster.

1. Créez un compte de service pour NetScaler Console. Par exemple, le nom du compte de service peut être `citrixadm-sa`. Pour créer un compte de service, consultez Utiliser plusieurs comptes de service.
2. Utilisez le rôle `cluster-admin` pour lier le compte de service NetScaler Console. Cette liaison accorde un `ClusterRole` à travers le cluster à un compte de service. Voici un exemple de commande pour lier un rôle `cluster-admin` au compte de service.

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   Après avoir lié le compte de service NetScaler Console au rôle `cluster-admin`, le compte de service dispose d'un accès à l'échelle du cluster. Pour plus d'informations, consultez `kubectl` créer `clusterrolebinding`.
3. Obtenez le jeton du compte de service créé.

   Par exemple, exécutez la commande suivante pour afficher le jeton du compte de service `citrixadm-sa` :

   ```
   kubectl describe sa citrixadm-sa
   ```
4. Exécutez la commande suivante pour obtenir la chaîne secrète du jeton :

   ```
   kubectl describe secret <token-name>
   ```

Ajouter le cluster Kubernetes dans NetScaler Console

Après avoir configuré un agent NetScaler et configuré des routes statiques, vous devez enregistrer le cluster Kubernetes dans NetScaler Console.

Pour enregistrer le cluster Kubernetes :

1. Connectez-vous à NetScaler Console avec les informations d'identification de l'administrateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Accédez à **Orchestration** > **Kubernetes** > **Cluster**. La page Clusters s'affiche.
3. Cliquez sur **Ajouter**.
4. Dans la page **Ajouter un cluster**, spécifiez les paramètres suivants :
   a. **Nom** - Spécifiez un nom de votre choix.
   b. **URL du serveur API** - Vous pouvez obtenir les détails de l'URL du serveur API à partir du nœud principal Kubernetes.
      i. Sur le nœud principal Kubernetes, exécutez la commande `kubectl cluster-info`.

      

      ii. Saisissez l'URL qui s'affiche pour **« Kubernetes master est en cours d'exécution à. »**
   c. **Jeton d'authentification** - Spécifiez la chaîne du jeton d'authentification obtenue lorsque vous configurez NetScaler Console pour gérer un cluster Kubernetes. Le jeton d'authentification est requis pour valider l'accès à la communication entre le cluster Kubernetes et NetScaler Console. Pour générer un jeton d'authentification :
      i. Sur le nœud principal Kubernetes, exécutez les commandes suivantes :

      ```
      kubectl describe secret <token-name>
      ```

      ii. Copiez le jeton généré et collez-le comme jeton d'authentification.

      Pour plus d'informations, consultez la documentation Kubernetes.
   d. Sélectionnez l'agent dans la liste.
   e. Cliquez sur **Créer**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Paramètres

NetScaler Console fournit des paramètres qui vous aident à configurer et à intégrer votre déploiement pour répondre aux besoins de votre infrastructure. Les rubriques suivantes vous aident à configurer ces paramètres :

- Configurer IPAM
- Configurer les stratégies d'action
- Intégration de l'observabilité
- Configurer les listes de contrôle d'accès
- Utiliser les messages de journal de NetScaler Console pour gérer et surveiller votre infrastructure

Configurer la gestion des adresses IP (IPAM)

L'IPAM de NetScaler Console vous permet d'attribuer et de libérer automatiquement des adresses IP dans les configurations gérées par NetScaler Console. Vous pouvez attribuer des adresses IP à partir de réseaux ou de plages d'adresses IP définis à l'aide des fournisseurs d'adresses IP suivants :

- Fournisseur IPAM intégré à NetScaler Console.
- Solution IPAM Infoblox.

Vous pouvez utiliser l'IPAM de NetScaler Console dans :

- **StyleBooks** : attribuez automatiquement des adresses IP aux serveurs virtuels lorsque vous créez des configurations.
- **Passerelle API** : attribuez automatiquement une adresse IP au proxy API.

Vous pouvez également suivre les adresses IP de chaque réseau ou la plage d'adresses IP gérée par NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter un fournisseur d'adresses IP externe

NetScaler Console dispose d'un fournisseur IPAM intégré pour gérer les adresses IP et les plages d'adresses IP. Vous pouvez également utiliser un fournisseur d'adresses IP externe pour NetScaler Console.

IMPORTANT :

Avant de commencer, assurez-vous que les autorisations suivantes sont activées dans le fournisseur d'adresses IP externe :

- Possibilité d'interroger les réseaux présents dans le fournisseur.
- Réserver une adresse IP dans le réseau.
- Libérer une adresse IP du réseau.
- Récupérer les adresses IP utilisées d'un réseau.
- Récupérer les adresses IP disponibles d'un réseau.

Effectuez les étapes suivantes pour ajouter une solution de fournisseur IPAM externe dans NetScaler Console :

1. Accédez à **Paramètres > IPAM**.
2. Dans **Fournisseurs**, cliquez sur **Ajouter**.
3. Spécifiez les détails suivants pour ajouter un fournisseur IPAM :
   - **Nom** - Spécifiez le nom du fournisseur IP à utiliser dans NetScaler Console.
   - **Fournisseur** - Sélectionnez un fournisseur IPAM dans la liste.
   - **URL** - Spécifiez l'URL de la solution IPAM qui attribue des adresses IP dans un environnement NetScaler Console. Assurez-vous de spécifier l'URL au format suivant :

     ```
     https://<host name>
     ```

     Exemple : `https://myinfoblox.example.com`
   - **Est-ce un point de terminaison privé ?** - Si l'Infoblox DDI est hébergé en privé, cochez cette case, puis sélectionnez un agent.
   - **Nom d'utilisateur** - Spécifiez le nom d'utilisateur pour vous connecter à la solution IPAM.
   - **Mot de passe** - Spécifiez le mot de passe pour vous connecter à la solution IPAM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez sur **Ajouter**.

Infoblox DDI en tant que fournisseur externe

Actuellement, NetScaler® Console prend en charge Infoblox DDI en tant que fournisseur externe. L'Infoblox DDI peut être accessible publiquement ou hébergé en privé, accessible uniquement au sein du réseau interne d'une entreprise. Dans le cas d'un Infoblox DDI hébergé en privé, vous devez sélectionner un agent NetScaler pendant le processus de configuration. L'agent NetScaler agit comme un proxy pour accéder au fournisseur qui réside au sein de l'intranet de l'entreprise.

Vous pouvez utiliser l'IPAM de NetScaler Console avec le fournisseur Infoblox pour effectuer les actions suivantes :

- Lister les réseaux IPAM
- Créer, mettre à jour et supprimer des réseaux IPAM
- Réserver et libérer une adresse IP des réseaux IPAM

Créer un réseau IPAM

Pour créer un réseau IPAM NetScaler Console à l'aide du fournisseur Infoblox, un réseau avec la même plage d'adresses IP CIDR doit exister sur Infoblox.

Lorsque vous créez un réseau IPAM au sein de NetScaler Console, vous enregistrez uniquement l'utilisation du réseau Infoblox au sein de la Console. NetScaler Console collabore ensuite avec Infoblox pour gérer les adresses IP allouées à partir du réseau. Le réseau Infoblox peut continuer à être utilisé en dehors de NetScaler Console.

De même, si vous supprimez le réseau IPAM de NetScaler Console, NetScaler Console désenregistre le réseau Infoblox. Cela signifie que NetScaler Console n'interagit plus avec Infoblox pour la gestion des adresses IP dans ce réseau.

API Infoblox DDI

L'IPAM de NetScaler Console utilise les API Infoblox suivantes pour effectuer les actions respectives :

- (/network) - Liste tous les réseaux Infoblox disponibles
- (/network?network={id}) - Récupère les détails d'un réseau Infoblox spécifique
- (/ipv4address) - Liste toutes les adresses IP sur un réseau Infoblox
- (/record:host) - Récupère les détails d'une adresse IP spécifique
- (/{IP}) - Réserve et libère des adresses IP sur un réseau Infoblox

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations sur les API Infoblox, consultez le guide de référence de l'API REST Infoblox disponible sur Infoblox DDI.

Ajouter un réseau

Ajoutez un réseau pour utiliser l'IPAM avec les configurations gérées par NetScaler Console.

1. Accédez à **Paramètres > IPAM**.
2. Sous **Réseaux**, cliquez sur **Ajouter**.
3. Spécifiez les détails suivants :

   - **Nom du réseau** - Spécifiez le nom du réseau pour l'identifier dans NetScaler Console.
   - **Fournisseur** - Sélectionnez le fournisseur dans la liste.

     Cette liste affiche les fournisseurs ajoutés dans NetScaler Console.
   - **Type de réseau** - Sélectionnez **Plage d'adresses IP** ou **CIDR** dans la liste en fonction de vos besoins.
   - **Valeur du réseau** - Spécifiez la valeur du réseau.

     REMARQUE :

     L'IPAM de NetScaler Console ne prend en charge que les adresses IPv4.

     Pour la **plage d'adresses IP**, spécifiez la valeur du réseau au format suivant :

     ```
     <first-IP-address>-<last-IP-address>
     ```

     Exemple :

     ```
     10.0.0.20-10.0.0.100
     ```

     Pour **CIDR**, spécifiez la valeur du réseau au format suivant :

     ```
     <IP-address>/<subnet-mask>
     ```

     Exemple :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10.70.124.0/24
```

4. Cliquez sur **Créer**.

Afficher les adresses IP allouées

Pour afficher plus de détails sur les adresses IP allouées à partir du réseau IPAM, procédez comme suit :

1. Accédez à **Paramètres > IPAM**.
2. Sous l'onglet **Réseaux**, cliquez sur **Afficher toutes les adresses IP allouées**.

   Ce volet affiche l'adresse IP, le nom du fournisseur, le fournisseur et la description. Il affiche également les détails de la ressource qui a réservé cette adresse IP :

   - **Module** : Affiche le module NetScaler Console qui a réservé l'adresse IP. Par exemple, si StyleBooks a réservé l'adresse IP, cette colonne affiche StyleBooks comme module.
   - **Type de ressource** : Affiche le type de ressource dans ce module. Pour le module StyleBooks, seul le type de ressource de configurations utilise le réseau IPAM. Il affiche donc Configurations sous cette colonne.
   - **ID de ressource** : Affiche l'ID de ressource exact avec un lien. Cliquez sur ce lien pour accéder à la ressource qui utilise l'adresse IP. Pour le type de ressource de configuration, il affiche l'ID du pack de configuration comme ID de ressource.

REMARQUE :

Si vous souhaitez libérer l'adresse IP, sélectionnez l'adresse IP que vous souhaitez libérer et cliquez sur **Libérer les adresses IP allouées**.

Configurer une politique d'action pour recevoir des notifications d'événements d'application

Outre la vue analytique existante des événements d'application, vous pouvez configurer une politique d'action pour recevoir des notifications d'événements d'application via Slack, Email, PagerDuty ou ServiceNow. Les événements d'application incluent les problèmes de performance, les violations de bot et de WAF, ainsi que les violations de graphe de service. En tant

© 1997–2026 Citrix Systems, Inc. All rights reserved.

qu'administrateur, vous pouvez, grâce à la politique d'action, recevoir des notifications d'événements en temps réel.

À l'aide de la politique d'action, vous pouvez :

- Prédéfinir certaines conditions pour les événements d'application.
- Recevoir des notifications pour les événements suivants via Slack, Email, PagerDuty et ServiceNow :

CATÉGORIES D'ÉVÉNEMENTS	SOUS-CATÉGORIES D'ÉVÉNEMENTS	ÉVÉNEMENTS
Violations de sécurité	Toutes les violations de sécurité	Toutes les violations de bot (pour plus d'informations sur la liste des violations de bot, consultez catégories de violations).
		Toutes les violations WAF (violations SQL WAF, violations XSS WAF et violations XML WAF)
	Toutes les violations de sécurité par client	Violations de bot par client
		Violations WAF par client
		Remarque : Pour recevoir la notification de violation WAF, le nombre minimum de transactions de violation doit être de 20 %. Par exemple, sur 100 transactions, au moins 20 doivent être des transactions de violation.
Performances des applications		Violation du score d'application
		Latence du réseau client

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIES D'ÉVÉNEMENTS	SOUS-CATÉGORIES D'ÉVÉNEMENTS	ÉVÉNEMENTS
		Latence du réseau du serveur
		Temps de traitement du serveur
		Temps de réponse
		Requêtes
		Bande passante
		Violation du graphique de service
Utilisation de l'application		Requêtes par seconde
		Débit
		Volume de données

Configurer une stratégie d'action

1. Accédez à **Settings > Action > Action Policies**.
2. Cliquez sur **Add**.
3. Dans la page **Create Action Policy** :

    a. **Policy Name** – Indiquez un nom de stratégie de votre choix.

    b. **Enabled** – Cette option est sélectionnée par défaut.

    c. **If the Following Event Occurs** – Dans la liste, sélectionnez un événement.

    d. **And the Following Condition is Met** – Dans la liste, sélectionnez pour définir une condition pour laquelle vous souhaitez être averti. Vous pouvez cliquer sur **+** pour ajouter d'autres conditions. Pour supprimer une condition, cliquez sur **–**.

    Vous pouvez configurer la stratégie d'action à l'aide des opérateurs suivants. Les opérateurs apparaissent en fonction des conditions que vous sélectionnez.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPÉRATEUR	DESCRIPTION
Égal à	Égal à une valeur définie
Différent de	Différent d'une valeur définie
Supérieur à	Supérieur à une valeur définie
Supérieur ou égal à	Supérieur ou égal à une valeur définie
Inférieur à	Inférieur à une valeur définie
Inférieur ou égal à	Inférieur ou égal à une valeur définie
Contient	Contient le terme ou la valeur définie
Commence par	Commence par un terme ou une valeur définie
Se termine par	Se termine par un terme ou une valeur définie
DANS	Permet de sélectionner plusieurs valeurs

e. **Ensuite, effectuez les opérations suivantes** – Sélectionnez **Notifier**. Après avoir sélectionné **Notifier**, l'option Type de notification s'affiche.

f. **Type de notification** – Sélectionnez le type de notification Email, Slack, PagerDuty ou ServiceNow. Selon le type de notification que vous sélectionnez, l'option correspondante (liste de distribution, profil Slack, profil PagerDuty ou profil ServiceNow) apparaît. Sélectionnez un profil dans la liste.

   Si vous souhaitez créer un nouveau profil, cliquez sur **Ajouter**.

g. Cliquez sur **Créer une stratégie**.

   La stratégie est configurée. Vous pouvez afficher les détails de la stratégie configurée.

   Après avoir configuré la stratégie, vous pouvez sélectionner la stratégie et cliquer sur :

   - **Modifier** pour mettre à jour ou modifier la stratégie d'action. Après la mise à jour, cliquez sur Mettre à jour la stratégie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Supprimer** pour supprimer la stratégie d'action. Vous pouvez sélectionner plusieurs stratégies et cliquer sur **Supprimer** pour les supprimer.
- **Historique des actions** pour afficher des détails tels que l'heure, l'action effectuée, le nom de la stratégie, le type d'alerte et le message d'alerte.

Le tableau suivant décrit les détails de la configuration de la stratégie d'action.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
Toutes les violations de sécurité	Adresse IP de l'instance	Adresse IP de l'instance NetScaler. Sélectionnez l'adresse IP dans la liste.
	Nombre de violations	Le nombre de violations pour lequel vous souhaitez être averti. Par exemple, si vous configurez le nombre de violations comme étant inférieur ou égal à 10, vous serez averti si 10 transactions de violation de bot ou moins sont reçues.
	Ratio de violations	Cette valeur indique le nombre total de violations provenant de transactions spécifiques et la valeur doit être comprise entre 0 et 1. Par exemple, sur 100 transactions, 20 sont des violations et si vous souhaitez être averti pour un tel scénario, vous devez saisir 0,2.
Toutes les violations de bot	Profil de bot	Le nom du profil de bot utilisé pour configurer la gestion des bots sur l'instance NetScaler.
	Adresse IP de l'instance	Adresse IP de l'instance NetScaler. Sélectionnez l'adresse IP dans la liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
	Nombre de violations	Le nombre de violations pour lequel vous souhaitez être averti. Par exemple, si vous configurez le nombre de violations comme étant inférieur ou égal à 10, vous serez averti si 10 transactions de violation de bot ou moins sont reçues.
	Ratio de violations	Cette valeur indique le nombre total de violations provenant de transactions spécifiques et la valeur doit être comprise entre 0 et 1. Par exemple, sur 100 transactions, 20 sont des violations et si vous souhaitez être averti pour un tel scénario, vous devez saisir 0,2.
Toutes les violations WAF, violation SQL WAF, violation XSS WAF, violation XML inférée WAF	Profil WAF	Le nom du profil WAF utilisé pour configurer les paramètres de sécurité WAF sur l'instance NetScaler.
	Adresse IP de l'instance	Adresse IP de l'instance NetScaler. Sélectionnez l'adresse IP dans la liste.
	Nombre de violations	Le nombre de violations pour lesquelles vous souhaitez être averti. L'exigence minimale pour être averti des violations WAF est de 20 %.
	Ratio de violations	Cette valeur indique le nombre total de violations provenant de transactions spécifiques et la valeur doit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		être comprise entre 0 et 1. Par exemple, sur 100 transactions, 20 sont des transactions de violation SQL WAF et si vous souhaitez être averti pour un tel scénario, vous devez saisir 0,2.
Toutes les violations de sécurité par client	Nom de l'application	Le nom de l'application personnalisée. Sélectionnez l'application dans la liste. Si vous n'ajoutez pas cette condition, toutes les applications de l'instance NetScaler sont prises en compte.
	Adresse IP de l'instance	Adresse IP de l'instance NetScaler. Sélectionnez l'adresse IP dans la liste.
	Adresse IP du client	La source d'où provient le Bot. Spécifiez l'adresse IP.
	Nombre total d'attaques	Le nombre total d'attaques pour lesquelles vous souhaitez être averti.
	URL de la requête	L'URL que vous souhaitez configurer pour bloquer. Spécifiez l'URL.
	Nom du serveur virtuel	Les applications associées configurées pour les applications personnalisées. Sélectionnez l'application dans la liste. Si vous n'ajoutez pas cette condition, toutes les applications de l'instance NetScaler sont prises en compte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
Violations de bot par client	Nom de l'application	Le nom de l'application personnalisée. Sélectionnez l'application dans la liste. Si vous n'ajoutez pas cette condition, toutes les applications de l'instance NetScaler sont prises en compte.
	IP de l'instance	Adresse IP de l'instance NetScaler. Sélectionnez l'adresse IP dans la liste.
	IP du client	La source d'où provient le Bot. Spécifiez l'adresse IP.
	Nombre total d'attaques	Le nombre total d'attaques pour lesquelles vous souhaitez être averti.
	Type de violation	Sélectionnez la violation de bot dans la liste.
	URL de la requête	L'URL que vous souhaitez configurer pour bloquer. Spécifiez l'URL.
	Nom du Vserver	Les applications associées configurées pour les applications personnalisées. Sélectionnez l'application dans la liste. Si vous n'ajoutez pas cette condition, toutes les applications de l'instance NetScaler sont prises en compte.
Violations WAF par client	Nom de l'application	Le nom de l'application personnalisée. Sélectionnez l'application dans la liste. Si vous n'ajoutez pas cette

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		condition, toutes les applications de l'instance NetScaler sont prises en compte.
	IP de l'instance	Adresse IP de l'instance NetScaler. Sélectionnez l'adresse IP dans la liste.
	IP du client	La source d'où provient le bot. Spécifiez l'adresse IP.
	Nombre total d'attaques	Le nombre total d'attaques pour lesquelles vous souhaitez être averti.
	Type de violation	Sélectionnez la violation WAF dans la liste.
	URL de la requête	L'URL que vous souhaitez configurer pour bloquer. Spécifiez l'URL.
	Nom du serveur virtuel	Les applications associées configurées pour les applications personnalisées. Sélectionnez l'application dans la liste. Si vous n'ajoutez pas cette condition, toutes les applications de l'instance NetScaler sont prises en compte.
Violation du score d'application	Indicateur de performance	Les composants du score d'application et leurs valeurs seuils. Sélectionnez le composant du score d'application dans la liste. Pour plus d'informations, consultez Sélectionner les composants du score

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		d'application et définir les seuils.
	Nombre de violations	Le nombre de violations pour lesquelles vous souhaitez être averti. Par exemple, si vous configurez le nombre de violations égal à 5 pour le temps de réponse, vous serez averti lorsque le seuil de temps de réponse est dépassé 5 fois.
	Nom de l'application	Cliquez sur **Sélectionner les applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti de la violation.
Latence du réseau client	Latence moyenne du réseau client	Spécifiez la valeur de latence client (client vers NetScaler) en millisecondes pour laquelle vous souhaitez être averti.
	Anomalies de latence du réseau client	Spécifiez le nombre d'anomalies pour la latence du réseau pour lesquelles vous souhaitez être averti.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti de la violation.
Latence du réseau du serveur	Latence moyenne du réseau du serveur	Spécifiez la valeur de latence du serveur (serveur vers NetScaler) en millisecondes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		pour laquelle vous souhaitez être averti.
	Anomalies de latence du réseau du serveur	Spécifiez le nombre d'anomalies pour la latence du réseau pour lesquelles vous souhaitez être averti.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti de la violation.
Temps de réponse	Temps de réponse moyen	Spécifiez la valeur (en millisecondes) pour laquelle vous souhaitez être averti.
	Anomalies du temps de réponse moyen	Spécifiez le nombre d'anomalies pour lesquelles vous souhaitez être averti.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti. Si vous ne sélectionnez aucune application, la règle s'applique à toutes les applications.
Requêtes	Nombre total de requêtes	Spécifiez le nombre total de requêtes pour lesquelles vous souhaitez être averti.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti. Si vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		ne sélectionnez aucune application, la règle s'applique à toutes les applications.
Bande passante	Bande passante totale	Spécifiez la bande passante (Mo) pour laquelle vous souhaitez être averti.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti. Si vous ne sélectionnez aucune application, la règle s'applique à toutes les applications.
Temps de traitement du serveur	Temps moyen de traitement du serveur	Spécifiez la valeur de traitement du serveur (serveur vers NetScaler) en millisecondes pour laquelle vous souhaitez être averti.
	Anomalies du temps de traitement du serveur	Spécifiez le nombre d'anomalies pour le temps de traitement du serveur pour lequel vous souhaitez être averti.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti de la violation.
Violation du graphique de service		Microservices qui dépassent les seuils configurés. Pour plus d'informations, consultez

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		Configurer les seuils dans le graphique de service.
Requêtes par seconde	Moyenne des requêtes par seconde	Le nombre de requêtes reçues par l'application par seconde. Spécifiez la valeur moyenne pour être averti.
	Anomalies de la moyenne des requêtes par seconde	Spécifiez le nombre moyen d'anomalies pour lequel vous souhaitez être averti.
		Remarque : Si vous utilisez la condition ET pour cet événement, vous pouvez configurer soit la moyenne des requêtes par seconde et le nom de l'application, soit la moyenne des anomalies des requêtes par seconde et le nom de l'application.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti de la violation.
Débit	Débit moyen	Quantité totale de données transmises sur une période spécifique. Spécifiez la valeur moyenne (en Mo) pour être averti.
	Anomalies du débit moyen	Spécifiez le nombre moyen d'anomalies pour lequel vous souhaitez être averti.
		Remarque : Si vous utilisez la condition ET pour cet événement, vous pouvez

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NOM DE LA VIOLATION	CONDITION	DESCRIPTION
		configurer soit le débit moyen et le nom de l'application, soit l'anomalie du débit moyen et le nom de l'application.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être averti de la violation.
Volume de données	Volume total de données	Quantité totale de données à transférer sur une durée spécifique. Spécifiez la valeur (en Mo) pour être averti.
	Anomalies du volume de données	Spécifiez le nombre d'anomalies pour lequel vous souhaitez être averti.
		Remarque : Si vous utilisez la condition ET pour cet événement, vous pouvez configurer soit le volume total de données et le nom de l'application, soit les anomalies de volume de données et le nom de l'application.
	Nom de l'application	Cliquez sur **Sélectionner des applications** pour sélectionner les applications pour lesquelles vous souhaitez être informé de la violation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Utiliser la barre de recherche

La barre de recherche vous permet de filtrer les résultats. Lorsque vous cliquez sur la barre de recherche, elle vous propose une liste de suggestions de recherche. Vous pouvez sélectionner le composant et filtrer les résultats en fonction de vos besoins.



Utiliser l'option des journaux d'audit

Cliquez sur **Journaux d'audit** et sélectionnez la durée dans la liste pour afficher les stratégies d'action qui ont été créées, modifiées et supprimées pour la durée sélectionnée, puis cliquez sur **Rechercher**.

REMARQUE

Les stratégies de stockage de données devraient changer dans les prochaines versions. Avec ces changements, vous ne pourrez plus stocker de données historiques une fois qu'elles auront dépassé la limite de stockage. Pour l'instant, il est recommandé d'ajouter plus de stockage ou de maintenir le stockage dans les limites des droits de licence.

Intégration de l'observabilité

En raison de la complexité croissante des applications modernes, les administrateurs sont confrontés à des défis concernant :

- Surveiller et dépanner les applications.
- Obtenir une visibilité sur le comportement de l'infrastructure et des applications.

L'observabilité comble cette lacune en fournissant ces informations sur l'ensemble de l'infrastructure. Grâce à la fonctionnalité d'intégration de l'observabilité dans NetScaler Console, vous pouvez :

- Intégrer NetScaler Console à Splunk.
- Intégrer NetScaler Console à New Relic.
- Configurer les instances NetScaler pour l'exportation d'informations vers Prometheus à l'aide du schéma par défaut.

Intégration avec Splunk

Vous pouvez désormais intégrer NetScaler Console à Splunk pour afficher les analyses pour :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Violations WAF
- Violations de bot
- Informations sur les certificats SSL
- Informations sur la passerelle
- Événements et métriques
- Informations HDX™
- Journaux d'audit de NetScaler® Console

L'add-on Splunk vous permet de :

- Combiner toutes les autres sources de données externes.
- Offrir une meilleure visibilité des analyses dans un emplacement centralisé.

NetScaler Console collecte les événements de bot, WAF et SSL et les envoie périodiquement à Splunk. L'add-on Splunk Common Information Model (CIM) convertit les événements en données compatibles CIM. En tant qu'administrateur, en utilisant les données compatibles CIM, vous pouvez afficher les événements dans le tableau de bord Splunk.

Pour une intégration réussie, vous devez :

- Configurer Splunk pour recevoir des données de NetScaler Console
- Configurer NetScaler Console pour exporter des données vers Splunk
- Afficher les tableaux de bord dans Splunk

Configurer Splunk pour recevoir des données de NetScaler Console sur site

Dans Splunk, vous devez :

1. Configurer le point de terminaison du collecteur d'événements HTTP de Splunk et générer un jeton
2. Installer l'add-on Splunk Common Information Model (CIM)
3. Installer le normalisateur CIM (applicable uniquement pour les informations WAF et bot)
4. Préparer un exemple de tableau de bord dans Splunk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer le point de terminaison du collecteur d'événements HTTP de Splunk et générer un jeton

Vous devez d'abord configurer le collecteur d'événements HTTP dans Splunk. Cette configuration permet l'intégration entre NetScaler Console et Splunk pour l'envoi des données. Ensuite, vous devez générer un jeton dans Splunk pour :

- Activer l'authentification entre NetScaler Console et Splunk.
- Recevoir des données via le point de terminaison du collecteur d'événements.

1. Connectez-vous à Splunk.
2. Accédez à **Settings > Data Inputs > HTTP event collector** et cliquez sur **Add new**.
3. Spécifiez les paramètres suivants :

    a. **Nom** : Spécifiez un nom de votre choix.

    b. **Remplacement du nom de la source (facultatif)** : Si vous définissez une valeur, elle remplace la valeur de la source pour le collecteur d'événements HTTP.

    c. **Description (facultatif)** : Spécifiez une description.

    d. **Groupe de sortie (facultatif)** : Par défaut, cette option est sélectionnée comme Aucune.

    e. **Activer l'accusé de réception de l'indexeur** : NetScaler Console ne prend pas en charge cette option. Nous vous recommandons de ne pas la sélectionner.

    

4. Cliquez sur **Suivant**.
5. Vous pouvez éventuellement définir des paramètres d'entrée supplémentaires dans la page **Paramètres d'entrée**.
6. Cliquez sur **Vérifier** pour vérifier les entrées, puis cliquez sur **Soumettre**.

    Un jeton est généré. Vous devez utiliser ce jeton lorsque vous ajoutez des détails dans NetScaler Console.

    

Installer le modèle d'informations commun Splunk

Dans Splunk, vous devez installer l'add-on Splunk CIM. Cet add-on garantit que les données reçues de NetScaler Console normalisent les données ingérées et correspondent à une norme commune en utilisant les mêmes noms de champs et balises d'événements pour les événements équivalents.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous pouvez ignorer cette étape si vous avez déjà installé l'add-on Splunk CIM.

1. Connectez-vous à Splunk.
2. Accédez à **Applications > Rechercher plus d'applications**.



3. Tapez **CIM** dans la barre de recherche et appuyez sur **Entrée** pour obtenir l'add-on **Splunk Common Information Model (CIM)**, puis cliquez sur **Installer**.



Installer le normalisateur CIM

Le normalisateur CIM est un plug-in supplémentaire que vous devez installer pour afficher les informations WAF et bot dans Splunk.

1. Dans le portail Splunk, accédez à **Applications > Rechercher plus d'applications**.



2. Tapez **CIM normalization for NetScaler Console service events/data** dans la barre de recherche et appuyez sur **Entrée** pour obtenir l'add-on, puis cliquez sur **Installer**.



Préparer un tableau de bord d'exemple dans Splunk

Après avoir installé le CIM Splunk, vous devez préparer un tableau de bord d'exemple à l'aide d'un modèle pour les informations WAF et Bot, les informations sur les certificats SSL, ainsi que les événements et les métriques. Vous pouvez télécharger le fichier de modèle de tableau de bord (`.tgz`), utiliser n'importe quel éditeur (par exemple, le Bloc-notes) pour copier son contenu, et créer un tableau de bord en collant les données dans Splunk.

REMARQUE :

La procédure suivante pour créer un tableau de bord d'exemple est applicable à tous les cas d'utilisation. Vous devez utiliser le fichier `json` requis.

1. Connectez-vous à la page de téléchargements Citrix et téléchargez le tableau de bord d'exemple disponible sous Sample Dashboards for 3rd party Endpoints.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Extrayez le fichier, ouvrez le fichier `json` à l'aide de n'importe quel éditeur et copiez les données du fichier.

   Après l'extraction, vous obtenez trois fichiers `json`. Utilisez le :

   - fichier `adm_splunk_security_violations.json` pour créer un tableau de bord d'exemple WAF et Bot.
   - fichier `adm_splunk_ssl_certificate.json` pour créer un tableau de bord d'exemple d'aperçu des certificats SSL.
   - fichier `adm_splunk_events_and_metrics_history.json` pour créer un tableau de bord des événements et métriques de NetScaler Console.

3. Dans le portail Splunk, accédez à **Search & Reporting > Dashboards**, puis cliquez sur **Create New Dashboard**.

   

4. Dans la page **Create New Dashboard**, spécifiez les paramètres suivants :

   a. **Titre du tableau de bord** - Indiquez un titre de votre choix.

   b. **Description** - Vous pouvez éventuellement fournir une description pour votre référence.

   c. **Permission** - Sélectionnez **Private** ou **Shared in App** en fonction de vos besoins.

   d. Sélectionnez **Dashboard Studio**.

   e. Sélectionnez une disposition (**Absolute** ou **Grid**), puis cliquez sur **Create**.

      

      Après avoir cliqué sur **Créer**, sélectionnez l'icône **Source** dans la mise en page.

      

5. Supprimez les données existantes, collez les données que vous avez copiées à l'étape 2, puis cliquez sur **Retour**.

6. Cliquez sur **Enregistrer**.

   Vous pouvez afficher le tableau de bord d'exemple.

   Voici un exemple de tableau de bord pour WAF et bot.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer NetScaler Console sur site pour exporter des données vers Splunk

Tout est maintenant prêt dans Splunk. La dernière étape consiste à configurer NetScaler Console en créant un abonnement et en ajoutant le jeton.

Une fois la procédure suivante terminée, vous pouvez afficher le tableau de bord mis à jour dans Splunk, actuellement disponible dans votre NetScaler Console :

1. Connectez-vous à NetScaler Console.
2. Accédez à **Paramètres > Intégration de l'observabilité**.
3. Dans la page **Intégrations**, cliquez sur **Ajouter**.
4. Dans la page **Créer un abonnement**, spécifiez les détails suivants :
    a. Spécifiez un nom de votre choix dans le champ **Nom de l'abonnement**.
    b. Sélectionnez **NetScaler Console** comme **Source**, puis cliquez sur **Suivant**.
    c. Sélectionnez **Splunk**, puis cliquez sur **Configurer**. Dans la page **Configurer le point de terminaison** :
        i. **URL du point de terminaison** – Spécifiez les détails du point de terminaison Splunk. Le point de terminaison doit être au format `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>`.

            REMARQUE :

            Il est recommandé d'utiliser HTTPS pour des raisons de sécurité.

            - **SPLUNK_PUBLIC_IP** – Une adresse IP valide configurée pour Splunk.
            - **SPLUNK_HEC_PORT** – Indique le numéro de port que vous avez spécifié lors de la configuration du point de terminaison d'événement HTTP. Le numéro de port par défaut est 8088.
            - **Services/collector/event** – Indique le chemin d'accès de l'application HEC.

        ii. **Jeton d'authentification** – Copiez et collez le jeton d'authentification de Splunk.
        iii. Cliquez sur **Soumettre**.
    d. Cliquez sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. Cliquez sur **Ajouter des informations** et, dans l'onglet **Sélectionner la fonctionnalité**, vous pouvez sélectionner les fonctionnalités que vous souhaitez exporter, puis cliquez sur **Ajouter la sélection**.

> **REMARQUE :**
>
> Si vous avez sélectionné **Journaux d'audit de NetScaler Console**, vous pouvez sélectionner **Quotidien** ou **Horaire** pour la fréquence d'exportation des journaux d'audit vers Splunk.

f. Cliquez sur **Suivant**.

g. Dans l'onglet **Sélectionner l'instance**, vous pouvez choisir **Sélectionner toutes les instances** ou **Sélection personnalisée**, puis cliquez sur **Suivant**.

- **Sélectionner toutes les instances** - Exporte les données vers Splunk depuis toutes les instances NetScaler.
- **Sélection personnalisée** - Vous permet de sélectionner les instances NetScaler dans la liste. Si vous sélectionnez des instances spécifiques dans la liste, les données sont exportées vers Splunk uniquement à partir des instances NetScaler sélectionnées.

h. Cliquez sur **Soumettre**.

> **REMARQUE :**
>
> Les données des informations sélectionnées sont transmises à Splunk immédiatement après la détection des violations dans NetScaler Console.

Afficher les tableaux de bord dans Splunk

Une fois la configuration terminée dans NetScaler Console, les données sont exportées de NetScaler Console et les événements apparaissent dans Splunk.

Vous êtes prêt à afficher le tableau de bord mis à jour dans Splunk sans aucune étape supplémentaire.

Accédez à Splunk et cliquez sur le tableau de bord que vous avez créé pour afficher le tableau de bord mis à jour.

Voici un exemple de tableau de bord WAF et Bot mis à jour :



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le tableau de bord suivant est un exemple de tableau de bord des informations sur les certificats SSL mis à jour.

Le tableau de bord suivant est un exemple de tableau de bord des événements et métriques mis à jour.

REMARQUE :

Les données d'utilisation de la mémoire, du CPU et du disque affichent la valeur actuelle de la NetScaler Console. La tendance à la hausse et à la baisse de ces valeurs est affichée en fonction de la comparaison avec la valeur précédente toutes les 5 minutes.

Outre le tableau de bord, vous pouvez également afficher les données dans Splunk après avoir créé l'abonnement.

1. Dans Splunk, cliquez sur **Recherche et rapports**.
2. Dans la barre de recherche :
   - Tapez `sourcetype="metrics"` et sélectionnez la durée dans la liste pour afficher les données de métriques de NetScaler Console.
   - Tapez `sourcetype="event"` et sélectionnez la durée dans la liste pour afficher les données d'événements de NetScaler Console.
   - Tapez `sourcetype="bot"` ou `sourcetype="waf"` et sélectionnez la durée dans la liste pour afficher les données de bot/WAF.
   - Tapez `sourcetype="ssl"` et sélectionnez la durée dans la liste pour afficher les données d'informations sur les certificats SSL.
   - Tapez `sourcetype="gateway_insights"` et sélectionnez la durée dans la liste pour afficher les données d'informations sur la passerelle.
   - Tapez `sourcetype="hdx_insights"` et sélectionnez la durée dans la liste pour afficher les données d'informations sur la passerelle.
   - Tapez `sourcetype= "audit_logs"` et sélectionnez la durée dans la liste pour afficher les données des journaux d'audit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Intégration avec New Relic

Vous pouvez désormais intégrer NetScaler Console à New Relic pour afficher les analyses des journaux d'audit WAF, Bot, SSL, Gateway Insights et NetScaler Console dans votre tableau de bord New Relic. Grâce à cette intégration, vous pouvez :

- Combiner toutes les autres sources de données externes dans votre tableau de bord New Relic.
- Obtenir une visibilité des analyses dans un emplacement centralisé.

NetScaler Console collecte les événements Bot et WAF et les envoie à New Relic en temps réel ou périodiquement, selon votre choix. En tant qu'administrateur, vous pouvez également afficher les événements Bot et WAF dans votre tableau de bord New Relic.

Prérequis

Pour une intégration réussie, vous devez :

- Obtenir un point de terminaison d'événement New Relic au format suivant :

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  Pour plus d'informations sur la configuration d'un point de terminaison d'événement, consultez la documentation New Relic.

  Pour plus d'informations sur l'obtention d'un ID de compte, consultez la documentation New Relic.
- Obtenir une clé New Relic. Pour plus d'informations, consultez la documentation New Relic.
- Ajouter les détails de la clé dans NetScaler Console

Ajouter les détails de la clé dans NetScaler Console

Après avoir généré un jeton, vous devez ajouter des détails dans NetScaler Console pour l'intégrer à New Relic.

1. Connectez-vous à NetScaler Console.
2. Accédez à **Paramètres > Intégration de l'observabilité**.
3. Dans la page **Intégrations**, cliquez sur **Ajouter**.
4. Dans la page **Créer un abonnement**, spécifiez les détails suivants :
   a. Spécifiez un nom de votre choix dans le champ **Nom de l'abonnement**.
   b. Sélectionnez **NetScaler® Console** comme **Source** et cliquez sur **Suivant**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Sélectionnez **New Relic** et cliquez sur **Configurer**. Dans la page **Configurer le point de terminaison** :

   i. **URL du point de terminaison** – Spécifiez les détails du point de terminaison New Relic. Le point de terminaison doit être au format `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`.

> **REMARQUE**
>
> Il est recommandé d'utiliser HTTPS pour des raisons de sécurité.

d. **Jeton d'authentification** – Copiez et collez le jeton d'authentification de New Relic.

   i. Cliquez sur **Soumettre**.

e. Cliquez sur **Suivant**.

f. Cliquez sur **Ajouter des informations** et dans l'onglet **Sélectionner une fonctionnalité**, vous pouvez sélectionner les fonctionnalités que vous souhaitez exporter et cliquer sur **Ajouter la sélection**.

g. Cliquez sur **Suivant**.

h. Dans l'onglet **Sélectionner l'instance**, vous pouvez choisir **Sélectionner toutes les instances** ou **Sélection personnalisée**, puis cliquer sur **Suivant**.

   - **Sélectionner toutes les instances** - Exporte les données vers New Relic depuis toutes les instances NetScaler.
   - **Sélection personnalisée** - Vous permet de sélectionner les instances NetScaler dans la liste. Si vous sélectionnez des instances spécifiques dans la liste, les données sont exportées vers New Relic uniquement à partir des instances NetScaler sélectionnées.

i. Cliquez sur **Soumettre**.

> **REMARQUE :**
>
> Les données des informations sélectionnées sont transmises à New Relic immédiatement après la détection des violations dans NetScaler Console.

La configuration est terminée. Vous pouvez consulter les détails sur la page **Abonnements**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau de bord New Relic

Lorsque les événements sont exportés dans New Relic, vous pouvez afficher les détails de l'événement sous **Métriques et événements** au format JSON suivant :

`<subsription_name>_adm_<event name>` où le nom de l'événement peut être Bot, WAF, etc.

Dans l'exemple suivant, ADMSTAGING est le `<subscription_name>` et bot est le `<event_name>`.



Une fois que les données JSON sont ingérées dans votre tableau de bord New Relic, en tant qu'administrateur, vous pouvez utiliser le NRQL (New Relic Query Language) et créer un tableau de bord personnalisé avec des facettes et des widgets selon votre choix en construisant des requêtes autour des données ingérées. Pour plus d'informations, consultez `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`

Voici un exemple de tableau de bord créé à l'aide du NRQL :



Pour créer ce tableau de bord, les requêtes suivantes sont nécessaires :

- Widget 1 : Nombre total d'attaques uniques dans la table des événements

  `SELECT count(total_attacks) from <event_name> since 30 days ago`

- Widget 2 : Identifiants de transaction uniques dans la table des événements

  `SELECT uniqueCount(transaction_id) from <event_name> since 30 days ago`

- Widget 3 : Nombre total de types de bots uniques et leur nombre

  `SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago`

- Widget 4 : Nombre total de noms d'applications uniques subissant des violations de bot

  `SELECT uniques(appname) from <event_name> since 30 days ago`

Intégration avec Microsoft Sentinel

Vous pouvez intégrer NetScaler Console à Microsoft Sentinel pour exporter les analyses suivantes de NetScaler Console vers Microsoft Sentinel :

- Violations WAF

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Violations de bot
- Informations sur les certificats SSL
- Informations sur la passerelle
- Métriques et événements
- Journaux d'audit de NetScaler® Console

Microsoft Sentinel fournit une collecte de données centralisée qui rassemble des données provenant de diverses sources telles que des applications, des serveurs, etc. En tant qu'administrateur, vous pouvez consulter les données et prendre des décisions une fois que les informations ou les violations sont signalées dans Microsoft Sentinel.

Pour une intégration réussie, assurez-vous de disposer d'un abonnement Azure actif, puis suivez la procédure sous chaque section :

Configurer l'espace de travail Log Analytics

Un espace de travail Log Analytics est nécessaire pour stocker et analyser les données collectées.

1. Connectez-vous à Azure.
2. Cliquez sur **Créer une ressource**.

   
3. Dans la barre de recherche, tapez « espace de travail Log Analytics » et cliquez sur **Créer** sous **Espace de travail Log Analytics**.

   
4. Sur la page principale de l'**Espace de travail Log Analytics**, cliquez sur **Créer**.

   
5. Dans **Créer un espace de travail Log Analytics** :

   a. Sélectionnez l'abonnement actif et le groupe de ressources.

   REMARQUE :

   Vous pouvez également cliquer sur **Créer un nouveau** pour ajouter un groupe de ressources si vous disposez des privilèges nécessaires.

   b. Spécifiez un nom de votre choix.

   c. Sélectionnez votre région dans la liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Cliquez sur **Vérifier + Créer**.



e. Un message de validation réussie apparaît. Cliquez sur **Créer** pour déployer l'espace de travail.



f. Vous pouvez voir le message de déploiement en cours. Une fois le message de déploiement terminé affiché, cliquez sur **Accéder à la ressource**.



L'espace de travail est créé avec succès.

Créer une application Microsoft Entra

Vous devez créer une application Entra associée à votre abonnement Azure pour communiquer au nom de l'espace de travail Log Analytics. Après avoir créé l'application, vous devez également accorder l'autorisation avec le rôle **Contributeur Microsoft Sentinel**. L'application fournit également des détails tels que l'**ID client**, l'**ID de locataire** et le **Secret client**. Nous vous recommandons de noter ces détails. Ces détails sont requis lorsque vous créez un abonnement dans NetScaler Console pour terminer le processus d'intégration.

1. Dans votre portail Azure, tapez le mot-clé dans la barre de recherche.
2. Cliquez sur **Microsoft Entra ID**.



3. Cliquez sur **Ajouter** et sélectionnez **Enregistrement d'application**.



4. Spécifiez un nom pour l'application, sélectionnez l'option par défaut sous **Types de comptes pris en charge**, puis cliquez sur **Enregistrer**.



5. Après avoir enregistré l'application :

   a. Notez l'**ID client** et l'**ID de locataire**.



   b. Créez un ID secret pour votre application. Cliquez sur **Certificats et secrets** et sous **Secrets client**, cliquez sur **Nouveau secret client**. Fournissez une description, une validité, puis cliquez sur **Ajouter** pour créer un ID secret pour votre application.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Les détails sont affichés pour votre application. Assurez-vous de noter l'ID affiché sous **Valeur** immédiatement après la création du secret. Cette valeur est masquée si vous accédez à une autre option de l'interface graphique.



Envoyer des données à Microsoft Sentinel à l'aide du connecteur de données Microsoft Entra ID

Les journaux Microsoft Entra ID fournissent des informations complètes sur les utilisateurs, les applications et les réseaux accédant à votre locataire Entra. Pour plus d'informations, consultez Envoyer des données à Microsoft Sentinel à l'aide du connecteur de données Microsoft Entra ID.

Configurer le point de terminaison de collecte de données

Vous devez créer un point de terminaison de collecte de données pour obtenir l'URL du point de terminaison. Ceci est requis lorsque vous créez un abonnement dans NetScaler Console.

1. Dans votre portail Azure, sous **Services Azure**, sélectionnez **Points de terminaison de collecte de données** ou tapez le mot-clé dans la barre de recherche.



2. Cliquez sur **Créer** dans la page **Points de terminaison de collecte de données**.



3. Dans **Créer un point de terminaison de collecte de données** :

   a. Spécifiez un nom de point de terminaison de votre choix

   b. Sélectionnez l'**Abonnement, le Groupe de ressources** et la **Région**.

   c. Cliquez sur **Vérifier + créer**.

   d. Après avoir vu le message de validation réussie, cliquez sur **Créer**.

Vous devez noter l'URL du point de terminaison. Sur la page principale **Point de terminaison de collecte de données**, sélectionnez le point de terminaison créé, cliquez sur **Vue JSON** et notez l'ID du point de terminaison.

ID DCR(/en-us/netscaler-application-delivery-management-software/media/sentinel-dcr-id.png)

Créer des tables pour exporter des données

Vous devez créer une table et fournir les informations JSON pour chaque aperçu que vous souhaitez exporter de NetScaler Console vers Microsoft Sentinel. Vous pouvez vous référer aux détails suivants concernant les exigences de table pour chaque aperçu :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APERÇUS	NOMBRE TOTAL DE TABLES REQUISES
Aperçus SSL	3
WAF	1
Bot	1
Aperçus de passerelle	5
Événements	1
Métriques	1
Journaux d'audit	1

Vous pouvez créer un maximum de 10 tables pour chaque règle de collecte de données (DCR). Au-delà de 10 tables, vous devez créer une autre DCR.

1. Accédez à votre espace de travail dans le portail Azure et cliquez sur **Tables** sous **Paramètres**.
2. Cliquez sur **Créer** et sélectionnez **Nouveau journal personnalisé (basé sur DCR)**

   
3. Dans **Créer un journal personnalisé** :
   a. Spécifiez un nom de table. Le nom de la table doit être au format **console_insightname**. Par exemple : **console_ns_sslvserver**, **console_ns_ssl_certkey**. Vous pouvez vous référer à l'étape 4 pour obtenir les noms de table applicables à chaque insight.
   b. Fournissez une description pour ajouter plus d'informations sur le nom de la table. Ceci est facultatif.
   c. Créez une nouvelle règle de collecte de données et ajoutez-la.
   d. Sélectionnez le point de terminaison de collecte de données dans la liste.

      
   e. Cliquez sur **Suivant**.
4. Dans l'onglet **Schéma et transformation**, vous devez télécharger les journaux d'échantillon JSON pour l'information que vous souhaitez exporter. Vous pouvez utiliser l'exemple JSON suivant pour chaque information et créer un fichier JSON à télécharger :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
SSL (1)	{"id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED",	console_ns_sslvserver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"redirectportrewrite": "DISABLED", "skipclientcertpolicycheck": "", "tls13sessionticketsperauthcontext": 1, "cipherredirect": "DISABLED", "dropreqwithnohostheader": "NO", "sessionticketlifetime": -1, "maxage": 0, "pushenctrigger": "Always", "strictsigdigestcheck": "f", "sslredirect": "DISABLED", "sessionkeylifetime": -1, "alpnprotocol": "", "clientauthuseboundcachain": "", "sesstimeout": 120, "clientcert": "", "snihttphostmatch": "CERT", "preload": "NO", "prevsessionkeylifetime": -1, "sessionticketkeydata": "", "encrypttriggerpktcount": 45, "cleartextport": "", "ssliocspcheck": "", "hsts": "f", "sslinterception": "", "commonname": "", "sslireneg": "", "ocspstapling": "DISABLED",	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"quantumsize": 8192, "insertionencoding": "Unicode", "sslimaxsessperserver": -1, "cipherurl": "", "pushflag": 0, "zerorttearlydata": "DISABLED", "allowextendedmastersecret": "", "dhekeyexchangewithpsk": "NO", "clientauth": "DISABLED", "denysslreneg": "NONSECURE", "sendclosenotify": "YES", "dhcount": 0, "snienable": "DISABLED", "table_name": "ns_sslvserver"}	
SSL (2)	{"id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141",	console_ns_ssl_certkey

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "no_of_bound_entities": 0, "partition_name": "", "display_name": "10.106.186.141", "hostname": "athulsadc", "key_name": "", "subjaltname": "", "managed_by": "", "certificate_dn": "", "linkcertkeyname": "", "table_name": "ns_ssl_certkey"}	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
WAF	[{"ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-",	console_af_threat_exporter_data_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"violation_value": "-NA-", "violation_location": 4, "violation_threat_index": 5, "app_threat_index": 5, "http_method": 0, "violation_action": 3, "violation_action_desc": "Blocked", "severity_type": 2, "severity_type_desc": "Medium", "iprep_score": 0, "iprep_category": 0, "counter_value": 0, "appname": "vserver_1_10.106.185.156_lb", "violation_category": 12, "violation_category_desc": "Start URL", "source_ipv6_address": "", "true_client_ip": "\\N", "backend_vserver": "", "backend_appname": "", "transactionId": "0", "table_name": "af_threat_exporter_data_l2"}]	
Bot	{"ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2",	console_af_bot_attack_details_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	
Gateway Insight (1)	{"adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0,	console_af_vpn_error_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}	
Gateway Insight (2)	{"adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}	console_ns_vpnvserver
Gateway Insight (3)	{"adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1}	console_af_vpn_session_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
Gateway Insight (4)	{"active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}	console_af_vpn_active_session_1
Gateway Insight (5)	{"adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports"}	console_af_vpn_error_reports
Événements	{"rpt_sample_time": -1, "category": "HealthMonitoring", "entity": "10.106.186.148:HealthMonitoring:System Disk Usage", "counter_threshold_value": "", "id": "0f2607cf-f97d-4f71-9162-11e580262e93", "timestamp": 1712927472, "message": "Disk Usage High: 63.24%", "severity": "Critical", "user_name": "",	console_event

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"device_entity_type": "", "device_type": "", "counter_actual_value": "", "cmd_auth_status": "", "source": "10.106.186.148", "history": "Update Time= Fri, 12 Apr 2024 06:32:49 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:27:46 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:22:44 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:17:41 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:12:38 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:07:36 U",	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	"config_cmd": "", "failureobj": "System Disk Usage", "operation_type": "undefined", "device_entity_name": "", "cmd_exec_status": "", "device_family": "", "source_event_id": -1, "source_system_ip": "10.106.186.148", "trap_id": 35, "table_name": "event"}	
Métriques	{"memory_free": 28830060544.0, "disk_used": 81248694272.0, "disk_free": 29632114688.0, "node_type": "", "memory_total": 34355544064.0, "cpu_usage": 0.49, "disk_total": 120522616832.0, "disk_usage": 73.28, "node_id": "", "id": "1be15a09-d078-469c-868a-bfbfcffe5ef1", "disk_total_capacity": 0.0, "page_size": 4096.0, "memory_usage": 16.08, "table_name": "mps_health"}	console_mps_health
Journaux d'audit	{"system_gmt_time":1721868291,	console_syslog_messages

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INFORMATIONS	JSON	NOM DE LA TABLE À UTILISER
	`"source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage", "instance_ip":"X.X.X.X", "app_name":""}`	

Après avoir téléchargé le JSON, vous pouvez afficher les détails suivants :

Cliquez sur **Éditeur de transformation**, saisissez la requête suivante qui est applicable pour l'insight approprié, puis cliquez sur **Exécuter** pour accepter les données à partir de l'heure d'interrogation dans NetScaler Console.

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time) | project-rename sslvserver_id = id`
- **WAF** et **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

5. Cliquez sur **Suivant**, puis sur **Créer** pour terminer.
6. Accédez aux **règles de collecte de données**, puis cliquez sur la DCR que vous avez créée.
7. Sous **Configuration**, cliquez sur **Sources de données** pour afficher le tableau créé.

La DCR (règle de collecte de données) nécessite un accès au rôle **Éditeur de métriques de surveillance**.

a. Accédez à votre DCR, accessible depuis votre portail Azure sous **Récents**.
b. Sur la page de votre DCR, cliquez sur **Contrôle d'accès (IAM)**, puis sur **Ajouter une attribution de rôle**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Dans la barre de recherche, tapez le mot-clé « monitor » pour sélectionner **Éditeur de métriques de surveillance**, puis cliquez sur **Suivant**.

d. Dans l'onglet **Membres**, cliquez sur **Sélectionner des membres** et sélectionnez l'application Entra que vous avez créée.

e. Cliquez sur **Vérifier + attribuer**.

Vous devez noter l'ID des règles de collecte de données. Accédez à la page des règles de collecte de données, sélectionnez votre DCR et cliquez sur la vue JSON pour noter l'ID.

ID DCR(/en-us/netscaler-application-delivery-management-software/media/sentinel-dcr-value.png)

Créer un abonnement dans NetScaler Console

Vous avez maintenant tout ce qu'il faut. La dernière étape consiste à configurer NetScaler Console en créant un abonnement et en ajoutant les détails requis. Pour créer un abonnement dans NetScaler Console, vous avez besoin des détails suivants que vous avez notés :

- URL du point de terminaison
- ID des règles de collecte de données
- ID du locataire
- ID client
- Secret client

1. Connectez-vous à NetScaler Console.
2. Accédez à **Paramètres > Intégration de l'observabilité**.
3. Dans la page **Intégrations**, cliquez sur **Ajouter**.
4. Dans la page **Créer un abonnement**, spécifiez les détails suivants :

   a. Spécifiez un nom de votre choix dans le champ Nom de l'abonnement.

   b. Sélectionnez **NetScaler Console** comme **Source** et cliquez sur **Suivant**.

   c. Sélectionnez **Microsoft Sentinel** et cliquez sur **Configurer**. Dans la page **Configurer le point de terminaison**, saisissez tous les détails, puis cliquez sur **Soumettre**.

   d. Cliquez sur **Suivant**.

5. Cliquez sur **Ajouter des informations** et, dans l'onglet **Sélectionner une fonctionnalité**, en fonction des tables que vous avez ajoutées dans Microsoft Azure, sélectionnez les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fonctionnalités que vous souhaitez exporter, puis cliquez sur **Ajouter la sélection**, et cliquez sur **Suivant**.

6. Dans l'onglet **Sélectionner une instance**, vous pouvez choisir **Sélectionner toutes les instances** ou **Sélection personnalisée**, puis cliquer sur **Suivant**.

   - **Sélectionner toutes les instances** - Exporte les données vers Microsoft Sentinel à partir de toutes les instances NetScaler.
   - **Sélection personnalisée** - Vous permet de sélectionner les instances NetScaler dans la liste. Si vous sélectionnez des instances spécifiques dans la liste, les données sont exportées vers Microsoft Sentinel uniquement à partir des instances NetScaler sélectionnées.

7. Cliquez sur **Soumettre**.

Afficher les journaux dans Microsoft Azure

Après avoir tout configuré, nous vous recommandons d'attendre 30 minutes pour afficher les détails dans Microsoft Azure.

1. Dans votre portail Azure, accédez à votre **espace de travail Log Analytics**.
2. Cliquez sur **Journaux**, fournissez le nom de la table, puis cliquez sur **Exécuter** pour afficher les résultats.



Vous pouvez également dépanner et utiliser les journaux pour vérifier les configurations. Par exemple, utilisez l'option Poll Now dans l'interface graphique de NetScaler Console pour l'information configurée et :

1. Connectez-vous à votre NetScaler Console à l'aide d'un client SSH.
2. Tapez shell pour entrer en mode bash.
3. Utilisez la commande suivante pour afficher les journaux :

```
tail -f /var/mps/log/nbs/nbs_api.log
```

Les exemples suivants vous aident à analyser les erreurs possibles pour le dépannage :



1. Ce journal indique que vous avez fourni un ID client invalide pour l'abonnement Microsoft Sentinel dans NetScaler Console (**Paramètres > Intégrations d'observabilité**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solution de contournement : Assurez-vous d'avoir copié le bon ID client et modifiez l'abonnement en fournissant le bon ID client. Pour plus d'informations, consultez Créer une application Microsoft Entra.



2. Ce journal indique que vous n'avez pas configuré la table ssl_certkey requise dans votre Microsoft Azure.

   Solution de contournement : Configurez une table pour ssl_certkey dans Microsoft Azure. Pour plus d'informations, consultez Créer des tables pour exporter des données.

Configurer les instances NetScaler® pour l'exportation d'informations vers Prometheus à l'aide du schéma par défaut

NetScaler prend en charge l'exportation directe de métriques vers Prometheus. Vous pouvez utiliser l'ensemble riche de métriques fournies par l'instance NetScaler pour surveiller la santé de NetScaler et la santé des applications. Par exemple, vous pouvez collecter des métriques sur l'utilisation du CPU et de la mémoire pour connaître la santé de NetScaler. De même, vous pouvez utiliser des métriques telles que le nombre de requêtes HTTP reçues par seconde ou le nombre de clients actifs pour surveiller la santé des applications.

Pour exporter les métriques vers Prometheus, vous devez configurer un profil d'analyse de type série chronologique. Pour plus d'informations, consultez Surveiller NetScaler, les applications et la sécurité des applications à l'aide de Prometheus.

Avec la fonctionnalité d'intégration d'observabilité dans NetScaler Console, vous pouvez configurer l'exportation d'informations vers Prometheus à l'aide du schéma par défaut.

1. Accédez à **Paramètres > Intégration d'observabilité**.
2. Dans la page **Intégrations**, cliquez sur **Ajouter**.
3. Dans la page **Créer un abonnement**, spécifiez les détails suivants :
   a. Spécifiez un nom de votre choix dans le champ **Nom de l'abonnement**.
   b. Sélectionnez **NetScaler** comme **Source** et cliquez sur **Suivant**.
   c. Sélectionnez **Prometheus** comme Destination.
   d. Sélectionnez **Par défaut** pour les informations par défaut à exporter.
   e. Cliquez sur **Ajouter des instances** et sélectionnez les instances pour lesquelles vous souhaitez exporter des informations vers Prometheus.
   f. Cliquez sur **Soumettre**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les journaux des configurations échouées

Après avoir créé un abonnement, vous pouvez afficher l'état de l'abonnement créé dans **Paramètres > Intégration d'observabilité**. Si l'état indique **Échec**, cliquez pour afficher les détails.

☐ Cliquez sur **Afficher les détails** sous **Détails du travail de configuration**.

☐ Cliquez sur **Afficher les journaux** pour afficher les détails du problème.

☐

Configurer l'exportation des métriques et des journaux d'audit NetScaler® vers Splunk

NetScaler prend en charge l'exportation directe des métriques vers Splunk au format JSON. NetScaler fournit des métriques riches pour surveiller la santé de vos applications et la sécurité de vos applications. En exportant les métriques fournies par NetScaler vers Splunk, vous pouvez visualiser les métriques et obtenir des informations significatives.

La journalisation d'audit vous permet d'enregistrer les états et les informations de statut de NetScaler collectés par divers modules dans NetScaler. En examinant les journaux, vous pouvez résoudre les problèmes ou les erreurs et les corriger.

Pour plus d'informations, consultez :

- Exporter les journaux d'audit directement de NetScaler vers Splunk
- Exporter les métriques directement de NetScaler vers Splunk

Pour configurer l'exportation des métriques et des journaux d'audit vers Splunk via NetScaler Console :

1. Accédez à **Paramètres > Intégration de l'observabilité**.
2. Dans la page **Intégrations**, cliquez sur **Ajouter**.
3. Dans la page **Créer un abonnement**, spécifiez les détails suivants :
    a. Spécifiez un nom de votre choix dans le champ **Nom de l'abonnement**.
    b. Sélectionnez **NetScaler** comme **Source** et cliquez sur **Suivant**.
    c. Sélectionnez **Splunk** comme **Destination** et cliquez sur **Configurer**. Dans Configurer le point de terminaison :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **URL du point de terminaison** - Spécifiez les détails du point de terminaison Splunk. Le point de terminaison doit être au format `https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event``.
- **Jeton d'authentification** - Copiez et collez le jeton d'authentification de Splunk.
- Cliquez sur **Soumettre**.

d. Cliquez sur **Suivant**.

e. Cliquez sur **Ajouter des informations** et sélectionnez **Métriques NetScaler** et **Journaux d'audit NetScaler**, puis cliquez sur **Ajouter la sélection**.

f. Cliquez sur **Suivant**.

g. Cliquez sur **Ajouter des instances** et sélectionnez les instances.

h. Cliquez sur **Soumettre**.

Afficher les journaux des configurations ayant échoué

Après avoir créé un abonnement, vous pouvez afficher l'état de l'abonnement créé dans **Paramètres > Intégration de l'observabilité**. Si l'état indique **Échec**, cliquez pour afficher les détails.

Cliquez sur **Afficher les détails** sous **Détails du travail de configuration**.

Cliquez sur **Afficher les journaux** pour afficher les détails du problème.

Listes de contrôle d'accès

Une liste de contrôle d'accès (ACL) est un ensemble de conditions que vous pouvez appliquer à une appliance réseau pour filtrer le trafic IP et protéger votre appliance contre tout accès non autorisé.

Vous pouvez configurer l'ACL dans l'interface graphique de NetScaler Console pour limiter et contrôler l'accès à NetScaler Console. L'ACL sur NetScaler Console est prise en charge à partir de la version 14.1-29.x.

Directives d'utilisation

- Lorsque vous mettez à niveau NetScaler Console vers la version 14.1-29.x, la fonctionnalité ACL est désactivée par défaut.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- En tant qu'administrateur, vous ne pouvez contrôler que les paquets entrants via l'ACL sur NetScaler Console.
- Toute configuration sur NetScaler Console ne nécessite aucune modification de la configuration ACL existante.

Comment configurer une ACL

La configuration d'une ACL implique :

- Activer la fonctionnalité ACL
- Créer une règle ACL
- Activer la règle ACL

Activer la fonctionnalité ACL

1. Connectez-vous à l'interface graphique de NetScaler Console et accédez à **Paramètres > Liste de contrôle d'accès (ACL)**
2. À l'aide du bouton bascule, activez la fonctionnalité ACL.



Créer une règle ACL

1. Sur la page ACL, cliquez sur **Créer une règle**.
2. Dans la fenêtre **Créer une règle**, ajoutez les détails répertoriés dans le tableau suivant :

OPTIONS	DESCRIPTION
Nom	Spécifiez un nom de votre choix.
Protocole	Sélectionnez un protocole dans le menu. Par défaut, TCP est sélectionné. Vous pouvez sélectionner ANY pour autoriser tous les protocoles.
Adresse IP/Sous-réseau source	Spécifiez l'adresse IP source ou le sous-réseau source auquel la règle s'applique. Sélectionnez ANY si la règle doit être appliquée à tout le trafic entrant.
IP de destination	L'adresse IP de la console NetScaler est automatiquement renseignée comme IP de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTIONS	DESCRIPTION
	destination. Ce champ ne peut pas être modifié.
Port de destination	Spécifiez le port de destination auquel la règle s'applique. Sélectionnez ANY si la règle s'applique à tous les ports de destination.
Action	Sélectionnez l'action pour la règle, qui est Autoriser ou Refuser.
Priorité	Attribuez une priorité pour spécifier l'ordre dans lequel la règle doit être évaluée. Les numéros de priorité déterminent l'ordre dans lequel les règles ACL sont comparées à un paquet entrant. Un numéro de priorité inférieur a une priorité plus élevée. Par exemple, le numéro de priorité 1 a une priorité plus élevée que le numéro de priorité 2. Si aucune des règles ne correspond au paquet entrant, le paquet est bloqué.

3. Cliquez sur **OK** pour créer la règle.

Une fois la règle créée, elle est à l'état désactivé. Pour que la règle soit effective, vous devez l'activer.

REMARQUE :

Pour activer une règle, la fonctionnalité ACL doit être activée. Si la fonctionnalité est désactivée et que vous tentez d'activer une règle ACL, le message « ACL is not running » (ACL non exécutée) s'affiche.

Activer une règle ACL

1. Passez votre souris sur la règle que vous souhaitez activer et cliquez sur le cercle avec trois points.
2. Dans le menu, sélectionnez **Activer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur l'onglet Activer.
4. À l'invite, cliquez sur **Oui** pour confirmer.

Autres actions pour les règles ACL

Vous pouvez appliquer les actions suivantes aux règles ACL :

- Désactiver une règle ACL
- Modifier une règle ACL
- Supprimer une règle ACL
- Renuméroter la priorité des règles ACL

Désactiver une règle ACL

1. Passez la souris sur la règle que vous souhaitez désactiver et sélectionnez le cercle avec trois points.
2. Cliquez sur **Désactiver** dans la liste.
3. Vous pouvez également sélectionner le bouton radio de cette règle et cliquer sur le bouton **Désactiver**.
4. Cliquez sur **Oui** pour confirmer.

REMARQUE :

Lorsque vous désactivez une règle, celle-ci ne s'applique plus au trafic entrant. Cependant, la configuration de la règle reste sous les paramètres ACL.

Modifier une règle ACL

1. Passez la souris sur la règle que vous souhaitez modifier et sélectionnez le cercle avec trois points.
2. Cliquez sur **Modifier la règle** dans la liste.
3. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur le bouton **Modifier la règle**.
4. Effectuez les modifications et cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous pouvez modifier une règle à la fois à l'état activé et désactivé. Si vous modifiez une règle déjà activée, les modifications sont appliquées immédiatement. Pour une règle à l'état désactivé, les modifications sont appliquées lorsque vous activez la règle.

Supprimer une règle ACL

1. Assurez-vous que la règle est à l'état désactivé. Vous ne pouvez pas supprimer une règle à l'état activé.
2. Passez la souris sur la règle que vous souhaitez supprimer et sélectionnez le cercle avec trois points.
3. Cliquez sur **Supprimer la règle** dans la liste.
4. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur le bouton **Supprimer la règle**.
5. Cliquez sur **Oui** pour confirmer.

Renuméroter les priorités des règles ACL

1. Passez la souris sur la règle dont vous souhaitez renuméroter les priorités et sélectionnez le cercle avec trois points. Cliquez sur **Renuméroter la priorité** dans la liste.
2. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et, dans la liste **Sélectionner une action**, sélectionnez **Renuméroter la priorité**.

NetScaler® attribue automatiquement de nouveaux numéros de priorité, qui sont des multiples de 10, à toutes les règles existantes.

Modifiez les règles pour attribuer des numéros de priorité selon vos besoins. Consultez la section « Pour modifier une règle ACL » pour plus d'informations sur la modification d'une règle.

Exemple de numéros de priorité existants :



Exemple de la priorité renumérotée par NetScaler Console :



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dépannage

Si les règles ACL sont mal configurées, tous les comptes utilisateur peuvent se voir refuser l'accès. Si vous perdez involontairement tout accès réseau à NetScaler Console en raison d'une configuration ACL incorrecte, suivez ces étapes pour retrouver l'accès :

1. Connectez-vous à NetScaler Console à l'aide d'un client SSH.
2. Exécutez la commande `pfctl –d`.
3. Connectez-vous à l'interface graphique de NetScaler Console et reconfigurez l'ACL en conséquence.

Utiliser les journaux d'audit de NetScaler Console pour gérer et surveiller votre infrastructure

Vous pouvez utiliser le service NetScaler Console pour suivre tous les événements sur NetScaler Console et les événements syslog générés sur les instances NetScaler gérées par NetScaler Console. Ces messages peuvent vous aider à gérer et à surveiller votre infrastructure. Cependant, les messages de journal ne sont une excellente source d'informations que si vous les examinez, et NetScaler Console simplifie la manière d'examiner les messages de journal.

Vous pouvez utiliser des filtres pour rechercher les messages syslog et les journaux d'audit de NetScaler Console. Les filtres vous aident à affiner vos résultats et à trouver exactement ce que vous cherchez en temps réel. L'aide à la recherche intégrée vous guide pour filtrer les journaux. Une autre façon de consulter les messages de journal est de les exporter aux formats PDF, CSV, PNG et JPEG. Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à divers intervalles.

Vous pouvez consulter les types de messages de journal suivants à partir de l'interface graphique de NetScaler Console :

- Journaux d'audit liés à l'instance NetScaler
- Journaux d'audit liés à NetScaler Console
- Journaux d'audit des applications

Journaux d'audit liés à l'instance NetScaler

Avant de pouvoir afficher les messages syslog liés à l'instance NetScaler depuis NetScaler Console, configurez le service NetScaler Console comme serveur syslog pour votre instance NetScaler. Une fois la configuration terminée, tous les messages syslog sont redirigés de l'instance vers NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer le service NetScaler Console comme serveur syslog

Suivez ces étapes pour configurer NetScaler Console comme serveur syslog :

1. Depuis l'interface graphique de NetScaler Console, accédez à **Infrastructure > Instances**.
2. Sélectionnez l'instance NetScaler à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans NetScaler Console.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Syslog**.
4. Cliquez sur **Activer**.
5. Dans la liste déroulante **Facility**, sélectionnez une installation locale ou de niveau utilisateur.
6. Sélectionnez le niveau de journalisation requis pour les messages syslog.
7. Cliquez sur **OK**.

Ces étapes configurent toutes les commandes syslog dans l'instance NetScaler, et NetScaler Console commence à recevoir les messages syslog. Vous pouvez afficher les messages en accédant à **Infrastructure > Événements > Messages Syslog**. Cliquez sur **Besoin d'aide ?** pour ouvrir l'aide à la recherche intégrée. Pour plus d'informations, consultez Afficher et exporter les messages syslog.

Pour exporter les messages de journalisation, cliquez sur l'icône de flèche dans le coin supérieur droit.

Ensuite, cliquez sur **Exporter maintenant** ou **Planifier l'exportation**. Pour plus d'informations, consultez Afficher et exporter les messages syslog.

Journaux d'audit liés à NetScaler Console

Basé sur des règles préconfigurées, NetScaler Console génère des messages de journal d'audit pour les événements correspondants, vous aidant à surveiller la santé de votre infrastructure.

Configuration d'un serveur syslog pour surveiller les journaux d'audit et de shell

Vous pouvez configurer un serveur syslog externe pour surveiller les événements de journal d'audit et de shell pour vos déploiements NetScaler Console. Pour les versions 14.1-34.x et ultérieures, vous pouvez configurer un serveur syslog pour également recevoir les événements de journal de shell. Ceci s'ajoute à la configuration existante des journaux d'audit. Similaires aux journaux d'audit, les journaux de shell peuvent être configurés pour différents niveaux de journalisation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Suivez ces étapes pour configurer un serveur syslog sur NetScaler Console :

1. Accédez à **Paramètres de l'interface utilisateur > Journaux d'audit > Serveurs Syslog**.
2. Choisissez les niveaux de journalisation pour les journaux d'audit, les journaux de shell, ou pour les deux.
    - **Tout** : Sélectionne tous les niveaux de journalisation répertoriés pour les événements d'audit ou liés au shell.
    - **Aucun** : Efface toutes les sélections et aucun niveau de journalisation n'est sélectionné.
    - **Personnalisé** : Vous permet de sélectionner des niveaux de journalisation spécifiques dans la liste disponible, présentés sous forme de cases à cocher.
3. Cliquez sur **OK** pour continuer avec la configuration sélectionnée. Cela permet à NetScaler Console d'envoyer des événements d'audit et/ou liés au shell au serveur syslog configuré.

Pour afficher tous les messages de journal d'audit présents dans NetScaler Console, accédez à **Paramètres > Messages du journal d'audit**.

Pour exporter les messages du journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.

Journaux d'audit liés aux applications

Vous pouvez afficher les messages du journal d'audit pour toutes les applications NetScaler Console ou pour une application spécifique.

- Pour afficher tous les messages du journal d'audit pour toutes les applications présentes dans NetScaler Console, accédez à **Infrastructure > Fonctions réseau > Audit**.
- Pour afficher les messages du journal d'audit pour une application spécifique dans NetScaler Console, accédez à **Applications > Tableau de bord**, cliquez sur un serveur virtuel et sélectionnez **Journal d'audit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licences NetScaler

NetScaler Console vous permet de gérer, d'allouer et de surveiller les licences sur vos instances NetScaler. Les rubriques suivantes vous aident à gérer les licences NetScaler :

- Service d'activation des licences
- Bonnes pratiques
- Gestion des licences
- Capacité minimale et maximale pour l'extraction
- Licence NetScaler Flexed
- Configurer les licences
- Tableau de bord des licences
- Rapports de licence
- Transition vers les licences Flexed
- Scénarios d'expiration des licences Flexed ou Pooled et comportement en cas de problèmes de connectivité
- Configurer NetScaler Console en tant que serveur de licences Flexed ou Pooled
- Licences héritées

Service d'activation de licence

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licence (LAS) est la technologie de nouvelle génération pour l'activation des produits de la suite Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après April 15, 2026, prenant en charge les licences NetScaler Flexed (Citrix Platform License/Universal Hybrid Multi-Cloud), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les versions minimales requises de NetScaler compatibles avec le LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge du LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à partir du April 15 2026 pour les versions 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures de Console sur site. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou la version 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées, telles que les licences NetScaler de processeur virtuel (vCPU en pool), NetScaler VPX Check-In et Check-Out (CICO), et perpétuelles, ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront non licenciées lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa responsabilité, en plus de tout autre recours dont Citrix pourrait disposer en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Avant de commencer votre transition vers le LAS, nous vous recommandons de lire LAS pour NetScaler. Cela vous permettra de comprendre les prérequis généraux, les types de licences pris en charge ou non, le flux de travail précis pour vos types de licences et de déploiement spécifiques, ainsi que d'autres informations importantes.

Le service d'activation de licence (LAS) est une nouvelle solution de licence basée sur le cloud qui offre une alternative aux licences traditionnelles basées sur des fichiers. Le LAS introduit de nouveaux modules pour l'activation des produits Citrix et NetScaler, garantissant une approche fluide et moderne de la gestion des licences.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- LAS est un mécanisme de licence, pas un type de licence.
- La gestion des licences basée sur des fichiers fait référence à l'ancienne méthode de gestion des licences utilisant des droits manuels. Dans ce document, « gestion des licences basée sur des fichiers » et « droits gérés manuellement » sont utilisés de manière interchangeable car ils décrivent le même concept.

Voici les principaux avantages de LAS :

- Livraison automatisée des droits via un blob de droits.
- L'agent externe en tant que proxy pour la communication de licence est facultatif.
- LAS élimine le besoin de fichiers de licence logicielle Z-Cap sur les instances NetScaler MPX™ et SDX.

REMARQUES :

- La nouvelle option Synchroniser les licences vous permet de déclencher manuellement la synchronisation à la demande, garantissant que les droits sont mis à jour immédiatement.
- La fréquence par défaut de synchronisation des droits est d'une fois par heure si les droits LAS n'ont pas été synchronisés avec le service NetScaler Console, puis d'une fois toutes les 24 heures. Pour une synchronisation à la demande, cliquez sur `Sync Now`.

Compatibilité des versions de NetScaler pour LAS

Pour utiliser LAS, vos instances NetScaler doivent exécuter l'une des versions minimales suivantes :

- NetScaler ADCs : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour utiliser le LAS, assurez-vous d'avoir rempli les conditions préalables suivantes :

- Vous devez disposer d'un compte Citrix Cloud valide. Pour plus d'informations sur les comptes cloud existants ou pour intégrer de nouveaux comptes cloud, consultez Gestion des comptes.
- L'ID d'organisation (Org ID) lié au compte Citrix Cloud utilisé pour le flux de travail d'activation du LAS doit posséder des droits d'utilisation valides achetés. Pour afficher les droits d'utilisation actuels, visitez Droits d'utilisation.
- NetScaler Console et les instances NetScaler doivent exécuter une version compatible avec le LAS.
- L'instance NetScaler est ajoutée en tant qu'instance gérée dans NetScaler Console.
- Le LAS prend en charge les licences Flexed (UHMC/CPL), les licences de bande passante en pool et les licences de bande passante à durée déterminée. Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, ne sont pas prises en charge par le LAS.
- Pour les appliances SDX, mettez à niveau NetScaler SVM vers une version prise en charge par le LAS et passez à la licence basée sur le LAS. La version spécifique de la build VPX n'a pas d'impact sur la compatibilité du LAS.

Le diagramme suivant concerne le LAS avec Console on-prem Cloud Connect.



REMARQUE :

Si vous débutez avec NetScaler Console, commencez par Mise en route.

Transition vers le LAS

Activer le LAS avec Cloud Connect

L'option **Activer le LAS avec Cloud Connect** est destinée aux déploiements Console sur site connectés au cloud. Ce déploiement simplifie la gestion des licences en téléchargeant automatiquement les droits d'utilisation et en gérant les renouvellements en temps opportun directement depuis le service Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Assurez-vous que l'option **Activer Cloud Connect** est activée pour utiliser la méthode de déploiement **Activer LAS avec Cloud Connect**. Pour activer l'option, consultez Activer Cloud Connect.
- LAS est automatiquement activé une fois que Cloud Connect est activé.

Vous pouvez vérifier que Cloud Connect est activé en vérifiant le coin supérieur droit de l'interface graphique de la console. Une fois que vous êtes connecté au service NetScaler Console, vous êtes dirigé vers l'onglet **LAS** sous **Gestion des licences**. Ici, vous pouvez consulter les dates de renouvellement précédente et suivante, mais aucune action manuelle n'est nécessaire.

L'activation de LAS implique l'obtention d'un fichier ou d'un blob d'autorisation de licence sur NetScaler Console sur site. Lorsque vous accédez à **Licences NetScaler > Gestion des licences > LAS**, une introduction au service d'activation de licence (LAS) s'affiche.

Une fois que LAS est activé sur votre Console sur site, toutes vos autorisations de licence NetScaler Flexed et Pooled apparaissent dans la section **Licences NetScaler > Gestion des licences > Service d'activation de licence (LAS)**.



Grâce à sa fonctionnalité de connexion au cloud, Console sur site se connecte au service Console, qui récupère le fichier ou le blob d'autorisation de licence auprès de LAS.

Ce fichier ou blob d'autorisation est valide pendant 30 jours. Pour garantir une licence continue, la Console connectée au cloud actualise automatiquement ce blob d'autorisation chaque jour avec LAS.

Avec la gestion des licences basée sur des fichiers, vos autorisations et configurations appliquées sont visibles sous l'onglet **Licences NetScaler > Gestion des licences > Gestion manuelle des fichiers de licence**.



L'indicateur d'état de la télémétrie sur la page de gestion des licences sert d'alerte critique pour le maintien de la conformité de la télémétrie.

- **Icône rouge** : Indique qu'une attention immédiate est requise. Le système ne collecte pas de télémétrie pour certaines ou toutes les instances NetScaler gérées. Cet état indique une non-conformité potentielle de la télémétrie et des impacts sur les licences.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Icône verte** : Confirme que la télémétrie est active, indiquant que la console envoie avec succès la télémétrie de toutes les instances NetScaler gérées.

Si l'état nécessite une attention immédiate, accédez à la page de télémétrie en cliquant sur l'indicateur. Assurez-vous que tous les problèmes mis en évidence sur la page de télémétrie NetScaler sont résolus. Pour plus de détails, consultez Diagnostics pour le dépannage des problèmes de collecte et de téléchargement de télémétrie.

Licencier ou migrer des instances NetScaler vers LAS

Lorsque vous accédez à **NetScaler Licenses > License management > License Activation Service (LAS)**, l'interface graphique se met à jour dynamiquement en fonction de la compatibilité de vos instances NetScaler. Si vous n'avez aucune instance NetScaler sur une version compatible avec LAS, un message s'affiche à l'écran vous invitant à mettre à niveau ou à ajouter un NetScaler.

REMARQUE :

Si certaines de vos instances NetScaler sont mises à niveau vers une version compatible, vous pouvez utiliser LAS pour ces instances spécifiques.

Si une ou plusieurs de vos instances NetScaler sont compatibles avec LAS, elles sont organisées en deux catégories :

Licencier les instances NetScaler avec LAS : Il s'agit d'instances qui n'utilisent pas encore LAS mais qui sont compatibles.

Migrer les instances NetScaler sous licence vers LAS : Il s'agit d'instances déjà sous licence via une méthode différente et qui sont éligibles à la migration vers LAS.

L'interface graphique de NetScaler s'adapte dynamiquement selon que vous êtes un utilisateur LAS pour la première fois (avec zéro instance sur LAS) ou un utilisateur existant (ayant déjà des instances sur LAS et en ajoutant maintenant d'autres).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Supprimez les licences locales basées sur des fichiers sur le SVM une fois que la licence ou la migration vers LAS est terminée. Les licences basées sur des fichiers se trouvent dans le dossier SVM `/mpsconfig/license` et doivent être supprimées de ce dossier à l'aide de l'invite de commande shell. Cette remarque s'applique aux workflows **Licencier avec LAS** et **Migrer vers LAS** pour les utilisateurs débutants et existants.

Utilisateur débutant

L'image suivante s'affiche pour l'utilisateur débutant :



LICENCES DES INSTANCES NETSCALER AVEC LAS

La section **Licencier les instances NetScaler avec LAS** répertorie les instances NetScaler qui ne sont pas actuellement sous licence ou qui n'utilisent pas de licence basée sur un fichier de bande passante flexible ou de bande passante groupée.

Pour attribuer des licences aux instances avec LAS, effectuez les étapes suivantes :

1. Sélectionnez **Licence avec le service d'activation de licence (LAS)**, cliquez sur **Suivant**.
2. Sélectionnez une instance, puis cliquez sur **Continuer**.
3. Saisissez les détails et cliquez sur **Soumettre**. Répétez les étapes pour chaque instance NetScaler que vous souhaitez licencier avec LAS.

REMARQUE :

- Les instances sélectionnées redémarrent pour que la licence prenne effet, à l'exception des instances SDX.

MIGRATION DES INSTANCES NETSCALER SOUS LICENCE EXISTANTES VERS LAS

La section **Migrer les instances sous licence existantes vers LAS** répertorie toutes les instances NetScaler avec des licences basées sur des fichiers Flexed ou Pooled. Elles sont classées comme suit :

- **Instances prêtes à être migrées :** Répertorie les instances qui sont sur des versions ou des builds compatibles avec LAS et qui sont prêtes à être migrées vers LAS. Pour migrer, effectuez les étapes suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Sélectionnez **Migrer vos instances NetScaler sous licence existantes vers LAS**, puis cliquez sur **Suivant**.

b. Dans **Migrer vers le service d'activation de licence (LAS)**, sélectionnez une ou plusieurs instances NetScaler, puis cliquez sur **Migrer**.



.

- **Instances nécessitant une mise à niveau avant la migration :** Répertorie les instances qui doivent être mises à niveau vers une version ou des builds compatibles avant la migration. Pour effectuer la mise à niveau, suivez les étapes suivantes :

  Prérequis :

  Pour utiliser les licences basées sur LAS, l'édition de votre instance NetScaler doit correspondre à l'édition de votre licence basée sur fichier Pooled ou Flexed. Assurez-vous de modifier l'édition de l'instance pour qu'elle corresponde à la nouvelle licence avant de commencer la migration.

  a. Sélectionnez **Migrez vos instances NetScaler sous licence existantes vers LAS**, puis cliquez sur **Mettre à niveau**.

  b. Dans la page **Mettre à niveau NetScaler**, sélectionnez l'instance et mettez à niveau les instances vers des versions ou des builds compatibles avec LAS.

Utilisateur LAS existant

Si vous êtes un utilisateur LAS existant, vous voyez l'interface graphique suivante.



.

Remarque : Pour afficher les instances CPX sous licence avec LAS, consultez l'interface graphique du tableau de bord Flexed. Les instances CPX ne sont pas répertoriées ici sous l'instance NetScaler avec LAS.

LICENCE DES INSTANCES NETSCALER AVEC LAS

La section **Licence des instances NetScaler avec LAS** répertorie les instances NetScaler qui ne sont pas actuellement sous licence ou qui utilisent une licence autre qu'une licence basée sur un fichier de bande passante Flexed ou de bande passante Pooled.

Pour attribuer une licence aux instances avec LAS, effectuez les étapes suivantes :

1. Sous **Licence avec License Activation Service (LAS)**, cliquez sur **Licence avec LAS**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sélectionnez une instance, et cliquez sur **Continuer**.
3. Saisissez les détails et cliquez sur **Soumettre**. Répétez les étapes pour chaque instance NetScaler que vous souhaitez licencier avec LAS.



.

REMARQUE :

- Les instances sélectionnées redémarrent pour que la licence prenne effet, à l'exception des instances SDX.

MIGRER LES INSTANCES NETSCALER SOUS LICENCE VERS LAS

La section **Migrer les instances NetScaler sous licence vers LAS** répertorie toutes les instances NetScaler dotées d'une licence basée sur un fichier Flexed ou Pooled. Elles sont classées comme suit :

- **Instances dans LAS :** Répertorie les instances qui utilisent déjà la licence basée sur LAS.
- **Instances prêtes à être migrées :** Répertorie les instances compatibles prêtes à être migrées. Pour migrer, suivez les étapes suivantes :
  a. Sélectionnez **Migrer les instances NetScaler sous licence vers LAS**, cliquez sur **Migrer**.
  b. Sélectionnez une ou plusieurs instances NetScaler, puis cliquez sur **Migrer**.
- **Instances nécessitant une mise à niveau avant la migration :** Répertorie les instances qui doivent être mises à niveau vers une version compatible. Pour mettre à niveau, suivez les étapes suivantes :

  Prérequis :

  Pour utiliser la licence basée sur LAS, l'édition de votre instance NetScaler doit correspondre à l'édition de votre licence Pooled ou Flexed. Assurez-vous de modifier l'édition de l'instance pour qu'elle corresponde à la nouvelle licence avant de commencer la migration.

  a. Sélectionnez **Instances nécessitant une mise à niveau avant la migration**, cliquez sur **Mettre à niveau**.
  b. Sélectionnez une ou plusieurs instances NetScaler, puis cliquez sur **Mettre à niveau**.
  c. Saisissez les détails et cliquez sur **Soumettre**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comportement du blob d'activation de licence

Les blobs d'activation de licence que les instances NetScaler obtiennent de Console sur site dans le cadre de **Licence avec LAS ou Migrer vers LAS** sont valides pendant 30 jours. Si un NetScaler perd puis retrouve la connectivité avec Console sur site, le blob d'activation de licence est immédiatement restauré.

Lorsqu'un NetScaler est incapable de se reconnecter à Console sur site pendant 24 heures, il entre dans une période de grâce. Par défaut, les blobs d'activation de licence se rafraîchissent toutes les 8 heures. Si trois tentatives de rafraîchissement consécutives de 8 heures échouent sur 24 heures, le NetScaler entre dans une période de grâce.

Alerte de période de grâce de la licence

Voici les points de contact pour l’alerte de période de grâce de la licence :

- Sur le tableau de bord Flexed, une icône d’avertissement apparaît, indiquant que l’instance est en période de grâce et le nombre de jours restants avant l’expiration du blob d’activation de licence.
- Chaque fois qu’un administrateur se connecte à l’interface graphique de l’instance NetScaler, un message contextuel apparaît, indiquant que l’instance est en période de grâce et le nombre de jours restants avant l’expiration du blob d’activation de licence.
- Des notifications par e-mail sont envoyées à l’adresse e-mail configurée. Pour plus d’informations, consultez Configurer les paramètres de messagerie.

  Remarque : Assurez-vous de sélectionner **Licences** pour la catégorie d’événements système afin de recevoir les notifications par e-mail liées aux licences.

Comportement mis à jour de NetScaler lorsque la connectivité est interrompue entre la console sur site et le service de console

Dans un déploiement connecté au cloud, LAS émet un blob d’activation LAS directement vers NetScaler Console sur site. Le blob d’activation pour NetScaler Console sur site est actualisé quotidiennement et reste valide pendant 30 jours, ou jusqu’à l’expiration du droit de licence, selon la première éventualité.

Une fois que NetScaler Console sur site reçoit ce blob d’activation valide, elle est autorisée à émettre des blobs d’activation en aval vers ses instances NetScaler sous licence. La NetScaler Console n’émet ces blobs en aval que tant que son propre blob est valide.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les blobs d’activation émis vers les instances NetScaler sont également valides pendant 30 jours, ou jusqu’à la date d’expiration restante du blob d’activation de NetScaler Console, selon la première éventualité.

Scénario A : La connectivité est interrompue entre NetScaler et NetScaler Console sur site

Si un NetScaler perd la connexion à NetScaler Console sur site, NetScaler Console sur site ne peut pas actualiser le blob d’activation de l’instance. NetScaler Console sur site tente d’actualiser toutes les 8 heures.Après 3 tentatives infructueuses (24 heures au total), l’instance NetScaler passe à l’état **Grace**. Les instances NetScaler affectées sont signalées sous l’état **Grace** dans l’interface graphique de NetScaler Console sur site.

REMARQUE :

Ce comportement s’applique à toutes les versions de NetScaler Console sur site qui prennent en charge LAS.

Scénario B : La connectivité est interrompue entre NetScaler Console sur site et le service NetScaler Console

Si le lien entre NetScaler Console sur site et le service NetScaler Console est interrompu, NetScaler Console sur site ne peut pas actualiser son propre blob d'activation.

Dans un tel cas, NetScaler Console sur site ne peut pas émettre les blobs d'activation glissants standard de 30 jours ; il émet des blobs aux instances NetScaler avec une validité décroissante (29, 28, 27... jusqu'à 0 jour). Si la connexion n'est pas rétablie dans les 30 jours, les instances NetScaler risquent une panne totale.

Dans les versions précédentes, cela se produisait brusquement sans que les instances NetScaler n'entrent jamais dans un statut **Grace** pour avertir l'administrateur.

À partir de la version 14.1-72.x, ce comportement a été mis à jour pour éviter les pannes inattendues. Les instances NetScaler sous licence par NetScaler Console sur site sont désormais automatiquement placées en statut **Grace** si la connexion au service NetScaler Console est interrompue et que le blob NetScaler Console sur site ne peut pas être actualisé.

Si la connectivité entre NetScaler Console sur site et le service NetScaler Console est rétablie dans les 30 jours, les instances NetScaler quittent avec succès la période de grâce.

Ce changement garantit que les administrateurs sont immédiatement alertés via le statut **Grace** dans l'interface graphique de NetScaler Console afin qu'ils puissent identifier, dépanner et résoudre le problème de connexion avant qu'une panne ne se produise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informations envoyées à LAS pendant le flux de travail de licence LAS

Cette section détaille toutes les informations envoyées dans le cadre de la demande d'un blob d'activation à LAS lors de chaque demande initiale et de chaque demande d'actualisation de blob d'activation LAS. Le tableau suivant récapitule les paramètres envoyés à LAS pendant le flux de travail de licence :

PARAMÈTRE	DESCRIPTION	NÉCESSITÉ DANS LE FLUX DE TRAVAIL LAS
GUID du serveur de licences	ID unique de Console sur site au format UUID	Paramètre de liaison LAS
ID du serveur de licences	ID unique de la console sur site en SHA256	Paramètre de liaison LAS
clé publique	Clé publique de la console sur site utilisée pour la distribution de jetons NetScaler	Garantit que le LAS a autorisé cette console
identifiant CC	ID Citrix Cloud utilisé pour l'intégration de la console sur site	Paramètre de liaison LAS
version LS	Version de build de la console sur site	Exigence d'activation LAS
Adresse IP et nom d'hôte de la console	Nom d'hôte de la console sur site au format IP_hostname	Exigence d'activation LAS
activated_clients	Liste des NetScalers avec les licences LAS, les fonctionnalités et les heures de demande. Remarque : les NSIP ne sont pas partagés ; seul le LPEID (ID unique) est fourni.	Liste des NetScalers avec les blobs d'activation LAS générés par cette console.
ID de dernière activation	ID d'activation LAS précédent, fourni lors du renouvellement	Pour le suivi côté LAS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

À partir de la version 14.1-60.57 de NetScaler Console sur site, le flux de travail de licence basé sur LAS pour les déploiements connectés au cloud n'utilise plus l'adresse IP et le nom d'hôte. Au lieu de cela, un identifiant système (`lsguid`) est utilisé par LAS pour identifier de manière unique le déploiement NetScaler Console sur site connecté au cloud.

Bonnes pratiques pour la surveillance de votre environnement NetScaler Console sur site connecté au cloud ayant migré vers LAS

Ce document présente les bonnes pratiques que vous pouvez suivre pour surveiller vos environnements NetScaler qui utilisent LAS. Ce document s'applique aux déploiements qui utilisent LAS avec Console sur site.

Prérequis

- Lisez la page LAS pour NetScaler, y compris la FAQ pour LAS avec le service Console.
- Lisez le Service d'activation de licence et effectuez votre migration LAS.
- Assurez-vous de configurer les notifications pertinentes et de surveiller régulièrement l'interface graphique et la CLI de NetScaler.

REMARQUE :

Nous avons l'intention d'apporter des améliorations continues aux notifications et de maintenir cette documentation à jour en conséquence.

Pour NetScaler Console sur site, LAS fournit le blob d'activation LAS à NetScaler Console sur site connecté au cloud. Le blob est valide pendant 30 jours ou jusqu'à l'expiration du droit de licence, selon la première éventualité, et est actualisé chaque jour. Si la connectivité entre NetScaler Console sur site et le service NetScaler Console est interrompue, NetScaler Console sur site ne peut pas actualiser son blob d'activation LAS.

La section Surveiller l'expiration du blob d'activation LAS de Console sur site détaille la notification déclenchée lorsque le blob d'activation LAS de Console sur site est à moins de 30 jours de son expiration. Si cela se produit, votre connexion cloud nécessite une attention immédiate. Pour

© 1997–2026 Citrix Systems, Inc. All rights reserved.

résoudre ce problème, exécutez l'outil de diagnostic de connexion cloud pour réparer les problèmes identifiés, ou contactez le support Citrix pour obtenir de l'aide.

Une fois que NetScaler Console sur site a obtenu son blob d'activation LAS, il est autorisé à émettre des blobs d'activation pour toutes les instances NetScaler nécessitant une licence via NetScaler Console sur site. NetScaler Console sur site ne peut le faire que tant que son propre blob d'activation LAS reste valide. Il émet des blobs d'activation LAS aux instances NetScaler avec une période de validité de 30 jours (ou jusqu'à l'expiration de son propre blob, selon la première éventualité).

Si la connectivité entre NetScaler et NetScaler Console sur site est perdue :

- La Console ne peut pas actualiser le blob d'activation LAS de l'instance NetScaler.
- La Console tente de rétablir la connexion toutes les huit heures.
- Après trois tentatives infructueuses (24 heures au total), le NetScaler passe en statut 'de grâce', ce qui est reflété dans l'interface utilisateur de la Console.

La section (#monitor-netscaler-instances-las-activation-blob-expiry-netscaler-licensed-through-console-on-premises-cloud-connected) détaille les notifications concernant le blob d'activation LAS qui approche de sa date d'expiration (moins de 30 jours). Si cela se produit, votre connexion au cloud nécessite une attention immédiate. Pour résoudre ce problème, exécutez l'outil de diagnostic de connexion au cloud pour réparer les problèmes identifiés, ou contactez le support Citrix pour obtenir de l'aide.

Surveiller l'expiration du blob d'activation LAS de Console sur site

Surveiller la dernière date de renouvellement à l'aide de l'interface graphique

Pour surveiller la dernière date de renouvellement ou d'activation, accédez à Console sur site GUI > NetScaler Licensing > License Management > LAS.

Le renouvellement/l'actualisation a lieu quotidiennement. Si la dernière date de renouvellement/d'activation date de plus de quelques jours, cela indique un problème de connectivité ou d'activation.



Notifications

Bannière sur l'interface graphique de NetScaler Console sur site :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lorsque NetScaler Console sur site ne parvient pas à actualiser le blob d'activation LAS, une bannière d'avertissement apparaît dans l'interface graphique de NetScaler Console, comme illustré dans l'image suivante.



Notifications basées sur les événements système pour les problèmes de connexion au cloud :

NetScaler Console génère des événements pour les changements d'état de la connexion au cloud. Ces événements se déclenchent lorsque l'état de la connexion entre NetScaler Console sur site et le service Console change, y compris les transitions :

- De Connecté à Déconnecté ou Erreur
- De Déconnecté ou Erreurs à nouveau à Connecté

Pour afficher ces événements, accédez à **Console sur site GUI > Settings > System Events**.



Vous pouvez également configurer des notifications par e-mail pour les problèmes liés à la connexion au cloud.

1. Accédez à **Console on-premises GUI > Settings > Event notifications**.
2. Sélectionnez la catégorie **CloudConnectStatus**.
3. Sélectionnez et configurez une ou plusieurs formes de notifications, telles que l'e-mail, les SMS, PagerDuty.
4. Cliquez sur **Enregistrer**.



Notification basée sur les événements système pour l'expiration du blob d'activation LAS de Console on-premises :

NetScaler Console on-premises génère des événements pour informer les administrateurs de l'expiration du blob d'activation LAS pour NetScaler Console on-premises. Vous pouvez également configurer des alertes par e-mail pour ces événements.

Pour configurer les notifications d'expiration du blob d'activation LAS :

1. Accédez à **Console on-premises GUI > Settings > Event notifications**.
2. Sélectionnez les catégories **Licenses and License Pool**.
3. Sélectionnez et configurez une ou plusieurs formes de notifications, telles que l'e-mail, les SMS, PagerDuty.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez sur **Enregistrer**.

REMARQUE :

La liste des événements configurés peut en inclure plus que ces deux, en fonction de vos autres cas d'utilisation et des notifications configurées. La capture d'écran ne représente que ces deux-là par souci de simplicité.

Surveiller l'expiration du blob d'activation LAS des instances NetScaler (NetScaler sous licence via Console sur site connectée au cloud)

Afficher les instances NetScaler à l'aide de l'interface graphique :

Pour afficher les instances NetScaler en état de grâce, accédez à **Console sur site GUI > NetScaler Licensing > Flexed Licensing > Dashboard**

Afficher l'état de l'instance NetScaler à l'aide de la CLI

Pour afficher les instances NetScaler en état de grâce et la durée restante de la période de grâce, exécutez la commande `sh licenseserver`.

Exemple :

```
> sh licenseserver

     License Server: 10.102.123.31 Status: Disconnected

        Grace: Yes         Grace Time Left: 652

Done
```

Notifications

Bannière sur NetScaler Console sur site :

L'interface graphique de NetScaler Console sur site affiche une bannière répertoriant les instances NetScaler dont le blob d'activation LAS expire dans x jours, où x est inférieur à 30 jours.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bannière sur l'interface graphique de NetScaler :

L'interface graphique de NetScaler Console sur site affiche une bannière si l'instance NetScaler est en état de grâce.

Notification basée sur les événements système :

NetScaler Console on-premises génère des événements lorsque le blob d'activation LAS expire pour les instances NetScaler. Vous pouvez également configurer des alertes par e-mail pour ces événements.

Pour configurer les notifications d'expiration du blob d'activation LAS :

1. Accédez à **Console on-premises GUI > Settings > Event notifications**.
2. Sélectionnez les catégories **Licenses and License Pool**.
3. Sélectionnez et configurez une ou plusieurs formes de notifications, telles que l'e-mail, les SMS, PagerDuty.
4. Cliquez sur Enregistrer.

Traps SNMP générés par NetScaler pour l'état de grâce :

Si les instances NetScaler sont en état de grâce, NetScaler génère les traps SNMP suivants :

- pooledLicenseGraceStarted : Déclenché lorsque l'instance est entrée dans la période de grâce.
- pooledLicenseGraceNormal : Déclenché si NetScaler a été en période de grâce pendant 30 jours et que la période de grâce est terminée, ce qui signifie que le déploiement est affecté ou devient sans licence.
- pooledLicenseGracePeriodOver : Déclenché lorsque la période de grâce est terminée.

Exemple :

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceStarted
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceNormal
(nsPartitionName = default)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGracePeriodOver
(nsPartitionName = default)
```

Surveiller l'expiration des droits de licence

La **date d'expiration de l'abonnement de licence** désigne la date d'expiration de l'abonnement ou du contrat de licence du client.

Pour afficher les informations d'expiration de l'abonnement de licence à l'aide de l'interface graphique, accédez à **Console Service GUI > NetScaler Licensing > License Management > LAS**.

La section **Jours avant expiration** affiche la date d'expiration de l'abonnement pour la licence correspondante.

Notifications

Bannière de l'interface graphique du service NetScaler Console :

L'interface graphique du service NetScaler Console affiche une bannière indiquant que l'abonnement de licence approche de son expiration dans x jours.



Notifications par e-mail

Pour configurer les notifications par e-mail :

1. Accédez à **Console Service GUI > NetScaler Licensing > License Management > Notification Settings**.
2. Saisissez la valeur requise dans **Combien de jours avant l'expiration de la licence souhaitez-vous recevoir une notification ?**.
3. Cliquez sur **Enregistrer**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion des licences

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licence (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x et ultérieures. Cependant, les licences basées sur des fichiers sont obsolètes à compter du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou la version 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site, et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge par le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

REMARQUE :

Lorsque vous achetez une licence Universal Hybrid Multi-Cloud (UHMC) ou une licence Citrix Platform (CPL), les licences NetScaler livrées sont appelées licences Flexed.

Les licences Flexed sont prises en charge dans les versions 14.1 et 13.1 de NetScaler Console sur site. Pour une meilleure expérience produit présentant l'interface graphique Flexed et offrant un droit groupé, nous vous recommandons de mettre à niveau votre NetScaler Console sur site vers la version 14.1–12.34 ou ultérieure.

Dans la version 14.1–12.34 et ultérieure de NetScaler Console sur site :

- Vous pouvez gérer les licences Flexed via l'interface utilisateur du tableau de bord Flexed (NetScaler® **Licensing > Flexed Licensing)**.
- Le droit groupé de VIP NetScaler Console illimités pour l'analyse est disponible si vous appliquez des licences Flexed.

Pour les versions 13.1 et les builds 14.1 antérieures à 14.1-12.34 de NetScaler Console sur site :

- Lorsque vous appliquez des licences Flexed, NetScaler Console les traite de la même manière que les licences en pool et affiche les détails dans l'interface utilisateur du tableau de bord en pool (**Infrastructure > Pooled Licensing**).
- Lorsque la licence Flexed est appliquée, le droit groupé de VIP NetScaler Console illimités pour l'analyse n'est pas disponible dans ces versions.-

Licence basée sur LAS

Vos droits apparaissent dans la section **Console UI > License Management > License Activation Service (LAS)** après avoir activé LAS.



Ports du serveur de licences

Le LAS utilise le port 443 pour toutes les communications de licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour utiliser LAS, ajoutez votre instance NetScaler® en tant qu'instance gérée.

Informations sur l'expiration des licences

Afficher l'expiration de la licence

1. Accédez à **Licences NetScaler > Gestion des licences**.
2. La section **Informations sur l'expiration des droits de licence** fournit des détails sur les licences approchant de l'expiration.
    - **Fonctionnalité** : Type de licence qui va expirer.
    - **Nombre** : Nombre d'instances ou de bande passante (en Mbps) affectées.
    - **Jours avant expiration** : Nombre de jours avant l'expiration de la licence (date de fin de contrat).

Une fois que vous avez activé les LA et établi une connexion cloud, les droits initiaux pour les licences groupées ou flexibles sont récupérés dans l'heure. Toutes les licences groupées ou flexibles nouvelles ou renouvelées ultérieures sont récupérées dans les 24 heures.

Comportement d'expiration de la licence

Lorsqu'une licence gérée via NetScaler Console expire, l'instance NetScaler associée cesse de traiter le trafic et sa configuration peut être perdue.

E-mail de notification et bannière contextuelle concernant la date de fin de licence (date de fin de contrat de licence)

Dans l'interface graphique de NetScaler Console, un message contextuel apparaît concernant la date de fin de licence. Par défaut, un message contextuel s'affiche dans l'interface graphique (à chaque connexion) à partir de 30 jours (par défaut) avant la date de fin de licence. Vous pouvez configurer le nombre de jours dans **Paramètres de notification > Paramètre d'expiration de licence.**

En tant qu'administrateur, vous recevez également un e-mail de notification pour la date de fin de licence si la notification par e-mail est configurée dans les **Paramètres de notifications**. Un e-mail de notification est envoyé à une fréquence de 30, 20 et 10 jours avant la date de fin de licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Paramètres de notifications

Pour configurer les notifications pour les licences flexibles ou groupées gérées par LAS qui expirent, suivez ces étapes :

1. Accédez à NetScaler **Licences > Gestion des licences > Paramètres de notification**.
2. Dans la section Paramètres de notification, sélectionnez **Me notifier** sur l'utilisation des licences. Définissez le seuil d'alerte en pourcentage de la capacité de licence flexible ou groupée à allouer pour envoyer une notification.
3. Choisissez le type de notification que vous souhaitez envoyer lorsque les licences atteignent le seuil ou sont sur le point d'expirer en cochant la case appropriée. Les types de notification sont les suivants.
    - **E-mail** : Profil de messagerie ou liste de distribution pour l'envoi de notifications. Pour plus d'informations, consultez Créer une liste de distribution de messagerie.
    - **Slack** : Détails du profil Slack pour l'envoi de notifications.
    - **PagerDuty** : Profil PagerDuty pour l'envoi de notifications.
    - **ServiceNow** : Le profil Citrix ServiceNow est spécifié par défaut et est la seule option disponible. Pour plus d'informations sur la création de ces profils, consultez Configurer les notifications.
4. Sélectionnez un type de notification et cliquez sur **Ajouter** pour ajouter des détails. Vous pouvez également tester chaque système de notification avant d'enregistrer vos paramètres.
5. Spécifiez les Jours avant expiration, qui est le nombre de jours avant lequel vous souhaitez être informé de l'expiration de la licence.
6. Cliquez sur **Enregistrer**.

Créer une liste de distribution de messagerie

Procédez comme suit pour créer une liste de distribution de messagerie :

1. Sélectionnez **E-mail** et cliquez sur **Ajouter**.
2. Dans **Créer une liste de distribution de messagerie**, spécifiez les détails suivants :
    - **Nom** - Spécifiez le nom de la liste de distribution.
    - **Serveur de messagerie** - Sélectionnez le serveur de messagerie qui envoie la notification par e-mail. Pour ajouter un serveur de messagerie, cliquez sur Ajouter. Spécifiez le nom du serveur/l'adresse IP et le port. Sélectionnez Authentification pour exiger une authentification

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pour accéder au serveur de messagerie. Sélectionnez Sécurisé si le serveur de messagerie prend en charge l'authentification SSL. Cliquez sur Créer.

- **De** - Spécifiez l'adresse e-mail à partir de laquelle NetScaler Console envoie le message.
- **À** - Spécifiez les adresses e-mail auxquelles NetScaler Console envoie le message.
- **Cc** - Spécifiez les adresses e-mail auxquelles NetScaler Console envoie une copie du message.
- **Cci** - Spécifiez les adresses e-mail auxquelles NetScaler Console envoie une copie conforme invisible (n'affiche pas l'adresse e-mail) du message.
- Cliquez sur **Créer**.

Créer un profil Slack

Procédez comme suit pour créer un profil Slack :

1. Dans Slack, cliquez sur **Ajouter**.
2. Dans **Créer un profil Slack**, spécifiez les détails suivants :

   - **Notifications** - Lorsqu'elle est activée, envoie des alertes et des notifications d'événements directement à un canal Slack désigné.
   - **Notifications avec pièces jointes** - Lorsqu'elle est activée, des informations détaillées sur les alertes et les événements déclenchés sont envoyées sous forme de pièce jointe à un e-mail ou de charge utile JSON dans un webhook.
   - **Nom du profil** - Spécifiez le nom du profil. Ce nom apparaît dans la liste des profils Slack.
   - **Nom du canal** - Spécifiez le nom du canal Slack auquel NetScaler Console envoie la notification.
   - **URL du webhook** - Spécifiez l'URL du webhook du canal. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom du canal. Toutes les notifications d'événements envoyées à cette URL sont publiées sur le canal Slack désigné. Voici un exemple de webhook : `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

Créer un profil PagerDuty

PagerDuty vous permet de configurer des notifications par e-mail, des notifications push et des appels téléphoniques sur un numéro enregistré. Avant d'ajouter un profil PagerDuty dans NetScaler Console, assurez-vous d'avoir effectué les configurations requises dans PagerDuty. Pour commencer avec PagerDuty, consultez la documentation PagerDuty.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Effectuez les étapes suivantes pour créer un profil PagerDuty :

1. Dans PagerDuty, cliquez sur **Ajouter**.
2. Dans **Créer un profil PagerDuty**, spécifiez les détails suivants :
    - **Nom du profil** - Spécifiez un nom de profil. Ce nom est utilisé par différents modules, tels que les règles d'événement et les notifications SSL, pour envoyer des alertes PagerDuty.
    - **Clé d'intégration** - Spécifiez la clé d'intégration. Vous pouvez obtenir cette clé depuis votre portail PagerDuty. Lors de la création d'un service dans PagerDuty pour l'intégration, utilisez l'option **Intégration d'API d'événements génériques**.
    - Cliquez sur **Créer**.

Pour plus d'informations, consultez Services et intégrations dans la documentation PagerDuty.

Afficher le profil ServiceNow

Pour activer les notifications ServiceNow pour les événements NetScaler, vous devez intégrer NetScaler Console à ServiceNow à l'aide du connecteur ITSM.

Pour plus d'informations, consultez Intégrer NetScaler Console à l'instance ServiceNow.

Effectuez les étapes suivantes pour afficher et vérifier le profil ServiceNow :

1. Dans **ServiceNow**, le profil **Citrix_Workspace_SN** est sélectionné par défaut.
2. Cliquez sur **Tester** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

REMARQUE :

Pour plus d'informations sur les différents types de licences NetScaler, consultez Présentation des licences.

Prise en charge RBAC pour LAS

Vous pouvez utiliser le contrôle d'accès basé sur les rôles (RBAC) pour gérer l'accès aux applications LAS avec les niveaux de contrôle suivants :

- **Niveau de fonctionnalité** : Restreindre la visibilité de la fonctionnalité de licence pour des administrateurs spécifiques.
- **Niveau d'instance** : Limiter les administrateurs autorisés à appliquer des licences uniquement aux instances NetScaler sélectionnées.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus de détails sur la configuration, consultez Contrôle d'accès basé sur les rôles.

Droits gérés manuellement (licences basées sur des fichiers)

Les sections suivantes s'appliquent aux droits gérés manuellement (licences basées sur des fichiers).

Fichiers de licence

La licence NetScaler Flexed inclut les fichiers suivants que vous devez télécharger depuis le portail MyCitrix. Pour plus d'informations sur la transition de votre type de licence NetScaler actuel vers la licence Flexed, consultez Transition vers la licence Flexed.

Les fichiers de licence présents sur votre NetScaler sont répertoriés dans cette section.

LE NOM DU FICHIER CONTIENT	DESCRIPTION	INFORMATIONS DE TÉLÉCHARGEMENT	OÙ TÉLÉCHARGER/ APPLIQUER LA LICENCE
Instance logicielle NetScaler Flexed VPX	Vous donne droit à des instances logicielles VPX/CPX/ BLX	Téléchargez ce fichier à l'aide de l'ID d'hôte de votre NetScaler Console	Sur NetScaler Console
Instance logicielle NetScaler Flexed MPX	Vous donne droit à des instances logicielles MPX	Téléchargez ce fichier à l'aide de l'ID d'hôte de votre NetScaler Console	Sur NetScaler Console
Instance logicielle NetScaler Flexed SDX	Vous donne droit à des instances logicielles SDX	Téléchargez ce fichier à l'aide de l'ID d'hôte de votre NetScaler Console	Sur NetScaler Console
Bande passante NetScaler Flexed Platinum	Vous donne droit à une capacité de débit Flexed Platinum	Téléchargez ce fichier à l'aide de l'ID d'hôte de votre NetScaler Console	Sur NetScaler Console
Instance logicielle NetScaler Flexed VPX FIPS	Vous donne droit à des instances logicielles VPX FIPS	Téléchargez ce fichier à l'aide de l'ID d'hôte de votre NetScaler Console	Sur NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LE NOM DU FICHIER CONTIENT	DESCRIPTION	INFORMATIONS DE TÉLÉCHARGEMENT	OÙ TÉLÉCHARGER/ APPLIQUER LA LICENCE
Licence de plate-forme MPX-Z à capacité zéro	Vous donne le droit de faire participer votre NetScaler MPX HW/NetScaler MPX FIPS HW à la licence Flexed	Téléchargez ce fichier	Sur NetScaler MPX
Licence de plate-forme SDX-Z à capacité zéro	Vous donne le droit de faire participer votre NetScaler SDX HW/NetScaler SDX FIPS HW à la licence Flexed	Téléchargez ce fichier	Sur NetScaler SDX

Points importants à noter

1. Si vous êtes un client de licences groupées (Pooled licensing) passant à la licence Flexed et que votre matériel MPX et SDX dispose déjà de licences perpétuelles Z-Cap, vous n'avez pas besoin d'appliquer les licences Z-Cap reçues avec Flexed. Cependant, si les licences Z-Cap actuelles appliquées sur NetScaler MPX/NetScaler SDX sont valides pour une période spécifique, vous devez appliquer les licences Z-Cap reçues avec la licence Flexed. La licence logicielle Flexed comprend l'instance logicielle NetScaler Flexed MPX/SDX/VPX/VPX FIPS et les licences de bande passante NetScaler Flexed Platinum.
2. Vous devez appliquer les licences Flexed sur NetScaler Console pour le facteur de forme NetScaler que vous utilisez dans votre déploiement. Par exemple :

   Appliquez les licences suivantes si vous utilisez le facteur de forme NetScaler SDX :

   |Fichier de licence|Appliquer sur| |-|-| |Instance logicielle NetScaler Flexed SDX|NetScaler Console| |Instance logicielle NetScaler Flexed VPX|NetScaler Console| |Bande passante NetScaler Flexed Platinum|NetScaler Console| |Plateforme ADC Zero Capacity SDX-Z| NetScaler SDX|

   Appliquez les licences suivantes si vous utilisez le facteur de forme NetScaler MPX :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

|Fichier de licence|Appliquer sur| |-|-| |Instance logicielle NetScaler MPX Flex|NetScaler Console| |Bande passante NetScaler Platinum Flex|NetScaler Console| |Plateforme ADC MPX-Z à capacité zéro|NetScaler MPX|

Appliquez les licences suivantes si vous utilisez le facteur de forme NetScaler VPX, NetScaler BLX ou NetScaler CPX :

|Fichier de licence|Appliquer sur| |-|-| |Instance logicielle NetScaler VPX Flex|NetScaler Console| |Bande passante NetScaler Platinum Flex|NetScaler Console|

Appliquez les licences suivantes si vous utilisez le facteur de forme NetScaler VPX FIPS

|Fichier de licence|Appliquer sur| |-|-| |Instance logicielle NetScaler Flexed VPX FIPS|NetScaler Console| |Bande passante Platinum Flexed NetScaler|NetScaler Console|

Appliquer un fichier de licence

Vous pouvez ajouter, supprimer et télécharger des licences. Vous devez appliquer les licences avant de pouvoir les utiliser.

1. Accédez à **NetScaler Licensing > License Management**.
2. Dans la section **Fichiers de licence**, cliquez sur **Ajouter un fichier de licence** et sélectionnez l'une des options suivantes :
   - **Télécharger les fichiers de licence depuis un ordinateur local** : Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger vers NetScaler Console.
   - **Utiliser le code d'accès à la licence** : Spécifiez le code d'accès à la licence que vous avez achetée auprès de Citrix. Cliquez sur **Obtenir les licences**, puis sur **Terminer**.
3. Cliquez sur **Terminer**. Les fichiers de licence sont ajoutés à NetScaler Console. La section **Informations sur l'expiration de la licence** répertorie les licences présentes dans NetScaler Console, leur nombre et les jours restants avant l'expiration.

   La capture d'écran suivante montre le nombre de licences d'instance logicielle Flexed NetScaler VPX, NetScaler MPX, NetScaler SDX et NetScaler VPX FIPS, la capacité de bande passante premium Flexed présente et les jours restants avant l'expiration (date de fin de contrat).

   

   La capture d'écran suivante montre la bande passante mutualisée Standard, Advanced et Premium disponible et les jours restants avant l'expiration (date de fin de contrat).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Expiration de la licence groupée(/en-us/netscaler-application-delivery-management-software/media/pooled-license-expiry.png)

4. Sélectionnez un fichier de licence et cliquez sur **Appliquer les licences**.

Supprimer un fichier de licence

Pour supprimer un fichier de licence, sélectionnez un ou plusieurs fichiers et cliquez sur **Supprimer**. Lorsque vous supprimez une licence, vous devez d'abord l'ajouter, et ce n'est qu'ensuite que vous pouvez l'appliquer.

Télécharger un fichier de licence

Pour télécharger un fichier de licence, sélectionnez un fichier et cliquez sur **Télécharger**. Vous pouvez enregistrer le fichier de licence hors ligne comme sauvegarde.

Paramètres de port du serveur de licences

Les ports sont utilisés par les instances NetScaler pour communiquer avec le serveur de licences. Cliquez sur l'icône **Modifier** et spécifiez les valeurs des paramètres suivants :

- **Port du serveur de licences** : Port du serveur proxy utilisé par les instances NetScaler pour accéder au portail de licences Citrix pour l'allocation de licences. Valeur par défaut : 27000.
- **Port du démon du fournisseur** : Port du serveur de licences utilisé par les instances NetScaler pour communiquer avec le serveur de licences. Valeur par défaut : 7279.
- **Port du serveur proxy** : NetScaler Console peut être utilisé comme proxy HTTP avant pour les instances NetScaler afin d'accéder au portail MyCitrix pour la récupération automatisée des licences. Pour activer cette fonctionnalité, spécifiez un port TCP sur lequel le proxy écoute.

Informations sur l'expiration de la licence

Vous pouvez désormais configurer le seuil d'expiration de la licence pour les licences de capacité Flexed ou Pooled. Lorsque le seuil est défini, NetScaler Console envoie des notifications par e-mail ou SMS lorsqu'une licence est sur le point d'expirer. Un piège SNMP et une notification sont également envoyés lorsque la licence a expiré sur NetScaler Console.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée, et cet événement peut être consulté sur NetScaler Console à partir de **Infrastructure > Événements**.

Afficher l'expiration de la licence

1. Accédez à **NetScaler Licensing > License Management**.
2. Dans la page **License Settings**, sous la section **License Expiry Information**, vous trouverez les détails des licences qui vont expirer :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Feature** : Type de licence qui va expirer.
- **Count** : Nombre de serveurs virtuels ou d'instances concernés.
- **Days to expiry** : Nombre de jours avant l'expiration de la licence (date de fin de contrat).

REMARQUE :

Lorsque vous ajoutez de nouvelles licences au pool, les instances NetScaler utilisent les nouvelles licences à l'expiration de leurs licences existantes.

Paramètres de notification

Spécifiez les paramètres en fonction desquels des notifications seront envoyées concernant l'allocation des licences et les jours restants avant leur expiration.

1. Dans la section **Notification Settings**, cliquez sur l'icône **Edit** et sélectionnez **Notify me on license usage**. Définissez le seuil d'alerte en pourcentage de la capacité de licence Flexed ou Pooled à allouer pour envoyer une notification.
2. Choisissez le type de notification que vous souhaitez envoyer lorsque les licences atteignent le seuil ou sont sur le point d'expirer en cochant la case appropriée. Les types de notification sont les suivants. Sélectionnez un type de notification et cliquez sur **Add** pour ajouter des détails. Vous pouvez également tester que chaque notification est bien livrée avant d'enregistrer vos paramètres.

   - **Email** : Profil de messagerie ou liste de distribution pour l'envoi de notifications. Pour plus d'informations, consultez Créer une liste de distribution de messagerie.
   - **SMS** : Profil SMS ou liste de distribution pour l'envoi de notifications.
   - **Slack** : Détails du profil Slack pour l'envoi de notifications.
   - **PagerDuty** : Profil PagerDuty pour l'envoi de notifications.
   - **ServiceNow** : Le profil Citrix ServiceNow est spécifié par défaut et est la seule option disponible actuellement. Pour plus d'informations sur la création de ces profils, consultez Configurer les notifications
3. Spécifiez les Jours avant expiration, qui est le nombre de jours avant lequel vous souhaitez être averti de l'expiration de la licence.
4. Cliquez sur **Enregistrer**.

Créer une liste de distribution de courriels

Effectuez les étapes suivantes pour créer une liste de distribution de courriels :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Sélectionnez **E-mail** et cliquez sur **Ajouter**.
2. Dans **Créer une liste de distribution de courriels**, spécifiez les détails suivants :
   - **Nom** - Spécifiez le nom de la liste de distribution.
   - **Serveur de messagerie** - Sélectionnez le serveur de messagerie qui envoie une notification par e-mail. Pour ajouter un serveur de messagerie, cliquez sur Ajouter. Spécifiez le nom du serveur/l'adresse IP et le port. Sélectionnez Authentification pour exiger l'authentification pour accéder au serveur de messagerie. Sélectionnez Sécurisé si le serveur de messagerie prend en charge l'authentification SSL. Cliquez sur Créer.
   - **De** - Spécifiez l'adresse e-mail à partir de laquelle NetScaler Console envoie le message.
   - **À** - Spécifiez les adresses e-mail auxquelles NetScaler Console envoie le message.
   - **Cc** - Spécifiez les adresses e-mail auxquelles NetScaler Console copie le message.
   - **Bcc** - Spécifiez les adresses e-mail auxquelles NetScaler Console envoie une copie carbone invisible (n'affiche pas l'adresse e-mail) du message.
3. Cliquez sur **Créer**.

Créer une liste de distribution SMS

Effectuez les étapes suivantes pour configurer les paramètres de notification SMS :

1. Dans **SMS**, cliquez sur **Ajouter**.
2. Dans **Créer une liste de distribution SMS**, spécifiez les détails suivants :
   - **Nom** - Spécifiez le nom de la liste de distribution.
   - **Serveur SMS** - Sélectionnez le serveur SMS qui envoie les notifications SMS. Pour ajouter un serveur SMS, cliquez sur **Ajouter**. Spécifiez les détails du serveur et cliquez sur **Créer**.
   - **À** - Spécifiez le numéro de téléphone auquel la console NetScaler envoie le message.
3. Cliquez sur **Créer**.

Créer un profil Slack

Effectuez les étapes suivantes pour créer un profil Slack :

1. Dans **Slack**, cliquez sur **Ajouter**.
2. Dans **Créer un profil Slack**, spécifiez les détails suivants :
   - **Nom du profil** - Spécifiez le nom du profil. Ce nom apparaît dans la liste des profils Slack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Nom du canal** - Spécifiez le nom du canal Slack auquel la console NetScaler envoie la notification.
- **URL du webhook** - Spécifiez l'URL du webhook du canal. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom du canal. Toutes les notifications d'événements envoyées à cette URL sont publiées sur le canal Slack désigné. Voici un exemple de webhook : `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`.

Créer un profil PagerDuty

PagerDuty vous permet de configurer des notifications par e-mail, SMS, notifications push et appels téléphoniques sur un numéro enregistré. Avant d'ajouter un profil PagerDuty dans NetScaler Console, assurez-vous d'avoir effectué les configurations requises dans PagerDuty. Pour commencer avec PagerDuty, consultez la documentation PagerDuty.

Effectuez les étapes suivantes pour créer un profil PagerDuty :

1. Dans **PagerDuty**, cliquez sur **Ajouter**.
2. Dans **Créer un profil PagerDuty**, spécifiez les détails suivants :
   - **Nom du profil** - Spécifiez un nom de profil. Ce nom est utilisé par différents modules, tels que les règles d'événement et les notifications SSL, pour envoyer des alertes PagerDuty.
   - **Clé d'intégration** - Spécifiez la clé d'intégration. Vous pouvez obtenir cette clé depuis votre portail PagerDuty.
3. Cliquez sur **Créer**.

Pour plus d'informations, consultez Services et intégrations dans la documentation PagerDuty.

Afficher le profil ServiceNow

Pour activer les notifications ServiceNow pour les événements NetScaler et les événements NetScaler Console, vous devez intégrer NetScaler Console à ServiceNow à l'aide du connecteur ITSM. Pour plus d'informations, consultez Intégrer NetScaler Console à l'instance ServiceNow.

Effectuez les étapes suivantes pour afficher et vérifier le profil ServiceNow :

1. Dans **ServiceNow**, le profil **Citrix_Workspace_SN** est sélectionné par défaut.
2. Cliquez sur **Tester** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Pour plus d'informations sur les différents types de licences NetScaler, consultez Présentation des licences.

Capacité minimale et maximale pour les licences Flexed et Pooled

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADCs : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : Le support LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à partir du April 15 2026 pour les versions Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version Console sur site 14.1-51.x ou la version 13.1-60.x ou ultérieure, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au April 15 2026. Cependant, vous devez effectuer une mise à niveau vers la version Console sur site 14.1-51.x ou ultérieure, et passer au LAS avant le April 15 2026 car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des

© 1997–2026 Citrix Systems, Inc. All rights reserved.

licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou les réglementations l'interdisent.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
La licence NetScaler Flexed utilise la console NetScaler configurée comme serveur de licences pour gérer les licences Flexed : licences de pool de bande passante et licences de pool d'instances.

Lors de l'extraction de licences à partir du pool de bande passante et d'instances, le facteur de forme NetScaler et le numéro de modèle matériel sur un matériel à capacité zéro déterminent :

- La bande passante minimale et le nombre d'instances qu'une instance NetScaler doit extraire avant d'être fonctionnelle.
- La bande passante maximale et le nombre d'instances qu'un NetScaler peut emprunter.
- L'unité minimale de bande passante pour chaque emprunt. C'est la plus petite unité que NetScaler peut emprunter d'un pool. Tout emprunt doit être un multiple entier de cette unité. Par exemple, si l'unité minimale de bande passante d'un NetScaler est de 1 Gbit/s, 1000 Mbit/s peuvent être empruntés, mais pas 200 Mbit/s ou 150,5 Gbit/s. L'unité minimale de bande passante est différente de l'exigence de bande passante minimale. Une instance NetScaler ne peut fonctionner qu'après avoir été licenciée avec au moins la bande passante minimale. Une fois la bande passante minimale atteinte, l'instance peut emprunter plus de bande passante par multiples de l'unité minimale de bande passante.

Les tableaux 1 à 5 récapitulent la bande passante/les instances maximales, la bande passante/les instances minimales et l'unité de bande passante minimale pour toutes les instances NetScaler prises en charge. Le tableau 6 récapitule les exigences de licence pour différents facteurs de forme pour toutes les instances NetScaler prises en charge. Les tableaux suivants font référence aux exigences système.

REMARQUE :

L'unité d'emprunt de bande passante minimale pour NetScaler CPX/BLX/VPX est de 10 Mbit/s. L'unité d'emprunt de bande passante minimale pour NetScaler MPX/SDX est de 1 Gbit/s.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau 1. Capacité Flexed prise en charge pour MPX

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	UNITÉ DE BANDE PASSANTE MINIMALE
MPX 5900Z	1	10	1 Gbit/s
MPX 8900Z	5	30	1 Gbit/s
MPX 8900Z FIPS	5	20	1 Gbit/s
MPX 9100Z	10	95	1 Gbit/s
MPX 9200	10	95	1 Gbit/s
MPX 9100Z FIPS	10	95	1 Gbps
MPX 14000Z	20	100	1 Gbps
MPX 14000Z-40G	20	100	1 Gbps
MPX 14000Z-40S	40	100	1 Gbit/s
MPX 14000Z FIPS	30	80	1 Gbit/s
MPX 15000Z	20	120	1 Gbit/s
MPX 15000Z-50G	20	120	1 Gbit/s
MPX 15000Z FIPS	30	120	1 Gbps
MPX 16000Z	30	250	1 Gbps
MPX 22000Z	40	120	1 Gbps
MPX 24000Z	100	150	1 Gbps
MPX 25000Z	100	160	1 Gbit/s
MPX 25000Z-40G	100	200	1 Gbit/s
MPX 26000Z	100	200	1 Gbit/s
MPX 26000Z-50S	100	200	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	UNITÉ DE BANDE PASSANTE MINIMALE
MPX 26000Z-100G	100	200	1 Gbit/s

Tableau 2A. Capacité Flexed prise en charge pour NetScaler SDX version antérieure à la build 13.0-47.x

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 8900Z	10	30	2	7	1 Gbps
SDX 14000Z	20	100	5	25	1 Gbps
SDX 14000Z-40G	40	100	20	25	1 Gbps
SDX 15000Z	20	120	5	55	1 Gbit/s
SDX 15000Z-50G	20	120	5	55	1 Gbit/s
SDX 22000Z	40	120	80	80	1 Gbit/s
SDX 24000Z	100	150	80	80	1 Gbit/s
SDX 25000Z	100	200	20	115	1 Gbit/s
SDX 25000Z-40G	100	200	20	115	1 Gbps
SDX 26000Z	100	200	20	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 26000Z-50S	100	200	20	115	1 Gbit/s
SDX 26000Z-100G	100	200	20	115	1 Gbit/s

Tableau 2B. Capacité Flexed prise en charge pour NetScaler SDX version 13 (build 13.0-47.x et versions ultérieures), version 13.1 (build antérieure à 51.x) et version 14.1 (build antérieure à 12.x)

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9100Z	10	95	2	7	1 Gbit/s
SDX 14000Z	10	100	2	25	1 Gbps
SDX 14000Z-40G	20	100	10	25	1 Gbps
SDX 15000Z	10	120	2	55	1 Gbps
SDX 15000Z-50G	10	120	2	55	1 Gbps
SDX 16000Z	15	250	10	55	1 Gbps
SDX 22000Z	20	120	40	80	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 24000Z	50	150	40	80	1 Gbit/s
SDX 25000Z	50	200	10	115	1 Gbit/s
SDX 25000Z-40G	50	200	10	115	1 Gbps
SDX 26000Z	50	200	10	115	1 Gbps
SDX 26000Z-50S	50	200	10	115	1 Gbit/s
SDX 26000Z-100G	50	200	10	115	1 Gbit/s

Tableau 2C. Capacité Flexed prise en charge pour NetScaler SDX version 13.1 (build 51.x et ultérieure) et version 14.1 (build 12.x et ultérieure)

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9200Z	10	95	1	7	1 Gbit/s
SDX 9100Z	10	95	1	7	1 Gbit/s
SDX 14000Z	10	100	1	25	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MINIMALE (GBIT/S)	BANDE PASSANTE MAXIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 14000Z-40G	20	100	1	25	1 Gbps
SDX 15000Z	10	120	1	55	1 Gbps
SDX 15000Z-50G	10	120	1	55	1 Gbps
SDX 16000Z	30	250	1	55	1 Gbit/s
SDX 17000Z	30	350	1	55	1 Gbit/s
SDX 22000Z	20	120	1	80	1 Gbit/s
SDX 24000Z	50	150	1	80	1 Gbit/s
SDX 25000Z	50	200	1	115	1 Gbit/s
SDX 25000Z-40G	50	200	1	115	1 Gbit/s
SDX 26000Z	50	200	1	115	1 Gbit/s
SDX 26000Z-50S	50	200	1	115	1 Gbit/s
SDX 26000Z-100G	50	200	1	115	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- La quantité d'achat minimale peut être différente de la configuration système minimale requise.
- Sur NetScaler SDX exécutant la version 14.1-12.x et ultérieure, avec une licence Flexed, la restriction de retirer un nombre minimum de licences d'instance est supprimée. Autrement dit, vous pouvez retirer un minimum d'une licence d'instance.

Tableau 3. Bande passante minimale/maximale et instances minimales/maximales prises en charge pour les instances NetScaler CPX

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (MBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
CPX	10	10	1	1	10 Mbps

Tableau 4. Bande passante minimale/maximale et instances minimales/maximales prises en charge pour les instances NetScaler VPX sur les hyperviseurs et les services cloud

HYPERVISEUR/ SERVICE CLOUD	BANDE PASSANTE MAXIMALE (GBPS)	BANDE PASSANTE MINIMALE (MBPS)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
Citrix Hypervisor	40 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
VMware ESXI	100 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Linux KVM	100 Gbit/s	10 Mbit/s	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HYPERVISEUR/ SERVICE CLOUD	BANDE PASSANTE MAXIMALE (GBPS)	BANDE PASSANTE MINIMALE (MBPS)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
Azure	10 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Google Cloud	10 Gbit/s	10 Mbit/s	1	1	10 Mbit/s

Remarque

La quantité d'achat minimale est différente de la configuration système minimale requise.

Tableau 5. Bande passante minimale/maximale prise en charge et instances minimales/maximales pour les instances NetScaler BLX

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBPS)	BANDE PASSANTE MINIMALE (MBPS)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
BLX	100	10	1	1	10 Mbps

Tableau 6. Exigence de licence de capacité zéro pour différents facteurs de forme

GAMME DE PRODUITS	MATÉRIEL À CAPACITÉ ZÉRO
MPX	Licence requise
SDX	Licence requise
VPX	-
CPX	-
BLX	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licence de capacité Flexed

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le Service d'activation de licence (LAS) est la technologie de nouvelle génération pour les activations de produits sur l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles avec LAS sont :

- NetScaler ADCs : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou la version 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
La licence NetScaler Flexed est le nouveau cadre de licences visant à simplifier le processus de gestion des licences. Votre licence Flexed inclut des licences d'instance logicielle (VPX/CPX/BLX, SDX, MPX et VPX FIPS) et des licences de capacité de bande passante.

Service d'activation de licence (LAS) – Activez LAS avec le déploiement Cloud Connect pour rendre vos droits Flexed visibles dans NetScaler Console sur site. Ensuite, allouez-les à n'importe quel facteur de forme NetScaler dans NetScaler Console sur site.

Droit géré manuellement (licence basée sur des fichiers) – Appliquez la licence Flexed directement sur NetScaler Console sur site. De plus, vous devez appliquer les licences MPX Z-Cap et SDX Z-Cap au matériel NetScaler MPX et NetScaler SDX respectif. Vous pouvez ensuite allouer ces droits à tous les facteurs de forme NetScaler, dans les déploiements cloud et sur site.

Une licence Flexed offre également des analyses pour un nombre illimité de serveurs virtuels.

Si vous possédez une licence Pooled et que vous avez maintenant acheté une licence Flexed, vous pouvez consulter les détails de votre licence dans le tableau de bord de la licence Flexed. La bande passante et les instances combinées apparaissent dans le tableau de bord de la licence Flexed.

La licence de bande passante inclut généralement uniquement l'édition Premium, sauf si vous aviez précédemment une licence Pooled Standard ou Advanced, auquel cas les éditions Standard, Advanced et Premium apparaissent dans le tableau de bord de la licence Flexed.

Pour plus de détails, consultez Tableau de bord de la licence Flexed.

Vous pouvez utiliser la licence Flexed pour maximiser l'utilisation de la bande passante en garantissant l'allocation de bande passante nécessaire à une instance, sans dépasser ses besoins. Augmentez ou diminuez la bande passante allouée à une instance en cours d'exécution sans affecter le trafic.

Matériel à capacité nulle

Lorsqu'elles sont gérées via la licence NetScaler® Flexed, les instances MPX et SDX sont appelées « matériel à capacité nulle » car ces instances ne peuvent pas fonctionner tant qu'elles n'ont pas extrait des ressources du pool de bande passante. Ainsi, ces plates-formes sont également appelées appliances MPX-Z et SDX-Z.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le matériel à capacité nulle nécessite une licence Z-cap pour extraire de la bande passante du pool commun.

REMARQUE :

- L'installation de la licence à capacité nulle fonctionne de la même manière que les autres licences locales NetScaler. Pour plus d'informations sur l'obtention et l'installation d'une licence à capacité nulle, consultez le Guide de gestion des licences pour NetScaler.

Gérer et installer les licences Z-cap

Vous devez installer une licence Z-cap manuellement, en utilisant le numéro de série du matériel ou le code d'accès à la licence. Une fois installée, une licence Z-cap est liée au matériel et ne peut pas être partagée entre les instances matérielles NetScaler à la demande. Cependant, vous pouvez déplacer manuellement la licence Z-cap vers une autre instance matérielle NetScaler.

Les instances NetScaler MPX exécutant la version logicielle NetScaler 11.1 build 54.14 ou ultérieure et les instances NetScaler SDX exécutant la version 11.1 build 58.13 ou ultérieure prennent en charge la licence NetScaler Flexed. Pour plus d'informations, consultez les tableaux 1 et 2 dans Capacité minimale et maximale pour les licences Flexed et Pooled.

REMARQUE :

Lorsque vous utilisez une licence basée sur LAS, vous n'avez pas besoin d'appliquer de licences Z-Cap.

Instances NetScaler VPX autonomes

Les instances NetScaler VPX exécutant la version logicielle NetScaler 11.1 Build 54.14 et ultérieure sur les hyperviseurs suivants prennent en charge les licences Flexed :

- VMware ESX 6.0
- Citrix Hypervisor™
- Linux KVM

Les instances NetScaler VPX exécutant la version logicielle NetScaler 12.0 Build 51.24 et ultérieure sur les hyperviseurs et plateformes cloud suivants prennent en charge les licences Flexed :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Les instances NetScaler VPX exécutant la version logicielle NetScaler 13.0 et 13.1 (toutes versions) sur les hyperviseurs et plateformes cloud suivants prennent en charge les licences Flexed :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

REMARQUE :

Pour permettre la communication entre NetScaler Console et Microsoft Azure ou AWS, un tunnel IPSEC doit être configuré. Pour plus d'informations, consultez Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler Console. Contrairement au matériel à capacité nulle, NetScaler VPX ne nécessite pas de licence à capacité nulle. Pour traiter le trafic, il doit extraire de la bande passante et une licence d'instance du pool.

Instances autonomes NetScaler CPX

Les instances NetScaler CPX déployées sur un hôte Docker prennent en charge la licence Flexed. Contrairement au matériel à capacité nulle, NetScaler CPX ne nécessite pas de licence Z-cap. Une seule instance NetScaler CPX consommant jusqu'à 1 Gbit/s de débit n'extrait qu'une seule instance et aucune bande passante du pool de licences. Par exemple, considérez que vous disposez de 20 instances NetScaler CPX avec un pool de bande passante de 20 Gbit/s. Si l'une des instances NetScaler CPX consomme un débit de 500 Mbit/s, le pool de bande passante reste de 20 Gbit/s pour les 19 instances NetScaler CPX restantes.

Si la même instance NetScaler CPX commence à consommer un débit de 1500 Mbit/s, le pool de bande passante dispose de 19,5 Gbit/s pour les 19 instances NetScaler CPX restantes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour la licence Flexed, vous ne pouvez ajouter de bande passante que par multiples de 10 Mbit/s.

Instances autonomes NetScaler BLX

Les instances NetScaler BLX prennent en charge la licence Flexed. Une instance NetScaler BLX ne nécessite pas de licence Z-cap. Pour traiter le trafic, une instance NetScaler BLX doit extraire de la bande passante et une licence d'instance du pool.

Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par les instances NetScaler, qu'elles soient physiques ou virtuelles. Le pool de bande passante comprend un pool pour l'édition logicielle Premium. Si vous passez d'une licence Pooled à une licence Flexed, vous pourriez trouver un mélange d'éditions logicielles Standard, Advanced et Premium. Une instance NetScaler MPX/VPX/CPX/BLX donnée ne peut pas avoir de bande passante extraite de différents pools simultanément. Le pool de bande passante à partir duquel elle peut extraire de la bande passante dépend de son édition logicielle pour laquelle elle est sous licence.

Pool d'instances

Il existe trois types de pools d'instances logicielles :

- Instance logicielle VPX/CPX/BLX
- Instance logicielle MPX (le même pool s'applique pour MPX FIPS)
- Instance logicielle SDX (le même pool s'applique pour SDX FIPS)
- Instance logicielle VPX FIPS

Lorsqu'une licence est extraite du pool, elle déverrouille les ressources de l'instance logicielle, y compris les CPU/PE, les cœurs SSL, les paquets par seconde et la bande passante.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer la licence

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits sur l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, ainsi que 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

REMARQUE :

Si vous disposez de licences groupées et que vous avez maintenant acheté et appliqué des licences Flexed, le droit combiné apparaît dans le tableau de bord des licences Flexed.

La licence NetScaler Flexed vous permet de partager la bande passante ou les licences d'instance entre différents facteurs de forme NetScaler. Utilisez cette capacité Flexed pour les instances qui se trouvent dans le centre de données ou les clouds publics. Lorsqu'une instance n'a plus besoin des ressources, elle restitue la capacité allouée au pool commun. Réutilisez la capacité libérée sur d'autres instances NetScaler qui ont besoin de ressources.

Vous pouvez utiliser la licence Flexed pour maximiser l'utilisation de la bande passante en garantissant l'allocation de bande passante nécessaire à une instance, sans dépasser ses besoins. Augmentez ou diminuez la bande passante allouée à une instance en cours d'exécution sans affecter le trafic.

Vous pouvez effectuer les tâches suivantes dans NetScaler Console :

- **Pour LAS :**
  a. Activez le service d'activation de licence (LAS) à l'aide de Cloud Connect.
  b. Une fois que les droits de licence apparaissent sur le serveur de licences sur site de la console, extrayez les licences pour les instances NetScaler.
  c. Assurez-vous que les licences sont basées sur la capacité minimale et maximale de chaque instance.
- **Pour les licences basées sur des fichiers :**
  a. Chargez vos licences Flexed, qui incluent des pools de bande passante et d'instances logicielles, sur le serveur de licences sur site de NetScaler Console.
  b. Chargez les licences à capacité zéro SDX ou MPX directement sur leur matériel respectif.
  c. Allouez des licences du pool de licences à vos instances NetScaler à la demande. Lors de l'extraction des licences, assurez-vous qu'elles sont basées sur la capacité minimale et maximale de l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez télécharger toutes les licences Flexed, y compris les licences de bande passante, d'instance et à capacité zéro (Z-cap), depuis le site web citrix.com. Pour plus d'informations, consultez le Guide de licences pour NetScaler®.

Licences basées sur LAS

Lorsque vous utilisez LAS, un agent externe est facultatif. Assurez-vous que le port 443 est disponible pour que les instances puissent extraire des licences de NetScaler Console. Pour plus d'informations, consultez les Exigences système.

Étape 1 : Activer LAS et récupérer les droits

1. Activez LAS à l'aide de **Cloud Connect**.

   Pour plus d'informations, consultez Activer le service d'activation de licence.

   Une fois activées, vos licences Flexed et Pooled apparaissent dans **License Management > LAS**.

   

   .

Étape 2 : Ajouter des instances NetScaler à NetScaler Console On-prem

Assurez-vous d'ajouter vos instances NetScaler à NetScaler Console On-prem afin qu'elles puissent recevoir des licences. Pour plus d'informations sur l'ajout d'instances, consultez Ajouter des instances NetScaler à NetScaler Console On-prem.

Étape 3 : Licencier ou migrer des instances NetScaler

1. Accédez à **Licensing management > LAS**.
2. Cliquez sur **License with LAS or Migrate to LAS**.

   Pour plus d'informations, consultez Service d'activation de licence.

Étape 4 : Modifier la capacité de débit flexible

Après avoir attribué une licence à une instance, modifiez sa capacité de débit allouée.

1. Accédez à **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. Sélectionnez l'onglet **LAS managed entitlements**.
3. Dans la section **Licensed NetScalers**, sélectionnez une instance et cliquez sur **Edit Throughput Capacity**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Saisissez la nouvelle capacité dans la colonne **Allouer** et cliquez sur **Soumettre**.

Licences spéciales pour les appliances MPX sans licence

Si le MPX sans licence est connecté à NetScaler Console sur site directement ou via un agent, les connexions HTTPS ne sont pas prises en charge. Par conséquent, l'étape 2 n'est pas réalisable. Naviguez plutôt vers le NetScaler pour effectuer les étapes suivantes.

Prérequis : Assurez-vous que l'authentification de base est activée sur votre NetScaler Console sur site si votre NetScaler MPX est connecté à NetScaler Console sur site directement (c'est-à-dire, sans agent). Après la configuration initiale (c'est-à-dire, après avoir géré et licencié votre NetScaler MPX dans NetScaler Console sur site), vous pouvez désactiver ce paramètre d'authentification de base à des fins de sécurité.

1. Connectez-vous à l'interface graphique de NetScaler.
2. Accédez à **Système > Licences > Licence ADC > Gérer les licences > Ajouter une nouvelle licence**.
3. Dans la page **Licences**, sélectionnez le bouton radio **Utiliser la licence à distance** et choisissez le mode **LAS** dans **Mode de licence à distance**.
4. Dans le champ **Nom du serveur/adresse IP**, saisissez l'adresse IP de l'agent externe de NetScaler Console.
5. Saisissez vos informations d'identification pour enregistrer l'instance auprès de NetScaler Console, puis cliquez sur **Continuer**.

   Remarque : Cochez la case Valider le certificat si vous disposez d'un certificat numérique pour la validation.
6. Dans le champ **Nom du profil de périphérique**, indiquez le profil d'instance que NetScaler Console utilise pour accéder à l'instance. Ce profil contient le nom d'utilisateur et le mot de passe des instances que vous souhaitez ajouter. Le profil par défaut est ns_nsroot_profile. Cependant, si vous avez modifié les informations d'identification de l'administrateur par défaut, assurez-vous de définir un nom de profil d'instance personnalisé.
7. Sous **Allouer des licences**, sélectionnez l'édition de licence et spécifiez la bande passante requise. La première fois que vous allouez des licences dans NetScaler, vous pouvez ensuite modifier ou libérer l'allocation directement depuis l'interface graphique de NetScaler Console.
8. Cliquez sur **Obtenir les licences**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Effectuez un redémarrage à chaud de l'instance après avoir modifié l'édition de la licence pour que les modifications prennent effet.

Comportement du blob d'activation de licence

Les blobs d'activation de licence que les instances NetScaler obtiennent de Console sur site dans le cadre de **Licence avec LAS ou Migration vers LAS** sont valides pendant 30 jours. Si un NetScaler perd puis retrouve la connectivité avec Console sur site, le blob d'activation de licence est immédiatement restauré.

Lorsqu'un NetScaler ne parvient pas à se reconnecter à Console sur site pendant 24 heures, il entre dans une période de grâce. Par défaut, les blobs d'activation de licence se rafraîchissent toutes les 8 heures. Si trois tentatives de rafraîchissement consécutives de 8 heures échouent sur 24 heures, le NetScaler entre dans une période de grâce.

Alerte de période de grâce de la licence

Voici les points de contact pour l'alerte de période de grâce de la licence :

- Sur le tableau de bord Flexed, une icône d'avertissement apparaît indiquant que l'instance est en période de grâce et les jours restants avant l'expiration du blob d'activation de licence.
- Chaque fois qu'un administrateur se connecte à l'interface graphique de l'instance NetScaler, un message contextuel apparaît indiquant que l'instance est en période de grâce et les jours restants avant l'expiration du blob d'activation de licence.
- Des notifications par e-mail sont envoyées à l'adresse e-mail configurée. Pour plus d'informations, consultez Configurer les paramètres de messagerie.

Remarque : Assurez-vous de sélectionner **Licences** pour la catégorie d'événements système afin de recevoir les notifications par e-mail liées aux licences.

Droit géré manuellement (licences basées sur des fichiers)

Avant de commencer

Assurez-vous que le prérequis suivant est rempli avant de configurer les licences Flexed :

- Les ports `27000` et `7279` sont accessibles de NetScaler à NetScaler Console, pour extraire les licences. Voir, Configuration système requise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Étape 1 - Appliquer les licences dans NetScaler Console

1. Accédez à **NetScaler® Licensing > License Management**.
2. Dans la section **Fichiers de licence**, sélectionnez **Ajouter un fichier de licence** et choisissez l'une des options suivantes :

   - **Télécharger des fichiers de licence depuis un ordinateur local**. Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger vers NetScaler Console.
   - **Utiliser le code d'accès à la licence**. Spécifiez le code d'accès à la licence que vous avez achetée auprès de Citrix. Ensuite, sélectionnez **Obtenir les licences**. Puis sélectionnez **Terminer**.

   REMARQUE :

   À tout moment, vous pouvez ajouter d'autres licences à NetScaler Console à partir des **Paramètres de licence**.

3. Cliquez sur **Terminer**.

   Les fichiers de licence sont ajoutés à NetScaler Console. La section **Informations sur l'expiration de la licence** répertorie les licences présentes dans NetScaler Console et les jours restants avant l'expiration.

4. Dans **Fichiers de licence**, sélectionnez un fichier de licence que vous souhaitez appliquer et cliquez sur **Appliquer les licences**.

   Cette action permet aux instances NetScaler d'utiliser la licence sélectionnée comme licence Flexed.

Étape 2 - Enregistrer NetScaler Console en tant que serveur de licences et allouer des licences

Vous pouvez enregistrer NetScaler Console en tant que serveur de licences auprès d'une instance NetScaler.

Enregistrer un serveur NetScaler Console à l'aide de l'interface graphique

Dans l'interface graphique de NetScaler Console, enregistrez le serveur NetScaler Console associé à une instance NetScaler.

1. Connectez-vous à l'interface graphique de NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Accédez à **Système > Licences > Gérer les licences**.
3. Cliquez sur **Ajouter une nouvelle licence**.
4. Sélectionnez **Utiliser la gestion des licences à distance** et sous **Mode de gestion des licences à distance**, sélectionnez **Licences en pool** dans la liste.
5. Dans le champ **Nom du serveur/adresse IP**, spécifiez l'adresse IP du serveur NetScaler Console.
6. Le port de licence par défaut est 27000.
7. Saisissez les informations d'identification de votre serveur NetScaler Console pour enregistrer une instance auprès de NetScaler Console et cliquez sur **Continuer**. Dans NetScaler Console, l'un des serveurs est le serveur de licences.

   REMARQUE :

   Cochez la case **Valider le certificat** uniquement si vous disposez d'un certificat d'autorité de certification (CA) numérique pour la validation.

8. Sous **Nom du profil de l'appareil**, spécifiez le profil d'instance que NetScaler Console peut utiliser pour accéder à l'instance. Ce profil d'instance contient le nom d'utilisateur et le mot de passe des instances que vous souhaitez ajouter à NetScaler Console. Le profil par défaut est **ns_nsroot_profile**. Si vous avez modifié les informations d'identification d'administrateur par défaut de vos instances, vous pouvez définir un nom de profil d'instance personnalisé.
9. Dans **Allouer des licences**, sélectionnez l'édition de licence et spécifiez la bande passante requise.

   Pour la première fois, allouez des licences dans NetScaler. Vous pouvez ultérieurement modifier ou libérer l'allocation de licences à partir de l'interface graphique de NetScaler Console.

   Cliquez sur **Obtenir des licences**.

   IMPORTANT

   Redémarrez à chaud l'instance si vous modifiez l'édition de licence. Les modifications de configuration ne prennent effet qu'après le redémarrage de l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter un serveur NetScaler Console à l'aide de l'interface de ligne de commande

Si une instance NetScaler n'a pas d'interface graphique, utilisez les commandes CLI suivantes pour ajouter un serveur NetScaler Console associé à une instance :

1. Connectez-vous à la console NetScaler.
2. Ajoutez l'adresse IP du serveur NetScaler Console associé qui est enregistré auprès de NetScaler Console. Le port de licence par défaut est 27000.

   ```
   > add ns licenseserver <adm-server-IP-address> -port <adm-server-license-port-number>
   ```

3. Affichez la bande passante de licence disponible sur le serveur de licences :

   ```
   > sh ns licenseserverpool
   ```

4. Allouez la bande passante de licence à partir de l'édition de licence requise :

   ```
   > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth> edition <specify-license-edition>
   ```

   IMPORTANT

   Redémarrez à chaud l'instance si vous modifiez l'édition de licence.

   `reboot -w`

   Les modifications de configuration ne prennent effet qu'après le redémarrage de l'instance.

Étape 3 - Modifier la capacité de débit flexible pour les instances NetScaler

1. Accédez à **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. Dans la section **Licensed NetScalers**, sélectionnez une instance et cliquez sur **Edit Throughput Capacity**.
3. Dans la page **Edit Throughput Capacity**, saisissez un nombre dans la colonne **Allocate**.
4. Cliquez sur **Submit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler MPX-Z

Le MPX-Z est l'appliance NetScaler MPX activée pour la capacité flexible. Le MPX-Z prend en charge le pool de bande passante uniquement pour les licences d'édition Premium.

Le MPX-Z nécessite une licence avant de pouvoir se connecter au serveur de licences. Vous pouvez installer la licence MPX-Z de l'une des manières suivantes :

- Chargement du fichier de licence depuis un ordinateur local.
- Utilisation du numéro de série matériel de l'instance.
- Le code d'accès à la licence de la section **Système** > **Licences** de l'interface graphique de l'instance.

Si vous supprimez la licence MPX-Z, le MPX n'est plus sous licence. Les licences sont libérées vers le serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance MPX-Z sans redémarrage. Un redémarrage n'est requis que si vous souhaitez modifier l'édition de la licence.

REMARQUE :

Lorsque vous redémarrez l'instance, elle extrait automatiquement les licences Flexed requises pour sa capacité configurée.

NetScaler SDX-Z

Le SDX-Z est l'appliance NetScaler SDX activée pour la capacité flexible. Le SDX-Z prend en charge le pool de bande passante et d'instances pour les licences d'édition Premium.

Le SDX-Z nécessite une licence avant de pouvoir se connecter au serveur de licences. Vous pouvez installer la licence SDX-Z de l'une des manières suivantes :

- Chargement du fichier de licence depuis un ordinateur local.
- Utilisation du numéro de série matériel de l'instance.
- Le code d'accès à la licence de la section **Système** > **Licences** de l'interface graphique de l'instance.

Si vous supprimez la licence SDX-Z, SDX devient sans licence. Les licences sont libérées vers le serveur de licences.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez modifier dynamiquement la bande passante d'une instance SDX-Z sans redémarrage.

REMARQUE :

Lorsque vous redémarrez l'instance, elle extrait automatiquement les licences Flexed requises pour sa capacité configurée.

Exigences de licence pour la paire haute disponibilité NetScaler (commun aux licences LAS et basées sur des fichiers)

Avant de commencer, assurez-vous que le serveur NetScaler Console est configuré en tant que serveur de licences. Pour plus d'informations, consultez Configurer NetScaler Console en tant que serveur de licences

Lorsque vous allouez la bande passante à une paire HA NetScaler, NetScaler Console extrait la bande passante allouée à l'instance principale. Vous devez répéter le processus pour l'instance secondaire.

Pour allouer des licences de pool à une paire HA NetScaler, consultez Allouer des licences Flexed aux instances NetScaler

La page **Capacité Flexed** affiche les instances et leur capacité allouée séparément.

États de licence Flexed NetScaler (commun aux licences LAS et basées sur des fichiers)

Les états de licence Flexed indiquent les exigences de licence sur une instance NetScaler. Les instances NetScaler configurées avec des licences Flexed affichent l'un des états suivants :

- **Alloué** : L'instance fonctionne avec une capacité de licence appropriée.
- **Période de grâce** : L'instance est en période de grâce. La période de grâce est de 30 jours, après quoi l'instance devient sans licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau de bord des licences Flexed

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits sur l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADCs : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité avec ces exigences sans engager

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

REMARQUES :

- Si vous aviez des licences groupées auparavant, et que vous avez maintenant acheté et appliqué des licences Flexed, le droit combiné apparaît désormais dans le tableau de bord des licences Flexed.
- Si vous n'avez que des licences en pool, consultez le tableau de bord des licences en pool.
- Si vous n'avez que des licences Flexed, ou à la fois des licences Flexed et en pool, consultez le tableau de bord des licences Flexed.
- **Point à noter basé sur la méthode de licence :**
  - Pour afficher les licences basées sur la licence LAS, accédez à l'onglet **NetScaler® licenses > Flexed Licensing > Dashboard > LAS managed entitlements**
  - Pour afficher les licences de droits gérés manuellement (licences basées sur des fichiers), accédez à l'onglet **NetScaler® licenses > Flexed Licensing > Dashboard > Manually managed entitlements**
  - Si vous utilisez les deux mécanismes de licence, référez-vous aux deux onglets. Le tableau de bord des licences Flexed vous offre une vue complète de la capacité de débit et des instances que vous avez achetées.

La capacité de débit pour toutes les éditions et les détails des instances pour différents facteurs de forme, tels que MPX, VPX et SDX, sont affichés sur cette page. NetScaler MPX et NetScaler MPX FIPS ont le même fichier de licence. De même, NetScaler SDX et NetScaler SDX FIPS ont le même fichier de licence. Cependant, NetScaler VPX FIPS a un fichier différent de NetScaler VPX et est affiché séparément. De plus, NetScaler VPX (y compris VPX sur SDX), NetScaler BLX et NetScaler CPX nécessitent des licences NetScaler VPX et font partie des droits et de l'allocation pour VPX. Une licence Flexed ne prend en charge que l'édition Premium. Cependant, si vous avez acheté des licences Flexed et aviez auparavant une capacité de bande passante en pool Standard ou Advanced, les détails relatifs à la capacité de bande passante (Standard ou Advanced) sont également répertoriés dans le tableau de bord des licences Flexed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les facteurs de forme VPX (y compris VPX sur SDX), BLX et CPX nécessitent un fichier de licence d'instance logicielle NetScaler Flexed VPX. C'est-à-dire que ces facteurs de forme font partie des droits et de l'allocation pour les licences d'instance logicielle Flexed VPX.

Les détails concernant vos instances NetScaler sous licence sont disponibles dans la section **Licensed NetScalers**. Vous pouvez sélectionner une instance et modifier la bande passante ou libérer la licence sur cette instance.

Vous pouvez filtrer les résultats en fonction des paramètres suivants :

- Filtrer par capacité de débit
  - Premium
  - Advanced
  - Standard
- Facteur de forme
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- État de la licence
  - Connexion perdue
  - Grâce
  - Alloué

Modifier la capacité de débit allouée sur une instance NetScaler

1. Accédez à **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. Dans la section **NetScaler sous licence**, sélectionnez une instance et cliquez sur **Modifier la capacité de débit**.
3. Dans la page **Modifier la capacité de débit**, saisissez un nombre dans la colonne **Allouer**.
4. Cliquez sur **Soumettre**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Libérer des licences sur une instance NetScaler

Pour transférer des licences vers une autre instance, vous devez libérer la licence sur l'instance actuelle, puis appliquer la licence à la nouvelle instance. La sélection de **Libérer la licence** effectue les opérations suivantes :

- Libère toutes les licences, qui sont extraites sur cette instance, vers le serveur de licences.
- Supprime la configuration du serveur de licences sur cette instance.

Si vous sélectionnez **Oui**, votre instance NetScaler devient sans licence et ne peut pas traiter de trafic.

Rapports de licences Flexed

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles avec le LAS sont :

- NetScaler ADCs : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge du LAS pour Console on-prem est à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont dépréciées à compter du April 15 2026 pour les versions de Console on-prem 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console on-prem, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

version 14.1-51.x ou ultérieure de Console on-prem et passer au LAS avant 15th April 2026 car Console on-prem 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront non licenciées lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Dans ce tableau de bord, vous pouvez consulter les détails concernant :

- Les droits et l'allocation des instances logicielles (VPX, MPX et SDX, et VPX FIPs)
- Les droits, l'allocation et l'utilisation réelle de la capacité de bande passante/débit
- Allocation maximale et moyenne sur toutes les instances gérées ou sélectionnées
- Utilisation maximale et moyenne sur toutes les instances gérées ou sélectionnées

FONCTIONNALITÉS (POUR LES INSTANCES NETSCALER)	DESCRIPTION
Droit d'utilisation	Les droits d'instance totaux pour les types d'instances logicielles (VPX, SDX, MPX).
Allocation	L'allocation d'instance totale pour les types d'instances logicielles (VPX, SDX, MPX).

FONCTIONNALITÉS (POUR LA CAPACITÉ DE BANDE PASSANTE/DÉBIT)	DESCRIPTION
Droit d'utilisation	Les droits totaux de capacité de bande passante/débit sur toutes les instances NetScaler gérées. Les droits totaux sont calculés à partir des licences appliquées dans la gestion des licences (**Licences NetScaler > Gestion des licences**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS (POUR LA CAPACITÉ DE BANDE PASSANTE/DÉBIT)	DESCRIPTION
Allocation	La capacité de bande passante/débit qui est allouée aux **NetScaler sous licence** dans le tableau de bord des licences flexibles (**Licences NetScaler > Licences flexibles > Tableau de bord**).
Utilisation	Le débit total consommé par les instances NetScaler.

REMARQUE :

Une licence flexible ne prend en charge que l'édition premium. Toutefois, si vous avez acheté et appliqué des licences flexibles, et que vous disposiez auparavant d'une capacité de bande passante standard ou avancée mutualisée, les détails relatifs à la capacité de bande passante/débit (standard ou avancée) sont également répertoriés. Par exemple, si vous avez appliqué une licence flexible de 1000 Gbit/s (qui est premium) et que vous disposez également d'une licence mutualisée active de 100 Gbit/s de bande passante avancée, le tableau de bord de reporting affiche à la fois Premium 1000 Gbit/s et 100 Gbit/s de bande passante avancée.

L'exemple suivant vous aide à comprendre comment le tableau de bord affiche l'utilisation maximale et l'utilisation moyenne :

Considérons qu'il existe 3 instances NetScaler gérées (NetScaler A, NetScaler B et NetScaler C) avec une licence flexible (bande passante Premium) et que la durée sélectionnée est de 1 jour. Pour les calculs, NetScaler Console prend en compte les points de données (en Mbit/s) pour chaque heure par instance NetScaler. Pour 1 jour, il y a 24 points de données pour chaque instance NetScaler. Ainsi, pour 3 instances NetScaler, il y a (24 * 3) points de données.

- **Utilisation maximale** = La somme du point de données le plus élevé (Mbit/s) sur les 24 heures de toutes les instances NetScaler. Par exemple, si le point de données le plus élevé sur la durée de 24 heures pour NetScaler A est de 30 Mbit/s, pour NetScaler B de 45 Mbit/s et pour NetScaler C de 120 Mbit/s, alors l'utilisation maximale affichée est de 195 Mbit/s (30 + 45 + 120).
- **Utilisation moyenne** = La somme de tous les points de données sur 24 heures divisée par 24 pour chaque instance NetScaler. Ainsi, pour 3 instances NetScaler, la moyenne totale des 3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

instances NetScaler est divisée par 3. Par exemple, si la moyenne de NetScaler A est de 25 Mbit/s, celle de NetScaler B de 20 Mbit/s et celle de NetScaler C de 45 Mbit/s, l'utilisation moyenne affichée est de 30 Mbit/s (25 + 20 + 45 divisé par 3).

De même, les détails d'allocation maximale et moyenne sont affichés en utilisant la même logique.

Vous pouvez sélectionner la durée dans la liste, d'une heure à un an, et afficher les détails sous forme de tableau et de graphique.

L'exemple suivant montre la vue tabulaire pour les instances utilisant une licence flexible (bande passante Premium) :



Les détails suivants apparaissent sur le tableau de bord :

- **Utilisation maximale** - L'utilisation la plus élevée (en Mbit/s) pour la durée sélectionnée.
- **Utilisation moyenne** - L'utilisation moyenne (en Mbit/s) pour la durée sélectionnée.
- **Allocation maximale** - L'allocation la plus élevée pour la durée sélectionnée.
- **Allocation moyenne** - L'allocation moyenne pour la durée sélectionnée.
- **Filtrer** - Vous pouvez sélectionner une ou plusieurs instances pour afficher les détails d'utilisation et d'allocation pour les instances spécifiques.
- **Exporter** - Vous pouvez exporter les détails au format PDF, JPEG et PNG.

L'exemple suivant montre la vue graphique des instances utilisant la licence Flexed (bande passante Premium) :



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Transition vers les licences Flexed

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans l'ensemble de la suite de produits Citrix. LAS sera le seul moyen d'activer et de licencier les instances NetScaler après April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible avec LAS.

Les versions minimales requises de NetScaler® compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à partir de April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'à 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site, et passer à LAS avant 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront non licenciées lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

Licences basées sur LAS

REMARQUE :

Assurez-vous que vos instances NetScaler (ADC et SDX) sont sur des versions compatibles avec le LAS.

Pour les informations relatives à la migration pour la licence suivante, reportez-vous à la section **Migrer les instances sous licence existantes** dans License Activation Service.

- Licences Flexed (licences basées sur des fichiers) vers licences Flexed (licences basées sur LAS)
- Licences en pool (licences basées sur des fichiers) vers licences Flexed (licences basées sur LAS)

Pour les informations relatives à la transition pour la licence suivante, reportez-vous à la section **Transition vers LAS** dans License Activation Service.

- Licences vCPU en pool (licences basées sur des fichiers) vers licences Flexed (licences basées sur LAS)
- Licences par abonnement fixe ou perpétuelles (licences basées sur des fichiers) vers licences Flexed (licences basées sur LAS)
- Licences vCPU fixes (licences basées sur des fichiers) vers licences Flexed (licences basées sur LAS)
- Licences CICO (licences basées sur des fichiers) vers licences Flexed (licences basées sur LAS)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Droits gérés manuellement (licences basées sur des fichiers)

REMARQUE :

Vous devez passer à la licence Flexed avant l'expiration de votre licence actuelle. Lors de la planification de la transition, gardez les étapes suivantes à l'esprit et prévoyez une fenêtre de maintenance si les étapes impliquent une reconfiguration de licence ou un redémarrage de NetScaler®.

Licence de bande passante en pool vers licence Flexed

Certaines étapes sont communes à MPX, SDX et VPX. Ces étapes sont énumérées en premier, suivies des étapes spécifiques à MPX, SDX ou VPX.

Étapes communes pour VPX/MPX/SDX

1. Téléchargez et appliquez les licences logicielles Flexed sur NetScaler Console. Consultez Fichiers de licence.
2. Si vous disposez d'une licence logicielle Z-Cap pour une période spécifique, appliquez cette licence sur le matériel NetScaler (MPX/SDX).

Pour VPX/MPX

Les étapes supplémentaires suivantes sont nécessaires :

1. Si vous disposez d'une licence de bande passante Pooled Premium (Platinum), la licence passe automatiquement en mode Flexed après l'expiration de l'ancienne licence.
2. Si vous disposez d'une licence de bande passante Pooled Standard ou Pooled Advanced, extrayez manuellement la bande passante Premium et redémarrez à chaud NetScaler.

Pour SDX

REMARQUE :

Assurez-vous de passer à la licence Flexed avant l'expiration de votre licence actuelle.

Les étapes supplémentaires suivantes sont nécessaires :

1. Extrayez l'instance requise et la licence de bande passante de la licence Flexed vers SDX. Un redémarrage de SDX n'est pas nécessaire.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Si tous les VPX sur SDX ont une édition Premium, la licence passe automatiquement en mode Flexed après l'expiration de l'ancienne licence.
3. Modifiez l'édition de tous les VPX (sur SDX) avec Standard ou Advanced en Premium. Ces instances VPX sont automatiquement redémarrées.
4. Réduisez la capacité de bande passante Standard et Advanced sur SDX à zéro.

vCPU en pool vers la capacité de bande passante Flexed

Pour VPX

1. Téléchargez et appliquez les licences logicielles Flexed sur NetScaler Console. Voir Fichiers de licence.
2. Supprimez le serveur de licences existant à l'aide de l'interface graphique de NetScaler. NetScaler n'est pas sous licence tant que toutes les étapes ne sont pas terminées.
3. Ajoutez le serveur de licences avec l'option Flexed/Pooled.
4. Extrayez les licences d'instance et de bande passante requises vers NetScaler.
5. Redémarrez à chaud NetScaler.

Pour CPX

1. Téléchargez et appliquez les licences flexed sur NetScaler Console. Voir Fichiers de licence.
2. Mettez à jour le fichier manifeste CPX YAML ou HELM avec les exigences de bande passante. Voir Licences CPX basées sur la bande passante.
3. Déployez l'instance CPX à l'aide de la commande `kubectl apply -f cpx.yaml` ou du graphique HELM.

Abonnement fixe ou licence perpétuelle vers licence Flexed

Certaines étapes sont communes à MPX, SDX et VPX. Ces étapes sont listées en premier, suivies des étapes spécifiques à MPX, SDX ou VPX.

Étapes communes pour VPX/MPX/SDX

1. Intégrez à NetScaler Console.
2. Téléchargez et appliquez les licences logicielles Flexed sur NetScaler Console. Voir Fichiers de licence.
3. Appliquer la licence logicielle Z-Cap sur le matériel NetScaler (MPX/SDX).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour VPX/MPX

Les étapes supplémentaires suivantes sont nécessaires :

1. Extraire les licences d'instance et de bande passante requises vers NetScaler.
2. Redémarrer à chaud NetScaler.
3. Supprimer la licence d'abonnement fixe après le redémarrage de NetScaler.

Pour SDX

Les étapes supplémentaires suivantes sont nécessaires :

1. Extraire la licence d'instance et de bande passante requise de la licence Flexed sur SDX.
2. Si tous les VPX sur SDX ont l'édition premium, un redémarrage de SDX n'est pas nécessaire.
3. Si un VPX a l'édition avancée ou standard, ce VPX doit être basculé vers l'édition premium. Le VPX redémarre automatiquement.
4. Appliquer la licence logicielle Z-Cap sur NetScaler SDX.
5. Extraire la licence d'instance et de bande passante requise de la licence Flexed sur SDX.
6. Supprimer la licence d'abonnement fixe après le redémarrage de NetScaler.

CICO vers la capacité de bande passante Flexed

Pour VPX

1. Téléchargez et appliquez les licences logicielles Flexed sur NetScaler Console. Voir Fichiers de licence.
2. Supprimez le serveur de licences existant à l'aide de l'interface graphique de NetScaler. NetScaler n'est pas sous licence tant que toutes les étapes ne sont pas terminées.
3. Ajoutez le serveur de licences avec l'option Flexed/Pooled.
4. Extrayez les licences d'instance et de bande passante requises vers NetScaler.
5. Redémarrez à chaud NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scénarios pour l'expiration des licences Flexed ou Pooled et le comportement en cas de problèmes de connectivité

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licence (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge du LAS pour Console sur site est à partir de la version 14.1-51.x et ultérieure. Cependant, les licences basées sur des fichiers sont obsolètes à partir du April 15 2026 pour les versions Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version Console sur site 14.1-51.x ou la version 13.1-60.x ou ultérieure, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version Console sur site 14.1-51.x ou ultérieure, et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.

Licences basées sur le LAS

Avant l'expiration du terme

- La licence doit être renouvelée avant l'expiration de son terme.
- Pour NetScaler Console sur site (connecté au cloud), le droit de licence est renouvelé automatiquement si le contrat de licence a été renouvelé dans les 24 heures.
- Si la licence est renouvelée avant l'expiration du terme, le NetScaler basculera de manière transparente vers la nouvelle licence après l'expiration de l'ancienne, tant que l'appareil est opérationnel.
- Un redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

Après l'expiration du terme

Si la licence n'est pas renouvelée avant l'expiration de son terme, l'instance NetScaler arrête ses opérations normales.

- Elle perd sa configuration.
- Tout le traitement du trafic s'arrête complètement.

Scénarios de comportement en cas de problèmes de connectivité

Les blobs d'activation de licence que les instances NetScaler reçoivent de Console sur site dans le cadre des processus **Licence avec LAS** ou **Migrer vers LAS** sont valides pendant 30 jours.

Si le NetScaler perd la connectivité avec Console sur site puis se reconnecte, il reçoit immédiatement le blob d'activation de licence sans aucun délai.

Si un NetScaler ne peut pas se reconnecter à Console sur site pendant 24 heures, il entre dans une période de grâce.

Par défaut, les blobs d'activation de licence sont actualisés toutes les 8 heures. Si une tentative d'actualisation échoue trois fois consécutives dans les 24 heures, le NetScaler entre dans une période de grâce.

Période de grâce :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler entre dans une période de grâce de 30 jours.
- Toutes les fonctionnalités de licence continuent de fonctionner. Cependant, le trente et unième jour :
    - Les instances NetScaler VPX, NetScaler CPX, NetScaler BLX et NetScaler MPX subissent un redémarrage forcé et deviennent sans licence.
    - Le débit sur toutes les instances VPX d'un NetScaler SDX est réduit à 1 Mbps.

Alerte de période de grâce de la licence

Sur le tableau de bord Flexed, une icône d'avertissement apparaît, indiquant que l'instance est en période de grâce et les jours restants avant l'expiration du blob d'activation de la licence. Chaque fois qu'un administrateur se connecte à l'interface graphique de l'instance NetScaler, un message contextuel apparaît, indiquant que l'instance est en période de grâce et les jours restants avant l'expiration du blob d'activation de la licence.

Licence gérée manuellement (licence basée sur un fichier)

Ce document présente différents scénarios d'expiration de licence et de comportement en cas de problèmes de connectivité dans NetScaler MPX, NetScaler SDX et NetScaler VPX/NetScaler BLX/ NetScaler CPX.

Types de licences Flexed

- Instance logicielle (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- Capacité de bande passante

Scénario : Facteur de forme MPX

Vous utilisez des licences Flexed/Pooled et les licences sont sur le point d'expirer. Les scénarios suivants expliquent le comportement lorsqu'une nouvelle licence est téléchargée sur NetScaler Console avant et après l'expiration du terme, ou lorsqu'un fichier de licence n'est pas présent.

Avant l'expiration du terme

Si la nouvelle licence est téléchargée avant l'expiration du terme et que l'ancienne licence est toujours valide, deux pools de capacité différents (ancien et nouveau) sont disponibles.

- Si NetScaler est opérationnel, il bascule de manière transparente vers la nouvelle licence Flexed/Pooled après l'expiration de l'ancienne licence.
- Le redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après l'expiration du terme

L'instance NetScaler arrête ses opérations normales après l'expiration de la licence, y compris la perte de configuration et l'arrêt complet du traitement du trafic.

Scénario : Facteur de forme SDX

Vous utilisez des licences Flexed/Pooled et celles-ci sont sur le point d'expirer. Les scénarios suivants expliquent le comportement lorsqu'une nouvelle licence est téléchargée sur NetScaler Console avant et après l'expiration du terme, ou lorsqu'aucun fichier de licence n'est présent.

Avant l'expiration du terme

Si la nouvelle licence est téléchargée avant l'expiration du terme et que l'ancienne licence est toujours valide, deux pools de capacité différents (ancien et nouveau) sont disponibles.

- Si NetScaler est opérationnel, il bascule de manière transparente vers la nouvelle licence Flexed/Pooled après l'expiration de l'ancienne licence.
- Le redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

Après l'expiration du terme

L'instance NetScaler arrête ses opérations normales après l'expiration de la licence, y compris la perte de configuration et l'arrêt complet du traitement du trafic.

Scénario : Facteur de forme VPX/BLX/CPX

Vous utilisez des licences Flexed/Pooled et celles-ci sont sur le point d'expirer. Les scénarios suivants expliquent le comportement lorsqu'une nouvelle licence est téléchargée sur NetScaler Console avant et après l'expiration du terme, ou lorsqu'aucun fichier de licence n'est présent.

Avant l'expiration du terme

Si la nouvelle licence est téléchargée avant l'expiration du terme et que l'ancienne licence est toujours valide, deux pools de capacité différents (ancien et nouveau) sont disponibles.

- Si NetScaler est opérationnel, il bascule de manière transparente vers la nouvelle licence Flexed/Pooled après l'expiration de l'ancienne licence.
- Un redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après l'expiration du terme

L'instance NetScaler arrête ses opérations normales après l'expiration de la licence, y compris la perte de configuration et l'arrêt complet du traitement du trafic.

Scénarios de comportement en cas de problèmes de connectivité

Si la connectivité est interrompue entre NetScaler et le serveur NetScaler Console sur site, le comportement est le suivant :

- NetScaler entre en période de grâce pendant 30 jours.
- Pendant cette période de grâce, la fonctionnalité de licence continue de fonctionner jusqu'au trentième jour.
- Le trente et unième jour,
  - NetScaler VPX/NetScaler CPX/NetScaler BLX et NetScaler MPX subissent un redémarrage forcé et deviennent sans licence.
  - Le débit sur tous les VPX de NetScaler SDX est réduit à 1 Mbps.

Configurer le serveur NetScaler Console en tant que serveur de licences Flexed ou Pooled

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits sur l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console sur site : 14.1-51.x

  Remarque : Le support LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à partir du April 15 2026 pour les versions Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version Console sur site 14.1-51.x ou la version 13.1-60.x ou ultérieure, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version Console sur site 14.1-51.x ou ultérieure, et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront non licenciées lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou les réglementations l'interdisent.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
En tant qu'administrateur, vous pouvez configurer le serveur NetScaler Console uniquement en tant que serveur de licences Flexed ou Pooled. Avec cette configuration, le serveur NetScaler Console ne reçoit que les données de licence des instances NetScaler.

Parfois, vous pouvez avoir un mandat réglementaire qui exige de restreindre les données des instances NetScaler de quitter la zone réglementaire. Dans de telles situations, vous pouvez déployer une instance locale du serveur NetScaler Console sur site dans votre zone réglementaire pour utiliser les capacités de gestion, de surveillance et d'analyse. Lorsque vous suivez la même approche pour utiliser la fonctionnalité de licences Flexed ou Pooled, vous devez répartir les licences Flexed ou Pooled entre différents serveurs de licences NetScaler Console. Cette approche ne vous offre pas la flexibilité d'allouer des licences Flexed ou Pooled à vos instances NetScaler déployées globalement.

Par conséquent, configurez le serveur NetScaler Console uniquement en tant que serveur de licences Flexed ou Pooled. Le serveur NetScaler Console ne reçoit que les données de licence de toutes les instances NetScaler. Ainsi, vous pouvez respecter le mandat réglementaire et allouer dynamiquement des licences de capacité Flexed ou Pooled à vos instances NetScaler déployées globalement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment configurer le serveur NetScaler Console uniquement comme serveur de licences Flexed ou Pooled

Avant de commencer, assurez-vous qu'aucune instance NetScaler n'est ajoutée au serveur NetScaler Console. N'ajoutez des instances NetScaler qu'après avoir terminé l'étape 4.

Procédez comme suit pour configurer le serveur NetScaler Console uniquement pour le serveur de licences Flexed ou Pooled :

1. Accédez à **Paramètres > Administration**.
2. Dans la section **Configurations système**, sélectionnez **Déploiement système**.
3. Dans **Déploiement ADM**, sélectionnez **NetScaler Console uniquement en tant que serveur de licences flexed/pooled**.

   

4. Cliquez sur **OK**.

   Cette action conserve uniquement la fonctionnalité de licence Flexed ou Pooled et désactive les fonctionnalités NetScaler Console suivantes :

   - Sauvegarde NetScaler Console
   - Gestion des événements
   - Gestion des certificats SSL
   - Rapports réseau
   - Fonctions réseau
   - Audit de configuration

   REMARQUE

   Par défaut, la fonctionnalité d'analyse de NetScaler Console est désactivée. Assurez-vous de désactiver cette fonctionnalité si vous l'avez activée.

   Dans la boîte de confirmation, cliquez sur **Oui**.

   L'interface graphique de NetScaler Console affiche désormais uniquement la fonctionnalité de licence Flexed ou Pooled. Et les fonctionnalités restantes n'apparaissent pas.

5. Après avoir configuré NetScaler Console uniquement pour la fonctionnalité de licence, ajoutez des instances NetScaler dans la page **Infrastructure > Instances**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Vous pouvez ajouter une instance NetScaler dans un ou plusieurs serveurs NetScaler Console. Lorsque vous modifiez le mot de passe de ces instances NetScaler, assurez-vous de mettre à jour le mot de passe sur tous les serveurs NetScaler Console où l'instance est découverte.
- Un utilisateur peut toujours effectuer certaines opérations des fonctionnalités désactivées dans l'interface graphique de NetScaler Console. Par exemple, l'interrogation d'événements et la sauvegarde NetScaler. En tant que super administrateur, si vous souhaitez restreindre de telles opérations, désactivez l'accès utilisateur pour les autres administrateurs à l'aide d'une politique d'accès appropriée. Pour plus d'informations, consultez Configurer les politiques d'accès sur NetScaler Console.

Vous pouvez également déployer le serveur NetScaler Console uniquement pour le serveur de licences Flexed ou Pooled avec les spécifications inférieures suivantes :

COMPOSANT	EXIGENCE
RAM	8 GB
CPU virtuel	4
Stockage	120 Go

Licences héritées

Les licences héritées couvrent les modèles de licence précédents de capacité mutualisée, d'enregistrement et de retrait, et de CPU virtuel pour vos instances NetScaler. Les rubriques suivantes vous aident à gérer les licences héritées :

- Licence mutualisée NetScaler
- Configurer la capacité mutualisée NetScaler
- Mettre à niveau une licence perpétuelle dans NetScaler VPX vers la capacité mutualisée NetScaler
- Mise à niveau d'une licence perpétuelle dans NetScaler MPX vers la capacité mutualisée NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Mettre à niveau une licence perpétuelle dans NetScaler SDX vers la capacité mutualisée NetScaler
- Capacité mutualisée NetScaler sur les instances NetScaler en mode cluster
- Licences d'enregistrement et de retrait NetScaler VPX
- Licences de CPU virtuel NetScaler
- Comportements attendus en cas de problèmes

Capacité mutualisée NetScaler

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licence (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge du LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer au LAS avant 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
La capacité mutualisée NetScaler vous permet de partager des licences de bande passante ou d'instance entre différents facteurs de forme NetScaler. Pour les instances basées sur un abonnement vCPU, vous pouvez partager la licence vCPU entre les instances. Utilisez cette capacité mutualisée pour les instances qui se trouvent dans le centre de données ou les clouds publics. Lorsqu'une instance n'a plus besoin des ressources, elle restitue la capacité allouée au pool commun. Réutilisez la capacité libérée pour d'autres instances NetScaler qui ont besoin de ressources.

Vous pouvez utiliser la licence mutualisée pour maximiser l'utilisation de la bande passante en garantissant l'allocation de bande passante nécessaire à une instance, sans dépasser ses besoins. Augmentez ou diminuez la bande passante allouée à une instance en cours d'exécution sans affecter le trafic. Avec les licences de capacité mutualisée, vous pouvez automatiser le provisionnement des instances.

Fonctionnement de la licence de capacité mutualisée NetScaler

La capacité groupée NetScaler comprend les composants suivants :

- Instances NetScaler, qui peuvent être classées en :
  - Matériel à capacité nulle
  - Instances NetScaler VPX autonomes ou instances NetScaler CPX ou instances NetScaler BLX
- Pool de bande passante
- Pool d'instances
- NetScaler Console configuré en tant que serveur de licences

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Matériel à capacité nulle

Lorsqu'elles sont gérées via la capacité groupée NetScaler, les instances MPX et SDX sont appelées « matériel à capacité nulle » car ces instances ne peuvent pas fonctionner tant qu'elles n'ont pas extrait des ressources des pools de bande passante et d'instances. Ainsi, ces plates-formes sont également appelées appliances MPX-Z et SDX-Z.

Le matériel à capacité nulle nécessite une licence de plate-forme pour pouvoir extraire de la bande passante et une licence d'instance du pool commun.

REMARQUE

- L'abonnement à la licence d'instance n'est pas requis pour les instances MPX. Consultez le tableau 1 de cette page pour connaître la capacité groupée prise en charge pour les instances MPX et SDX. Consultez le tableau 5 pour connaître les exigences de licence pour les différents facteurs de forme MPX et SDX.
- L'installation de la licence à capacité nulle fonctionne de la même manière que les autres licences locales NetScaler. Pour plus d'informations sur la façon d'obtenir et d'installer une licence à capacité nulle, consultez le Guide de licences pour NetScaler.

Gérer et installer les licences de plate-forme

Vous devez installer une licence de plate-forme manuellement, en utilisant le numéro de série du matériel ou le code d'accès à la licence. Une fois la licence de plate-forme installée, elle est verrouillée au matériel et ne peut pas être partagée entre les instances matérielles NetScaler à la demande. Cependant, vous pouvez déplacer manuellement la licence de plate-forme vers une autre instance matérielle NetScaler.

Les instances NetScaler MPX exécutant la version logicielle NetScaler 11.1 build 54.14 ou ultérieure et les instances NetScaler SDX exécutant la version 11.1 build 58.13 ou ultérieure prennent en charge la capacité groupée NetScaler. Pour plus d'informations, consultez **Tableau 1. Capacité groupée prise en charge pour les instances MPX et SDX**.

Instances NetScaler VPX autonomes

Les instances NetScaler VPX exécutant la version logicielle NetScaler 11.1 Build 54.14 ou ultérieure sur les hyperviseurs suivants prennent en charge la capacité groupée :

- VMware ESX 6.0
- Citrix Hypervisor™

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Linux KVM

Les instances NetScaler VPX exécutant la version logicielle NetScaler 12.0 Build 51.24 ou ultérieure sur les hyperviseurs et plateformes cloud suivants prennent en charge la capacité groupée :

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Les instances NetScaler VPX exécutant les versions logicielles NetScaler 13.0 et 13.1 (toutes versions) sur les hyperviseurs et plateformes cloud suivants prennent en charge la capacité groupée :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

REMARQUE

Pour permettre la communication entre NetScaler Console et Microsoft Azure ou AWS, un tunnel IPSEC doit être configuré. Pour plus d'informations, consultez Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler Console. Contrairement au matériel à capacité nulle, NetScaler VPX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, il doit extraire de la bande passante et une licence d'instance du pool.

Instances NetScaler CPX autonomes

Les instances NetScaler CPX déployées sur un hôte Docker prennent en charge la capacité groupée. Contrairement au matériel à capacité nulle, NetScaler CPX ne nécessite pas de licence de plate-forme. Une seule instance NetScaler CPX consommant jusqu'à 1 Gbit/s de débit n'extrait qu'une seule instance et aucune bande passante du pool de licences. Par exemple, considérez que vous disposez de 20 instances NetScaler CPX avec un pool de bande passante de 20 Gbit/s.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si l'une des instances NetScaler CPX consomme un débit de 500 Mbit/s, le pool de bande passante reste de 20 Gbit/s pour les 19 instances NetScaler CPX restantes.

Si la même instance NetScaler CPX commence à consommer un débit de 1500 Mbit/s, le pool de bande passante dispose de 19,5 Gbit/s pour les 19 instances NetScaler CPX restantes.

Pour les licences de pool, vous ne pouvez ajouter de bande passante que par multiples de 10 Mbit/s.

Instances NetScaler BLX autonomes

Les instances NetScaler BLX prennent en charge les licences de capacité groupée. Une instance NetScaler BLX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, une instance NetScaler BLX doit extraire de la bande passante et une licence d'instance du pool.

Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par les instances NetScaler, physiques et virtuelles. Le pool de bande passante comprend des pools distincts pour chaque édition logicielle (Standard, Advanced et Premium). Une instance NetScaler donnée ne peut pas avoir de bande passante extraite de différents pools simultanément. Le pool de bande passante à partir duquel elle peut extraire de la bande passante dépend de son édition logicielle pour laquelle elle est sous licence.

Pool d'instances

Le pool d'instances définit le nombre d'instances NetScaler VPX ou d'instances NetScaler CPX ou d'instances NetScaler BLX qui peuvent être gérées via la capacité groupée NetScaler ou le nombre d'instances NetScaler VPX dans une instance SDX-Z.

Lorsqu'elle est extraite du pool, une licence déverrouille les ressources de l'instance MPX-Z, SDX-Z, VPX, NetScaler CPX et NetScaler BLX, y compris les CPU/PE, les cœurs SSL, les paquets par seconde et la bande passante.

REMARQUE

Le service de gestion d'un SDX-Z ne consomme pas d'instance.

Serveur de licences NetScaler Console

La capacité groupée NetScaler utilise NetScaler Console configuré comme serveur de licences pour gérer les licences de capacité groupée : licences de pool de bande passante et licences de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pool d'instances. Vous pouvez utiliser le logiciel NetScaler Console pour gérer les licences de capacité groupée sans licence NetScaler Console.

Lors de l'extraction de licences du pool de bande passante et d'instances, le facteur de forme NetScaler et le numéro de modèle matériel sur un matériel à capacité nulle déterminent

- La bande passante minimale et le nombre d'instances qu'une instance NetScaler doit extraire avant d'être fonctionnelle.
- La bande passante maximale et le nombre d'instances qu'un NetScaler peut extraire.
- L'unité minimale de bande passante pour chaque extraction. C'est la plus petite unité qu'un NetScaler doit extraire d'un pool. Toute extraction doit être un multiple entier de cette unité minimale. Par exemple, si l'unité minimale de bande passante d'un NetScaler est de 1 Gbit/s, 1000 Mbit/s peuvent être extraits, mais pas 200 Mbit/s ou 150,5 Gbit/s. L'unité minimale de bande passante est distincte de l'exigence minimale de bande passante. Une instance NetScaler ne peut fonctionner qu'après avoir été licenciée avec au moins la bande passante minimale. Une fois la bande passante minimale atteinte, l'instance peut extraire davantage de bande passante en utilisant l'unité minimale.

Les tableaux 1, 2, 3 et 4 récapitulent la bande passante/les instances maximales, la bande passante/les instances minimales et l'unité de bande passante minimale pour toutes les instances NetScaler prises en charge. Le tableau 5 récapitule les exigences de licence pour différents facteurs de forme pour toutes les instances NetScaler prises en charge :

Tableau 1. Capacité groupée prise en charge pour les instances MPX et SDX

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
MPX 5900Z	10	1	N/A	N/A	1 Gbit/s
MPX 8900Z	30	5	NA	NA	1 Gbit/s
MPX 9100Z	30	10	NA	NA	1 Gbps
MPX 8900Z FIPS	33	5	NA	NA	1 Gbps
MPX 14000Z série	100	20	NA	NA	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
Série MPX 14000Z 40G	100	20	N/A	N/A	1 Gbit/s
Série MPX 14000Z FIPS	100	20	N/A	N/A	1 Gbit/s
Série MPX 14000Z 40S	100	20	N/A	N/A	1 Gbit/s
Série MPX 15000Z	120	20	N/A	N/A	1 Gbit/s
Série MPX 15000Z FIPS	120	20	N/A	N/A	1 Gbps
Série MPX 15000Z 50G	120	20	N/A	N/A	1 Gbps
Série MPX 16000Z	200	30	N/A	N/A	1 Gbps
Série MPX 22000Z	120	40	N/A	N/A	1 Gbit/s
Série MPX 24000Z	150	100	N/A	N/A	1 Gbit/s
MPX 25000Z 40G	200	100	N/A	N/A	1 Gbit/s
MPX 25000ZA	200	100	N/A	N/A	1 Gbit/s
Série MPX 26000Z	200	100	N/A	N/A	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
Série MPX 26000Z 100G	200	100	N/A	N/A	1 Gbit/s
Série MPX 26000Z 50S	200	100	N/A	N/A	1 Gbit/s
SDX 8900Z	30	10	1	7	1 Gbit/s
SDX 9100Z	95	20	1	7	1 Gbit/s
Série SDX 14000Z	100	10	1	25	1 Gbit/s
Série SDX 14000Z 40G	100	1	2	25	1 Gbit/s
Série SDX 14000Z 40S	100	20	1	25	1 Gbit/s
Série SDX 14000Z FIPS	100	10	1	25	1 Gbps
SDX 15000Z 50G	120	10	1	55	1 Gbps
SDX 15000Z	120	10	1	55	1 Gbps
Série SDX 16000Z	200	15	1	55	1 Gbit/s
Série SDX 22000Z	120	20	1	80	1 Gbit/s
SDX 25000Z 40G	200	50	1	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (GBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
SDX 25000ZA	200	50	1	115	1 Gbps
SDX 26000Z 100G	200	50	1	115	1 Gbps
SDX 26000Z	200	50	1	115	1 Gbps
SDX 26000Z 50S	200	50	1	115	1 Gbps
Série SDX 24000Z	150	50	1	80	1 Gbit/s

Remarque

La bande passante et les instances minimales sont applicables aux instances SDX exécutant les versions suivantes et supérieures : 11.1 64.x, 12.0 63.x, 12.1 54.x et 13.0 41.x.

La quantité d'achat minimale est différente de la configuration système minimale requise.

Tableau 2. Capacité groupée prise en charge pour les instances NetScaler CPX

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (MBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
CPX	10	10	1	1	10 Mbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau 3. Capacité groupée prise en charge pour les instances NetScaler VPX sur les hyperviseurs et les services cloud

HYPERVISEUR/ SERVICE CLOUD	BANDE PASSANTE MAXIMALE (GBPS)	BANDE PASSANTE MINIMALE (MBPS)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
AWS	30 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Azure	10 Gbit/s	10 Mbit/s	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

Remarque

La quantité d'achat minimale est différente de la configuration système minimale requise.

Tableau 4. Capacité groupée prise en charge pour les instances NetScaler BLX

GAMME DE PRODUITS	BANDE PASSANTE MAXIMALE (GBIT/S)	BANDE PASSANTE MINIMALE (MBIT/S)	INSTANCES MINIMALES	INSTANCES MAXIMALES	UNITÉ DE BANDE PASSANTE MINIMALE
BLX	100	10	1	1	10 Mbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau 5. Exigence de licence pour différents facteurs de forme

GAMME DE PRODUITS	ACHAT DE MATÉRIEL À CAPACITÉ NULLE	ABONNEMENT BANDE PASSANTE ET ÉDITION	ABONNEMENT D'INSTANCE
MPX	Licence requise	Licence requise	-
SDX	Licence requise	Licence requise	Licence requise
VPX	-	Licence requise	Licence requise
CPX	-	-	Licence requise
BLX	-	Licence requise	Licence requise

Configurer la capacité groupée NetScaler

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de concéder des licences aux instances NetScaler après April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge du LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à compter du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Pour utiliser la capacité groupée NetScaler, configurez NetScaler Console en tant que serveur de licences pour les instances NetScaler requises. Les instances NetScaler enregistrent et retirent des licences de NetScaler Console. Vous pouvez effectuer les tâches suivantes dans l'interface graphique de NetScaler Console :

- Téléchargez les fichiers de licence de capacité groupée (bande passante et pool d'instances) sur le serveur de licences.
- Allouez des licences du pool de licences aux instances NetScaler à la demande.
- Extraire les licences des instances NetScaler (MPX-Z /SDX-Z/VPX/CPX/BLX) en fonction de la capacité minimale et maximale de l'instance.
- Configurer la capacité en pool pour les instances NetScaler FIPS afin d'enregistrer ou d'extraire des licences.

Versions matérielles et logicielles prises en charge

Pour les versions matérielles et logicielles prises en charge pour la capacité en pool, consultez Capacité en pool NetScaler.

États de la capacité en pool NetScaler

Les états de la capacité en pool indiquent les exigences de licence sur une instance NetScaler. Les instances NetScaler configurées avec la capacité en pool affichent l'un des états suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Optimal** : L'instance fonctionne avec une capacité de licence appropriée.
- **Inadéquation de capacité** : L'instance fonctionne avec une capacité inférieure à celle configurée par l'utilisateur.
- **Grâce** : L'instance fonctionne avec une licence de grâce.
- **Grâce et inadéquation** : L'instance fonctionne en période de grâce mais avec une capacité inférieure à celle configurée par l'utilisateur.
- **Non disponible** : L'instance n'est pas enregistrée auprès de NetScaler Console pour la gestion, ou la communication NITRO de NetScaler Console vers les instances ne fonctionne pas.
- **Non allouée** : La licence n'est pas allouée dans l'instance.

Étape 1 - Appliquer les licences dans NetScaler Console

1. Dans NetScaler Console, accédez à **NetScaler Licensing > Pooled Licensing**.
2. Dans la section **Fichiers de licence**, sélectionnez **Ajouter un fichier de licence** et choisissez l'une des options suivantes :

   - **Télécharger les fichiers de licence depuis un ordinateur local**. Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger vers NetScaler Console.
   - **Utiliser le code d'accès à la licence**. Spécifiez le code d'accès à la licence que vous avez acheté auprès de Citrix. Ensuite, sélectionnez **Obtenir les licences**. Puis sélectionnez **Terminer**.

   REMARQUE

   À tout moment, vous pouvez ajouter d'autres licences à NetScaler Console à partir des **Paramètres de licence**.

3. Cliquez sur **Terminer**.

   Les fichiers de licence sont ajoutés à NetScaler Console. L'onglet **Informations d'expiration de la licence** répertorie les licences présentes dans NetScaler Console et le nombre de jours restants avant leur expiration.
4. Dans **Fichiers de licence**, sélectionnez un fichier de licence que vous souhaitez appliquer et cliquez sur **Appliquer les licences**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cette action permet aux instances NetScaler d'utiliser la licence sélectionnée comme capacité groupée.

Étape 2 - Enregistrer NetScaler Console en tant que serveur de licences

Pour enregistrer NetScaler Console en tant que serveur de licences auprès d'une instance NetScaler, suivez l'une des procédures :

- Via GUI
- Utiliser la CLI

Utiliser l'interface graphique pour enregistrer NetScaler Console en tant que serveur de licences

Dans l'interface graphique de NetScaler, enregistrez le serveur NetScaler Console en tant que serveur de licences.

1. Connectez-vous à l'interface graphique de NetScaler.
2. Accédez à **Système** > **Licences** > **Gérer les licences**.
3. Cliquez sur **Ajouter une nouvelle licence**.
4. Sélectionnez **Utiliser la gestion des licences à distance** et, sous **Mode de gestion des licences à distance**, sélectionnez **Licences en pool** dans la liste.
5. Dans le champ **Nom du serveur/adresse IP**, spécifiez l'adresse IP du serveur NetScaler Console.

   Pour un déploiement HA, utilisez une adresse IP flottante. Pour plus d'informations sur la configuration, consultez Configurer le déploiement haute disponibilité.

   > Pour un déploiement qui utilise une NetScaler Console autonome ou un agent, consultez Présentation des licences

6. Le port de licence par défaut est 27000.
7. Saisissez les informations d'identification de votre serveur NetScaler Console pour enregistrer une instance auprès de NetScaler Console, puis cliquez sur **Continuer**. Dans NetScaler Console, l'un des serveurs est le serveur de licences.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUES :

- Cochez la case **Valider le certificat** uniquement si NetScaler Console dispose d'un certificat numérique valide émis par une autorité de certification (CA) (sous **Paramètres > Administration > Paramètres SSL**).
- L'enregistrement de l'appareil peut échouer si NetScaler n'est accessible que via une adresse IP NAT. Vous pouvez toujours extraire la licence, mais NetScaler Console affiche ces instances NetScaler comme des instances non gérées.

8. Sous **Nom du profil de l'appareil**, spécifiez le profil d'instance que NetScaler Console peut utiliser pour accéder à l'instance. Ce profil d'instance contient le nom d'utilisateur et le mot de passe des instances que vous souhaitez ajouter à NetScaler Console. Le profil par défaut est **ns_nsroot_profile**. Si vous avez modifié les informations d'identification d'administrateur par défaut de vos instances, vous pouvez définir un nom de profil d'instance personnalisé.
9. Dans **Allouer des licences**, sélectionnez l'édition de licence et spécifiez la bande passante requise.

   Pour la première fois, allouez des licences dans NetScaler. Vous pouvez ensuite modifier ou libérer l'allocation de licences depuis l'interface graphique de NetScaler Console.

   a. Cliquez sur **Obtenir des licences**.

IMPORTANT :

Redémarrez à chaud l'instance si vous modifiez l'édition de la licence. Les modifications de configuration ne prennent effet qu'après le redémarrage de l'instance.

Utiliser la CLI pour ajouter NetScaler Console en tant que serveur de licences

Si une instance NetScaler n'a pas d'interface graphique, utilisez les commandes CLI suivantes pour ajouter le serveur NetScaler Console en tant que serveur de licences :

1. Connectez-vous à la console NetScaler.
2. Ajoutez l'adresse IP du serveur NetScaler Console :

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations, consultez Présentation des licences.

3. Affichez la bande passante de licence disponible sur le serveur de licences.

```
> sh ns licenseserverpool
```

Cette commande répertorie les licences en fonction du mode de licence spécifié lors de l'ajout du serveur de licences.

Exemple 1 :

Si le mode de licence spécifié est `CICO`, la sortie ne contient que les licences CICO.

Exemple 2 :

Si le mode de licence spécifié est `Pooled`, la sortie contient uniquement les licences de capacité groupée.

Exemple 3 :

Si le mode de licence spécifié est `vCPU`, la sortie contient uniquement les licences de CPU virtuel.

Pour afficher toutes les licences ensemble, exécutez la commande suivante :

```
> sh ns licenseserverpool -getallLicenses
```

Exemple de sortie :

4. Allouez la bande passante de licence à partir de l'édition de licence requise :

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify-
amount-license-bandwidth> -edition <specify-license-edition>
```

L'édition de licence peut être **Standard**, **Enterprise** ou **Platinum**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT

Redémarrez à chaud l'instance si vous modifiez l'édition de licence.

`reboot -w`

Les modifications de configuration ne prennent effet qu'après le redémarrage de l'instance.

Étape 3 - Allouer des licences groupées aux instances NetScaler

Pour allouer des licences de capacité en pool depuis l'interface graphique de NetScaler Console :

1. Connectez-vous à NetScaler Console.
2. Accédez à **Infrastructure > Licenses > Bandwidth Licenses > Pooled Capacity**.

   La capacité d'instance FIPS apparaît uniquement si vous téléchargez des licences d'instance FIPS vers NetScaler Console.
3. Cliquez sur le pool de licences que vous souhaitez gérer.

   REMARQUE

   Le champ **Allocated Capacity** ne reflète pas immédiatement la bande passante modifiée. La modification de la bande passante prend effet après le redémarrage à chaud de NetScaler.

   Dans **Allocation Details**, les champs **Requested** et **Applied** sont mis à jour lorsque vous modifiez l'allocation de bande passante de l'instance.
4. Sélectionnez une instance NetScaler dans la liste des instances disponibles en cliquant sur le bouton **>**.

   Instances en pool dans NetScaler Console(/en-us/netscaler-application-delivery-management-software/media/pooled-licenses-manage-licenses-3.png)

   La colonne **LICENSE STATUS** affiche les messages d'état d'allocation de licence correspondants.

   REMARQUE :

   L'onglet **Unmanaged Instances** affiche les instances découvertes mais non gérées dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instances non gérées(/en-us/netscaler-application-delivery-management-software/media/unmanaged-instances.png)

5. Cliquez sur **Change allocation** ou **Release allocation** pour modifier l'allocation de licence.
6. Une fenêtre contextuelle avec les licences disponibles sur le serveur de licences apparaît.
7. Vous pouvez choisir l'allocation de bande passante ou d'instance à l'instance en définissant les options de la liste **Allouer**. Après avoir fait vos sélections, cliquez sur **Allouer**.
8. Vous pouvez également modifier l'édition de licence allouée à partir des options de la liste dans la **fenêtre Modifier l'allocation de licence**.

   Fenêtre Modifier l'allocation de licence(/en-us/netscaler-application-delivery-management-software/media/change-license-allocation-10.png)

   REMARQUE

   Redémarrez à chaud une instance si vous modifiez l'édition de la licence.

Pour plus d'informations sur la modification de l'allocation de bande passante, consultez la vidéo associée :

<iframe src="https://www.youtube.com/embed/AMaHr-ska8s" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Configurer la capacité en pool sur les instances NetScaler

Vous pouvez configurer des licences de capacité en pool sur les instances NetScaler suivantes :

- Instances NetScaler
- Instances NetScaler VPX™
- Paire haute disponibilité NetScaler

Instances NetScaler MPX™

MPX-Z est l'appliance NetScaler MPX avec capacité en pool activée. MPX-Z prend en charge le regroupement de bande passante pour les licences d'édition Premium, Advanced ou Standard.

MPX-Z nécessite des licences de plate-forme avant de pouvoir se connecter au serveur de licences. Vous pouvez installer la licence de plate-forme MPX-Z de l'une des manières suivantes :

- Téléchargement du fichier de licence à partir d'un ordinateur local.
- Utilisation du numéro de série matériel de l'instance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le code d'accès à la licence de la section **Système** > **Licences** de l'interface graphique de l'instance.

Si vous supprimez la licence de plate-forme MPX-Z, la fonctionnalité de capacité groupée est désactivée. Les licences d'instance sont libérées vers le serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance MPX-Z sans redémarrage. Un redémarrage n'est nécessaire que si vous souhaitez modifier l'édition de la licence.

REMARQUE :

Lorsque vous redémarrez l'instance, elle extrait automatiquement les licences groupées requises pour sa capacité configurée.

Instances NetScaler VPX

Une instance NetScaler VPX avec capacité groupée activée peut extraire des licences d'un pool de bande passante (éditions Premium/Advanced/Standard). Vous pouvez utiliser l'interface graphique de NetScaler pour extraire des licences du serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance VPX sans redémarrage. Un redémarrage n'est nécessaire que si vous souhaitez modifier l'édition de la licence.

REMARQUE :

Lorsque vous redémarrez l'instance, les licences de capacité groupée configurées sont automatiquement extraites du serveur NetScaler Console.

Paire haute disponibilité NetScaler

Avant de commencer, assurez-vous que le serveur NetScaler Console est configuré en tant que serveur de licences. Pour plus d'informations, consultez Configurer NetScaler Console en tant que serveur de licences.

Pour les instances NetScaler configurées en mode haute disponibilité, vous devez configurer la capacité mutualisée sur chaque nœud de la paire haute disponibilité. Pour les nœuds principal et secondaire, vous devez allouer des licences de la même capacité. Par exemple, si vous souhaitez une capacité de 1 Gbit/s de chaque instance de la paire HA, vous avez besoin du double de la

© 1997–2026 Citrix Systems, Inc. All rights reserved.

capacité (2 Gbit/s) du pool commun. Vous pouvez ensuite allouer une capacité de 1 Gbit/s à chaque nœud.

Pour allouer une licence de pool à chaque nœud de la paire, suivez les étapes décrites dans Allouer des licences mutualisées aux instances NetScaler. Allouez d'abord la licence au premier nœud, puis répétez les mêmes étapes pour allouer la licence au second nœud.

Mettre à niveau une licence perpétuelle dans NetScaler VPX vers la capacité groupée NetScaler

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou la version 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité avec ces exigences sans responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Les instances NetScaler VPX avec licence perpétuelle peuvent être mises à niveau vers une licence de capacité groupée NetScaler. La mise à niveau vers une licence de capacité groupée vous permet d'allouer des licences du pool de licences aux instances VPX à la demande. Vous pouvez également configurer une licence de capacité groupée pour les instances NetScaler configurées en mode haute disponibilité. Pour configurer une licence de capacité groupée pour les instances VPX en mode haute disponibilité, consultez Mise à niveau de la licence perpétuelle dans une paire haute disponibilité NetScaler VPX vers la capacité groupée NetScaler.

Prérequis

Pour passer à la capacité groupée NetScaler :

1. Dans un navigateur Web, saisissez l'adresse IP de l'instance VPX, telle que `<http://192.168.100.1>`.
2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Dans l'onglet **Configuration**, accédez à **Système > Licences** et cliquez sur **Gérer les licences**.
5. Sur la page **Licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Sur la page **Licences**, choisissez **Utiliser la gestion des licences à distance** et effectuez les opérations suivantes :

   ☐

   a. Dans la liste déroulante **Mode de gestion des licences à distance**, choisissez **Licences en pool**.

   b. Dans le champ **Nom du serveur/Adresse IP**, saisissez les détails du serveur de licences.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Cliquez sur **Continuer**.

7. Dans **Allouer des licences**, effectuez les opérations suivantes :

   a. Sélectionnez l'édition de licence dans la liste déroulante.

   

   b. Allouez la bande passante à l'appliance NetScaler à partir du menu **Allouer** et cliquez sur **Obtenir les licences**.

   

8. Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance.

   Redémarrer l'instance NetScaler (/en-us/netscaler-application-delivery-management-software/media/upgrade-license5.jpg)

9. Dans la boîte de dialogue Confirmer, cliquez sur **Oui**.
10. Une fois l'instance VPX redémarrée, connectez-vous à l'instance. Sur la page **Bienvenue**, cliquez sur **Continuer**.

    La page **Licences** affiche toutes les fonctionnalités sous licence sur l'appliance NetScaler VPX. Cliquez sur **X**.

11. Accédez à **Système > Licences** et cliquez sur **Gérer les licences**.

    Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de licence et de la bande passante allouée.

Mettre à niveau la licence perpétuelle dans une paire haute disponibilité NetScaler VPX vers la capacité groupée NetScaler

Pour les instances VPX configurées en mode haute disponibilité, vous devez configurer la capacité groupée sur les instances principale et secondaire de la paire HA. Pour les deux instances, principale et secondaire, vous devez allouer des licences de même capacité. Par exemple, si vous souhaitez une capacité de 1 Gbit/s de chaque instance de la paire HA, vous avez besoin du double de la capacité (2 Gbit/s) du pool commun. Ensuite, vous pouvez allouer 1 Gbit/s de capacité à chaque instance principale et secondaire de la paire HA.

Pour mettre à niveau une configuration HA NetScaler VPX existante vers la capacité groupée NetScaler :

1. Connectez-vous à l'instance VPX secondaire (nœud 2). Dans un navigateur Web, saisissez l'adresse IP de l'appliance NetScaler, telle que `http://192.168.100.1`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Sous l'onglet Configuration, accédez à **Système > Licences** et cliquez sur **Gérer les licences**.
5. Sur la page **Licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Choisissez **Utiliser la gestion des licences à distance** et effectuez les opérations suivantes :

   

   a. Dans la liste déroulante **Mode de gestion des licences à distance**, choisissez **Licences en pool**.
   b. Dans le champ **Nom du serveur/adresse IP**, saisissez les détails du serveur de licences.
   c. Assurez-vous que la case **Enregistrer auprès de NetScaler Console** est cochée et saisissez les informations d'identification de NetScaler Console, si vous souhaitez gérer les licences en pool de votre instance via NetScaler Console.
   d. Cliquez sur **Continuer**.
7. Dans **Allouer des licences**, effectuez les opérations suivantes :

   a. Sélectionnez l'édition de licence dans la liste déroulante.

      

   b. Allouez la bande passante à l'appliance NetScaler à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.

      

   c. Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'instance à chaud.

      
8. Dans la boîte de dialogue **Confirmer**, cliquez sur **Oui**.

   L'instance VPX redémarre.

   Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance. Une fois l'appliance opérationnelle avec la nouvelle licence, forcez un basculement en tapant `force ha failover`. Ce basculement garantit que la paire HA est en bon état de fonctionnement.
9. Après le basculement, connectez-vous à la nouvelle instance VPX secondaire (nœud 1) et répétez le même processus pour ajouter le nouveau secondaire au pool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si vous souhaitez modifier les instances principales et secondaires de la paire HA pour revenir à votre configuration de paire HA d'origine, forcez un basculement. Exécutez la commande suivante sur n'importe quelle instance de la paire HA :

```
> force ha failover
```

10. Pour vérifier que l'instance VPX est mise à niveau vers la licence de capacité groupée, connectez-vous aux instances principales et secondaires et suivez les étapes suivantes.

    a. Sur la page **Bienvenue**, cliquez sur **Continuer**.

    b. Sous l'onglet Configuration, accédez à **Système > Licences** et cliquez sur **Gérer les licences**. Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de la licence et de la bande passante allouée.

Mise à niveau d'une licence perpétuelle dans NetScaler MPX vers la capacité groupée NetScaler

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licence (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

Note : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

NetScaler MPX avec licence perpétuelle peut être mis à niveau vers une licence de capacité groupée NetScaler. La mise à niveau vers une licence de capacité groupée NetScaler vous permet d'allouer des licences du pool de licences aux appliances NetScaler à la demande. Vous pouvez également configurer la licence de capacité groupée NetScaler pour les instances NetScaler configurées en mode haute disponibilité. Pour configurer la licence de capacité groupée NetScaler pour les instances NetScaler MPX en mode haute disponibilité, consultez Mise à niveau de la licence perpétuelle dans une paire haute disponibilité NetScaler MPX vers la capacité groupée NetScaler.

REMARQUE

La conversion d'une licence perpétuelle en une licence de capacité groupée est un processus à sens unique pour le droit à la licence. Vous ne pouvez pas annuler la licence de capacité groupée pour revenir à une licence perpétuelle. **Important**

Pour mettre à niveau NetScaler MPX vers une licence de capacité groupée NetScaler, vous devez télécharger la licence MPX-Z sur l'appliance.

Pour mettre à niveau vers la capacité groupée NetScaler :

1. Dans un navigateur Web, saisissez l'adresse IP du NetScaler, telle que `<http://192.168.100.1>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Téléchargez la licence de capacité zéro (licence MPX-Z). Sous l'onglet Configuration, accédez à **Système** \> **Licences**.
5. Dans le volet d'informations, cliquez sur **Gérer les licences**, puis sur Ajouter **Nouvelle licence**.
6. Sur la page **Licences**, sélectionnez **Télécharger les fichiers de licence** et cliquez sur **Parcourir** pour sélectionner la licence de capacité zéro depuis votre machine locale.
7. Une fois la licence téléchargée, cliquez sur **Redémarrer** pour redémarrer l'appliance.

   AVERTISSEMENT

   Après l'application de la licence MPX-Z, les fonctionnalités, y compris le déchargement SSL sur l'appliance, deviennent sans licence. L'appliance cesse de traiter les requêtes HTTPS.

   Si l'option **Accès sécurisé uniquement** est activée sur l'appliance avant la mise à niveau, vous ne pouvez pas vous connecter à l'appliance via l'interface graphique de NetScaler Console, en utilisant HTTPS.
8. Sur la page **Confirmer**, cliquez sur **Oui**.
9. Après le redémarrage de l'appliance, connectez-vous à l'appliance.
10. Sur la page d'accueil, cliquez sur la section **Licences**.

    
11. Dans la section **Serveur de licences**, effectuez les opérations suivantes :

    

    a. Dans le champ **Nom du serveur/Adresse IP**, saisissez les détails du serveur de licences.
    b. Dans le champ **Port de licence**, saisissez le port du serveur de licences. Valeur par défaut : 27000.
    c. Si vous souhaitez gérer les licences de pool de votre instance via NetScaler Console, cochez la case **S'enregistrer auprès du serveur de licences pour la gérabilité** et saisissez les informations d'identification de NetScaler Console.
    d. Cliquez sur **Continuer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Dans **Allouer des licences**, effectuez les opérations suivantes :

    a. Sélectionnez l'édition de licence dans la liste déroulante.

    b. Allouez la bande passante à NetScaler à partir du menu **Allouer** et cliquez sur **Obtenir les licences**.

    c. Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance.

13. Une fois que NetScaler MPX a redémarré, connectez-vous à NetScaler MPX. Sur la page **Bienvenue**, cliquez sur **Continuer**.

    La page **Licences** répertorie toutes les fonctionnalités sous licence.

14. Accédez à **Système > Licences** et cliquez sur **Gérer les licences**.

    Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de licence et de la bande passante allouée.

    Détails de la licence du serveur de licences(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-10.jpg)

Mise à niveau de la licence perpétuelle dans une paire haute disponibilité NetScaler MPX vers la capacité groupée NetScaler

Pour les appliances MPX configurées en mode haute disponibilité, vous devez configurer la capacité groupée sur les instances NetScaler principale et secondaire de la paire HA. Allouez des licences de même capacité aux instances NetScaler principale et secondaire de la paire HA. Par exemple, si vous souhaitez une capacité de 1 Gbit/s pour chaque instance de la paire HA, vous devez allouer une capacité de 2 Gbit/s à partir du pool commun. Avec une capacité de 2 Gbit/s, vous pouvez allouer 1 Gbit/s à chaque instance NetScaler principale et secondaire de la paire HA.

IMPORTANT

Pour mettre à niveau NetScaler MPX afin d'utiliser la licence de capacité groupée NetScaler, vous devez télécharger le MPX-Z sur l'appliance.

Prérequis

Assurez-vous de télécharger la licence MPX-Z sur les instances principale et secondaire de la paire HA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour télécharger la licence MPX-Z sur les instances NetScaler MPX de la paire HA :

1. Dans un navigateur Web, saisissez l'adresse IP de l'appliance, telle que `<http://192.168.100.1>`.
2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Téléchargez la licence de capacité zéro (licence MPX-Z). Sous l'onglet **Configuration**, accédez à **Système \> Licences**.
5. Dans le volet des détails, cliquez sur **Gérer les licences**, puis sur **Ajouter une nouvelle licence**.
6. Dans la page **Licences**, sélectionnez **Télécharger les fichiers de licence** et cliquez sur **Parcourir** pour sélectionner la licence de capacité zéro depuis votre machine locale.

   Une fois la licence téléchargée, vous êtes invité à redémarrer l'appliance.
7. Cliquez sur **Redémarrer** pour redémarrer l'appliance.
8. Sur la page **Confirmer**, cliquez sur **Oui**.

Pour mettre à niveau une configuration HA existante vers la capacité groupée NetScaler :

1. Connectez-vous à l'instance NetScaler MPX secondaire. Dans un navigateur Web, saisissez l'adresse IP de NetScaler, telle que `<http://192.168.100.1>`.
2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur la section **Licences**.

   
4. Dans la section **Serveur de licences**, effectuez les opérations suivantes :

   
   a. Dans le champ **Nom du serveur/Adresse IP**, saisissez les détails du serveur de licences.
   b. Dans le champ **Port de licence**, saisissez le port du serveur de licences. Valeur par défaut : 27000.
   c. Si vous souhaitez gérer les licences de pool de votre instance via NetScaler Console, cochez la case **S'enregistrer auprès du serveur de licences pour la gérabilité** et saisissez les informations d'identification de NetScaler Console.
   d. Cliquez sur **Continuer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Dans **Allouer des licences**, effectuez les opérations suivantes :

   a. Sélectionnez l'édition de licence dans la liste déroulante.

   

   b. Allouez la bande passante à NetScaler à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.

   

   c. Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance. Une fois l'appliance opérationnelle avec la nouvelle licence, forcez un basculement en tapant `force ha failover`. Ce basculement garantit que la paire HA est en bon état de fonctionnement.

6. Connectez-vous à l'appliance NetScaler MPX principale existante et redémarrez l'appliance. Effectuez les opérations suivantes :

   a. Dans un navigateur Web, tapez l'adresse IP du NetScaler, par exemple `<http://192.168.100.1>`.

   b. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

   c. Sur la page **Bienvenue**, cliquez sur **Continuer**.

   d. Sous l'onglet **Configuration**, cliquez sur **Système**.

   e. Sur la page **Système**, cliquez sur **Redémarrer**.

   f. Sur la page **Redémarrer**, sélectionnez **Redémarrage à chaud** et cliquez sur **OK**.

   

   Après le redémarrage du NetScaler MPX principal, il devient le NetScaler MPX secondaire dans la paire HA. Si vous souhaitez modifier les instances principale et secondaire de la paire HA pour retrouver votre configuration de paire HA d'origine, forcez un basculement. Exécutez la commande suivante sur n'importe quelle instance de la paire HA :

```
> force ha failover
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mettre à niveau une licence perpétuelle dans un NetScaler SDX vers la capacité groupée NetScaler

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- NetScaler Console Service : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, la licence basée sur des fichiers est obsolète à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser la licence basée sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront non licenciées lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité avec ces exigences sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
NetScaler SDX avec une licence perpétuelle peut être mis à niveau vers une licence de capacité groupée NetScaler. La mise à niveau vers une licence de capacité groupée NetScaler vous permet d'allouer des licences du pool de licences à NetScaler à la demande. Vous pouvez également configurer une licence de capacité groupée NetScaler pour les instances NetScaler configurées en mode haute disponibilité.

IMPORTANT

La conversion d'une licence perpétuelle en une licence de capacité groupée est un processus d'attribution de licence à sens unique. Vous ne pouvez pas revenir d'une licence de capacité groupée à une licence perpétuelle.

- Pour mettre à niveau NetScaler SDX vers la licence de capacité groupée NetScaler, vous devez télécharger la licence SDX-Z sur l'appliance.
- Assurez-vous d'avoir l'autorisation d'ajouter des instances NetScaler dans NetScaler Console.
- Pour s'assurer qu'il n'y a aucun impact sur les licences actuelles, le client doit allouer le même nombre d'instances et la même bande passante que ceux disponibles dans le cadre de la licence perpétuelle.

Pour passer à la capacité groupée NetScaler :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler SDX, telle que `<http://192.168.100.1>`.
2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Téléchargez la licence de capacité zéro. Dans l'onglet Configuration, accédez à **Système** > **Licences**.
5. Sur la page **Gérer les licences**, cliquez sur **Ajouter un fichier de licence**.
6. Dans la page **Licences**, sélectionnez **Télécharger les fichiers de licence depuis un ordinateur local** et cliquez sur **Parcourir** pour sélectionner la licence de capacité zéro depuis votre machine locale. Ensuite, cliquez sur **Terminer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Une fois la licence de capacité zéro appliquée avec succès, la section **Licences groupées** apparaît sur la page **Licences**.

REMARQUE

Pour supprimer l'ancien fichier de licence, vous n'avez pas besoin de redémarrer votre NetScaler SDX, ce qui évite les temps d'arrêt. Pour plus d'aide, contactez le support NetScaler.

7. Dans la section **Licences groupées**, effectuez les opérations suivantes :

   a. Dans le champ **Nom du serveur de licences ou adresse IP**, saisissez les détails du serveur de licences. Si vous souhaitez configurer le serveur NetScaler Console en tant que serveur de licences, spécifiez l'adresse IP du serveur NetScaler Console.

   b. Dans le champ **Numéro de port**, saisissez le port du serveur de licences. Valeur par défaut : 27000.

   c. Spécifiez le **Nom d'utilisateur** et le **Mot de passe** du serveur de licences.

      - Pour le serveur NetScaler Console, saisissez les informations d'identification de l'administrateur.
      - Pour l'agent NetScaler Console, saisissez les informations d'identification de l'agent.

   d. Cliquez sur **Obtenir les licences**.



8. Dans la fenêtre **Allouer des licences**, spécifiez les instances et la bande passante requises, puis cliquez sur **Allouer**.

   Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de licence, ainsi que les instances et la bande passante allouées à partir du pool.



REMARQUE

La mise à niveau d'une licence perpétuelle vers la capacité groupée ne nécessite pas le redémarrage de l'appliance SDX.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Capacité groupée NetScaler sur les instances NetScaler en mode cluster

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits sur l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x et ultérieures. Cependant, les licences basées sur des fichiers sont obsolètes à partir du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou la version 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au April 15 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le April 15 2026 car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou les réglementations l'interdisent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité avec ces exigences sans engager sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Vous pouvez configurer la capacité groupée NetScaler sur les instances NetScaler configurées en tant que cluster. Voici les prérequis pour configurer la capacité groupée sur les instances NetScaler en mode cluster :

- Les instances fonctionnent individuellement en mode de licence de capacité groupée pour former le cluster.
- Toutes les instances doivent fonctionner avec la même bande passante.
- Toutes les instances ont extrait la capacité groupée de la même console NetScaler.
- De nouvelles instances ne peuvent pas être ajoutées à un cluster NetScaler existant à moins que leur capacité et les configurations de la console NetScaler ne soient identiques à celles des instances existantes dans le cluster.

Toute extraction de capacité du cluster NetScaler attribue la même capacité à tous les nœuds du cluster et la bande passante extraite = bande passante fournie * nombre de nœuds.

Par exemple, si vous extrayez 50 Mbps de bande passante du cluster NetScaler, et que le cluster comprend 12 instances, chaque instance reçoit automatiquement 50 Mbps. Et, 600 Mbps sont extraits du pool.

REMARQUE

Si une ou plusieurs instances du cluster ne répondent plus, le cluster continue de traiter le trafic avec la capacité des instances restantes.

Allouer la capacité groupée NetScaler à un cluster NetScaler

Allouez les licences à chaque nœud du cluster séparément. En effet, les commandes de propagation et de synchronisation des licences entre les nœuds du cluster sont désactivées.

Répétez la procédure suivante sur chaque nœud du cluster :

1. Dans un navigateur Web, tapez l'adresse IP de NetScaler (NSIP). Par exemple, `http://192.168.100.1`.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Sous l'onglet **Configuration**, accédez à **Système > Licences > Gérer les licences**. Cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Utiliser la licence groupée**.
4. Entrez le nom ou l'adresse du serveur de licences dans le champ **Nom/adresse IP du serveur**.
5. Si vous souhaitez gérer les licences de pool de votre instance via NetScaler Console, cochez la case **S'enregistrer auprès de NetScaler Console pour la gérabilité** et entrez les informations d'identification de NetScaler Console.
6. Sélectionnez l'édition de la licence et la bande passante requise, puis cliquez sur **Obtenir les licences**.



7. Vous pouvez modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation**.



8. Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences.

REMARQUE

L'allocation de bande passante doit être un multiple entier de l'unité de bande passante minimale du facteur de forme correspondant.



9. Vous pouvez allouer de la bande passante ou des instances à l'instance NetScaler à partir de la liste déroulante **Allouer**. Cliquez ensuite sur **Obtenir des licences**.
10. Vous pouvez choisir l'édition de licence et la bande passante requise dans les listes déroulantes de la fenêtre contextuelle.

REMARQUE

Un redémarrage n'est pas nécessaire si vous modifiez l'allocation de bande passante, mais un redémarrage à chaud est requis si vous modifiez l'édition de licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allouer la capacité groupée NetScaler à un cluster NetScaler à l'aide de l'interface de ligne de commande

Allouez les licences à chaque nœud de cluster séparément. En effet, les commandes de propagation et de synchronisation des licences entre les nœuds du cluster sont désactivées.

Répétez la procédure suivante sur chaque nœud de cluster :

1. Dans un client SSH, entrez l'adresse IP de NetScaler (NSIP) et connectez-vous à l'aide des informations d'identification de l'administrateur.
2. Pour ajouter un serveur de licences, entrez la commande suivante :

   ```
   add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number >]
   ```

3. Pour afficher les licences disponibles sur le serveur de licences, entrez la commande suivante :

   ```
   sh licenseserverpool
   ```

4. Pour attribuer une licence à l'appliance NetScaler VPX, entrez la commande suivante :

   ```
   set capacity –platform V\[S/E/P\]\[Bandwidth\]
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Archiver et extraire les licences NetScaler VPX et NetScaler BLX

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le Service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits sur l'ensemble de la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : Pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge de LAS pour Console sur site est à partir de la version 14.1-51.x et versions ultérieures. Cependant, les licences basées sur des fichiers sont obsolètes à compter du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le 15th April 2026 car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront non licenciées lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Vous pouvez allouer des licences NetScaler VPX et NetScaler BLX aux instances NetScaler à la demande depuis NetScaler Console. Le logiciel NetScaler Console stocke et gère les licences, qui disposent d'un cadre de licences offrant un provisionnement de licences évolutif et automatisé.
Une instance peut extraire la licence de NetScaler Console lorsqu'elle est provisionnée.
Lorsqu'une instance est supprimée ou détruite, l'instance réintègre sa licence au logiciel NetScaler Console.

Prérequis

Assurez-vous que les prérequis suivants sont remplis :

- Vous utilisez une image NetScaler VPX exécutant la version logicielle 12.0.Par exemple : NSVPX-ESX-12.0-xx.xx_nc.zip
- Vous avez installé NetScaler Console exécutant la version 12.0.Par exemple : MAS-ESX-12.0-xx.xx.zip

REMARQUE

Pour gérer les licences NetScaler VPX existantes via NetScaler Console, vous devez réhéberger les licences sur NetScaler Console.

Installation des licences dans NetScaler Console

REMARQUE

Avant d'installer les licences, redémarrez l'appliance virtuelle NetScaler Console si vous avez modifié l'édition logicielle ou la bande passante.

Pour installer des fichiers de licence sur NetScaler Console :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler Console (par exemple, `<http://192.168.100.1>`).
2. Dans Nom d'utilisateur et Mot de passe, saisissez les informations d'identification de l'administrateur.
3. Accédez à **Infrastructure > Licences en pool**.
4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Télécharger des fichiers de licence depuis un ordinateur local** - Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur NetScaler Console.Pour ajouter des fichiers de licence, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.
- **Utiliser le code d'accès à la licence** - Citrix envoie par e-mail le code d'accès à la licence pour les licences que vous achetez.Pour ajouter des fichiers de licence, saisissez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir les licences**.

REMARQUE

Assurez-vous d'être connecté à Internet avant d'utiliser le code d'accès de licence pour installer les licences.

À tout moment, vous pouvez ajouter d'autres licences à NetScaler Console à partir de la page **Paramètres de licence**.

Vérification

Vous pouvez afficher les licences disponibles et allouées dans l'interface graphique de NetScaler Console.

Pour afficher les licences :

1. Dans un navigateur web, saisissez l'adresse IP de NetScaler Console (par exemple, `<http://192.168.100.1>`).
2. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sous l'onglet Configuration, accédez à **Infrastructure > Licences en pool > Licences VPX**.

   
4. Vous pouvez afficher les licences allouées dans le tableau sous la section des licences disponibles.

Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface graphique de NetScaler

1. Dans un navigateur web, saisissez l'adresse IP de l'instance NetScaler (par exemple, `<http://192.168.100.1>`).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. Sous l'onglet Configuration, accédez à **Paramètres > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Utiliser la gestion des licences à distance > Licences CICO**.
4. Saisissez les détails du serveur de licences dans le champ **Nom du serveur/Adresse IP**.
5. Dans **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de NetScaler Console et cliquez sur **Continuer**.

   
6. Sélectionnez l'édition de licence avec la bande passante requise, cliquez sur **Obtenir les licences**.

   
7. Cliquez sur **Redémarrer**, votre instance NetScaler redémarre.
8. Vous pouvez modifier ou libérer l'allocation de licence en accédant à **Système > Licences > Gérer les licences**, et en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation.**

   
9. Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences. Sélectionnez la licence requise, cliquez sur **Obtenir les licences**.

   

Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface de ligne de commande NetScaler

1. Dans un client SSH, saisissez l'adresse IP de l'instance NetScaler et connectez-vous à l'aide des informations d'identification de l'administrateur.
2. Pour ajouter un serveur de licences, saisissez la commande suivante :

   ```
   add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number >]
   ```

   
3. Pour afficher les licences disponibles sur le serveur de licences, saisissez la commande suivante :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sh licenseserverpool
```

4. Pour attribuer une licence à NetScaler, entrez la commande suivante :

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'API

Dans un navigateur web ou un client API, connectez-vous à l'instance NetScaler à l'aide des informations d'identification de l'administrateur.

Pour ajouter un serveur de licences :

1. Définissez le type de requête sur **Post**.
2. Définissez le chemin d'accès sur /nitro/v1/config/nslicensingserver.
3. Définissez la charge utile comme suit :

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

object= {“params”;{warning”:”yes”},”nslicensing server”;
{servername”:”\<NetScaler Console IP\>”, “port”:”27000”}}\\r\\n
```

NetScaler Console répond à la requête. L'exemple de réponse suivant indique le succès.

Pour afficher les licences disponibles sur le serveur de licences :

1. Définissez le type de requête sur **Get**.
2. Définissez le chemin d'accès sur /nitro/v1/config/nslicenseserverpool

NetScaler Console répond à la requête. L'exemple de réponse suivant montre le succès et la liste des licences disponibles sur le serveur de licences.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour attribuer une licence à NetScaler :

1. Définissez le type de requête sur **Post**.
2. Définissez le chemin d'accès sur /nitro/v1/config/nscapacity.
3. Définissez la charge utile comme suit :

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

{“nscapacity:{“platform”:”VE8000”}}\\r\\n
```

NetScaler Console répond à la requête. L'exemple de réponse suivant indique le succès.

Mettre à jour l'adresse IP d'un serveur de licences

Vous pouvez mettre à jour l'adresse IP du serveur de licences dans les instances NetScaler VPX et NetScaler BLX, sans aucun impact sur la bande passante de licence allouée sur l'instance et sans perte de données.

Mise à jour à l'aide de la CLI : Pour mettre à jour l'adresse IP du serveur de licences à l'aide de la CLI, tapez la commande suivante sur l'instance :

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Cette commande se connecte au nouveau serveur et libère les ressources associées au serveur de licences précédent.

Mise à jour à l'aide de l'interface graphique : Pour mettre à jour l'adresse IP du serveur de licences à l'aide de l'interface graphique, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**. Pour plus d'informations, consultez Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface graphique NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer les vérifications d'expiration pour les licences d'enregistrement et de retrait NetScaler VPX et NetScaler BLX

Vous pouvez désormais configurer le seuil d'expiration des licences NetScaler VPX et NetScaler BLX. En définissant des seuils, NetScaler Console envoie des notifications par e-mail ou SMS lorsqu'une licence est sur le point d'expirer. Un piège SNMP et une notification sont également envoyés lorsque la licence a expiré sur NetScaler Console.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur NetScaler Console.

Pour configurer les vérifications d'expiration de licence :

1. Accédez à **Infrastructure > Pooled Licensing**.
2. Dans la page **Paramètres de licence**, sous la section **Informations sur l'expiration de la licence**, vous trouverez les détails des licences qui vont expirer :
    - **Fonctionnalité** : Type de licence qui va expirer.
    - **Nombre** : Nombre de serveurs virtuels ou d'instances affectés.
    - **Jours avant expiration** : Nombre de jours avant l'expiration de la licence.
3. Dans la section **Paramètres de notification**, cliquez sur l'icône **Modifier** et spécifiez le seuil d'alerte. Vous pouvez définir un pourcentage de la capacité de licence groupée à utiliser pour avertir les administrateurs.
4. Choisissez le type de notification que vous souhaitez envoyer en cochant la case appropriée. Les types de notification sont les suivants :
    a. **Profil de messagerie** : Spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.
    b. **Profil SMS** : Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos licences sont sur le point d'expirer.
5. Ensuite, spécifiez quand vous souhaitez envoyer la notification en termes de nombre de jours avant l'expiration de la licence.
6. Cliquez sur **Enregistrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licences de processeur virtuel NetScaler

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, sera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles avec LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : la prise en charge de LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à compter du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer à LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge LAS.

Toutes les autres formes de licences NetScaler héritées, telles que Pooled vCPU, CICO, perpétuelles, ne seront pas prises en charge avec LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité avec ces exigences sans engager

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sa responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

REMARQUE :

La licence vCPU n'est plus disponible à l'achat. Pour plus d'informations, consultez Licences.

Les administrateurs de centres de données comme vous se tournent vers de nouvelles technologies qui simplifient les fonctions réseau tout en offrant des coûts réduits et une plus grande évolutivité. La nouvelle architecture de centre de données doit inclure au minimum les fonctionnalités suivantes :

- Mise en réseau définie par logiciel (SDN)
- Virtualisation des fonctions réseau (NFV)
- Virtualisation du réseau (NV)
- Micro-services

Un tel mouvement exige également que les exigences logicielles soient dynamiques, flexibles et agiles pour répondre aux besoins commerciaux en constante évolution. Les licences doivent également être gérées par un outil de gestion centralisé offrant une visibilité complète sur leur utilisation.

Licences de CPU virtuel pour NetScaler VPX

Auparavant, les licences NetScaler VPX étaient allouées en fonction de la consommation de bande passante par les instances. Un NetScaler VPX est limité à l'utilisation d'une bande passante spécifique et d'autres métriques de performance basées sur l'édition de licence à laquelle il est lié. Pour augmenter la bande passante disponible, vous devez passer à une édition de licence qui offre plus de bande passante. Dans certains scénarios, l'exigence de bande passante peut être moindre, mais l'exigence est plus élevée pour d'autres performances L7 telles que le SSL TPS et le débit de compression. La mise à niveau de la licence NetScaler VPX pourrait ne pas être adaptée dans de tels cas. Cependant, vous pourriez toujours devoir acheter une licence avec une bande passante importante pour débloquer les ressources système nécessaires au traitement intensif du CPU. NetScaler Console prend désormais en charge l'allocation de licences aux instances NetScaler en fonction des exigences en CPU virtuel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dans la fonctionnalité de licence basée sur l'utilisation du CPU virtuel, la licence spécifie le nombre de CPU auxquels un NetScaler VPX particulier a droit. Ainsi, NetScaler VPX peut extraire des licences du serveur de licences uniquement pour le nombre de CPU virtuels qui y sont exécutés. NetScaler VPX extrait les licences en fonction du nombre de CPU exécutés dans le système. NetScaler VPX ne prend pas en compte les CPU inactifs lors de l'extraction des licences.

Similaire aux fonctionnalités de capacité de licence en pool et de licence CICO, le serveur de licences NetScaler Console gère un ensemble distinct de licences de CPU virtuel. Ici aussi, les trois éditions gérées pour les licences de CPU virtuel sont Standard, Advanced et Premium. Ces éditions débloquent le même ensemble de fonctionnalités que celles débloquées par les éditions pour les licences de bande passante.

Il peut y avoir un changement dans le nombre de CPU virtuels ou un changement dans l'édition de la licence. Dans un tel cas, vous devez toujours arrêter l'instance avant d'initier une demande pour un nouvel ensemble de licences. Redémarrez NetScaler VPX après avoir extrait les licences.

Pour configurer le serveur de licences dans NetScaler VPX à l'aide de l'interface graphique :

1. Dans NetScaler VPX, accédez à **Système > Licences** et cliquez sur **Gérer les licences**.
2. Sur la page **Licence**, cliquez sur **Ajouter une nouvelle licence**.
3. Sur la page **Licences**, sélectionnez l'option **Utiliser la licence à distance**.
4. Sélectionnez **Licences CPU** dans la liste **Mode de licence à distance**.
5. Saisissez l'adresse IP du serveur de licences et le numéro de port.
6. Cliquez sur **Continuer**.

   REMARQUE

   Vous devez toujours enregistrer l'instance NetScaler VPX auprès de NetScaler Console. Si ce n'est pas déjà fait, activez **Enregistrer auprès de NetScaler Console** et saisissez les informations d'identification de connexion à NetScaler Console.

7. Dans la fenêtre **Allouer des licences**, sélectionnez le type de licence. La fenêtre affiche le nombre total et disponible de CPU virtuels, ainsi que les CPU pouvant être alloués. Cliquez sur **Obtenir des licences**.
8. Cliquez sur **Redémarrer** sur la page suivante pour appliquer la licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Vous pouvez également libérer la licence actuelle et en extraire une d'une édition différente. Par exemple, vous utilisez déjà une licence d'édition Standard sur votre instance. Vous pouvez libérer cette licence, puis en extraire une de l'édition Advanced.

Configuration d'un serveur de licences dans la licence NetScaler VPX à l'aide de l'interface de ligne de commande

Dans la console NetScaler VPX, saisissez les commandes suivantes pour les deux tâches suivantes :

1. Pour ajouter le serveur de licences à NetScaler VPX :

```
add licenseserver <IP address of the license server>
```

2. Pour demander les licences :

```
set capacity -vcpu - edition premium
```

Lorsque vous y êtes invité, redémarrez l'instance en tapant la commande suivante :

```
reboot -w
```

Mettre à jour l'adresse IP d'un serveur de licences

Vous pouvez mettre à jour l'adresse IP du serveur de licences dans l'instance NetScaler VPX, sans aucun impact sur la bande passante de licence allouée sur l'instance et sans perte de données. Pour mettre à jour l'adresse IP du serveur de licences, tapez la commande suivante sur l'instance NetScaler VPX :

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Cette commande se connecte au nouveau serveur et libère les ressources associées au serveur de licences précédent.

Gestion des licences de CPU virtuelles sur NetScaler Console

1. Dans NetScaler Console, accédez à **Infrastructure > Licences en pool > VCPU en pool**.
2. La page affiche les licences allouées pour chaque type d'édition de licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur le nombre dans chaque graphique en anneau pour afficher les instances NetScaler qui utilisent cette licence.



Licences de CPU virtuelles pour NetScaler CPX

Lors du provisionnement de l'instance NetScaler CPX, vous pouvez configurer l'instance NetScaler CPX pour qu'elle emprunte des licences au serveur de licences en fonction de l'utilisation du CPU sur l'instance.

NetScaler CPX s'appuie sur le serveur de licences, exécuté sur NetScaler Console, pour gérer les licences. NetScaler CPX emprunte les licences au serveur de licences lors de son démarrage. Les licences sont restituées au serveur de licences lorsque NetScaler CPX s'arrête.

Vous pouvez télécharger l'image NetScaler CPX depuis le registre de conteneurs Quay en utilisant la commande 'docker pull' et la déployer dans votre environnement.

Trois types de licences sont disponibles pour les licences NetScaler CPX :

1. Licences d'abonnement vCPU prises en charge pour NetScaler CPX et VPX
2. Licences de capacité groupée
3. Licences CP1000 prenant en charge un ou plusieurs vCPU pour NetScaler CPX uniquement

Pour configurer les licences d'abonnement vCPU lors du provisionnement de l'instance NetScaler CPX :

Spécifiez le nombre de licences vCPU utilisées par l'instance NetScaler CPX.

- Cette valeur est saisie en tant que variable d'environnement via Docker, Kubernetes ou Mesos/Marathon.
- La variable cible est « CPX_CORES ». NetScaler CPX peut prendre en charge de 1 à 16 cœurs.

Pour spécifier 2 cœurs, vous pouvez exécuter la commande docker run comme suit :

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2
```

Lors du provisionnement d'une instance NetScaler CPX, définissez le serveur de licences NetScaler comme variable d'environnement dans la commande **docker run** comme indiqué ci-dessous :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT>
cpx:11.1
```

Où,

- \<*LS*_*IP*_*ADDRESS*\> est l'adresse IP du serveur de licences NetScaler.
- \<*LS*_*PORT*\> est le port du serveur de licences NetScaler. Par défaut, le port est 27000.

REMARQUE

Par défaut, l'instance NetScaler CPX extrait la licence du pool d'abonnement vCPU. L'instance NetScaler CPX extrait « n » licences si l'instance s'exécute avec « n » CPU.

Pour configurer les licences de capacité groupée NetScaler ou CP1000 lors du provisionnement de l'instance NetScaler CPX :

Si vous souhaitez extraire la licence pour l'instance NetScaler CPX à l'aide de la licence groupée (basée sur la bande passante) ou du pool privé NetScaler CPX (CP1000 ou basé sur le pool privé), vous devez fournir les variables d'environnement en conséquence.

Par exemple,

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e
PLATFORM=CP1000 cpx:11.1
```

CP1000. Cette commande déclenche l'extraction du pool CP1000 (pool privé NetScaler CPX). L'instance NetScaler CPX récupère ensuite « n » instances pour « n » cœurs spécifiés pour CPX_CORES. Le cas d'utilisation le plus courant est de spécifier n = 1 pour l'extraction d'une seule instance. Les cas d'utilisation de NetScaler CPX multicœur extraient « n » vCPU (où « n » est compris entre 1 et 7).

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e
BANDWIDTH=2000 cpx:11.1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Capacité groupée. Cette commande extrait une licence du pool d'instances et consomme 1000 Mbps de bande passante du pool de bande passante Premium, tout en permettant à NetScaler CPX de fonctionner jusqu'à 2000 Mbps. Dans la licence groupée, les premiers 1000 Mbps ne sont pas facturés.

REMARQUE

Spécifiez le nombre correspondant de vCPU pour la bande passante cible souhaitée lors de l'extraction du pool de bande passante, comme détaillé dans le tableau suivant :

NOMBRE DE CŒURS (VCPU)	BANDE PASSANTE MAXIMALE
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps
5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

Comportements attendus en cas de problèmes

Voici les comportements attendus des serveurs de licences et des instances NetScaler lorsqu’ils rencontrent les problèmes décrits :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le serveur de licences ne répond plus

IMPORTANT :

Le système de licences basé sur des fichiers (également appelé droits gérés manuellement), traditionnellement utilisé pour activer divers composants sur site, arrivera en fin de vie (EOL) le April 15, 2026. Le service d'activation de licences (LAS) est la technologie de nouvelle génération pour les activations de produits dans toute la suite de produits Citrix. Le LAS sera le seul moyen d'activer et de licencier les instances NetScaler après le April 15, 2026, prenant en charge les licences NetScaler Flexed (CPL/UHMC), les licences NetScaler Pooled héritées et les licences NetScaler Fixed term Bandwidth. Pour rester pris en charge, vos déploiements NetScaler et NetScaler Console doivent être sur une version compatible LAS.

Les versions minimales requises de NetScaler® compatibles LAS sont :

- NetScaler ADC : 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1-51.x, 13.1-60.x
- Service NetScaler Console : pris en charge à partir de début septembre 2025.
- NetScaler Console sur site : 14.1-51.x

  Remarque : La prise en charge du LAS pour Console sur site est disponible à partir de la version 14.1-51.x. Cependant, les licences basées sur des fichiers sont obsolètes à compter du April 15 2026 pour les versions de Console sur site 14.1-51.x et ultérieures, et 13.1-60.x et ultérieures. Si vous effectuez une mise à niveau vers la version 14.1-51.x ou 13.1-60.x ou ultérieure de Console sur site, vous pouvez continuer à utiliser les licences basées sur des fichiers jusqu'au 15th April 2026. Cependant, vous devez effectuer une mise à niveau vers la version 14.1-51.x ou ultérieure de Console sur site et passer au LAS avant le 15th April 2026, car Console sur site 13.1 ne prend pas en charge le LAS.

Toutes les autres formes de licences NetScaler héritées telles que Pooled vCPU, CICO, perpétuelles ne seront pas prises en charge avec le LAS. Les instances NetScaler utilisant des licences perpétuelles sans maintenance active deviendront sans licence lors de la mise à niveau vers les versions logicielles mentionnées ci-dessus.
Les licences basées sur le LAS peuvent ne pas être disponibles pour les clients là où la loi ou la réglementation l'interdit.
Si vous avez des questions ou des préoccupations, contactez le service client. Citrix peut limiter ou suspendre votre maintenance Citrix en cas de non-conformité à ces exigences, sans engager sa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

responsabilité, en plus de tout autre recours que Citrix pourrait avoir en droit ou en équité. Ces exigences ne s'appliquent pas là où la loi ou la réglementation l'interdit.
Lisez la note suivante avant de continuer.

AVERTISSEMENT

Le serveur de licences ne répond pas. NetScaler continue de fonctionner avec la capacité actuelle pendant 30 jours. Après 30 jours, si la connectivité au serveur de licences n'est pas rétablie, NetScaler perd sa capacité actuelle et cesse de traiter le trafic. Si la connectivité est rétablie dans les 30 jours, NetScaler continue de fonctionner à sa capacité actuelle et de traiter le trafic.

L'instance NetScaler en pool cesse de répondre

Si l'instance NetScaler en pool cesse de répondre et que le serveur de licences est en bon état de fonctionnement, le serveur de licences enregistre toutes les licences de l'instance NetScaler après 10 minutes. Lorsque l'instance redémarre, elle envoie une demande pour extraire toutes les licences du serveur de licences.

Le serveur de licences et l'instance NetScaler en pool cessent de répondre

Si le serveur de licences et l'instance NetScaler en pool redémarrent et rétablissent la connexion, le serveur de licences enregistre toutes ses licences après 10 minutes, et les instances NetScaler en pool extraient automatiquement les licences une fois le redémarrage terminé.

L'instance NetScaler en pool s'arrête correctement

Lors d'un arrêt correct, vous pouvez choisir d'enregistrer les licences ou de conserver les licences qui ont été allouées avant l'arrêt correct. Si vous choisissez d'enregistrer les licences, l'instance NetScaler en pool n'est plus sous licence après son redémarrage. Si vous choisissez de conserver les licences, elles sont enregistrées sur le serveur de licences lorsque l'instance s'arrête. Après le redémarrage de l'instance, elle rétablit la connexion avec le serveur de licences et extrait les licences comme spécifié dans la configuration enregistrée.

Si le système redémarre et que l'extraction échoue en raison d'une capacité indisponible dans le pool, NetScaler vérifie l'inventaire des licences de pool NetScaler Console et extrait toute capacité disponible. Une alarme SNMP est déclenchée pour informer l'utilisateur de cette condition si NetScaler ne fonctionne pas à pleine capacité conformément à la configuration. Si aucune capacité n'est disponible dans le pool de bande passante, l'instance de pool devient sans licence.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Problèmes de connectivité réseau

MESSAGE D'ERREUR (SYSLOG)
Le serveur de licences ne répond pas.

Si le serveur de licences et les instances NetScaler en pool sont en bon état de fonctionnement mais que la connectivité réseau est perdue, les instances continuent de fonctionner à leur capacité actuelle pendant 30 jours. Après 30 jours, si la connectivité au serveur de licences n'est pas rétablie, les instances perdent leur capacité et cessent de traiter le trafic, et le serveur de licences enregistre toutes ses licences. Une fois que le serveur de licences rétablit la connectivité avec les instances NetScaler, les instances extraient à nouveau les licences.

Période de grâce

Lorsqu'une instance NetScaler en pool est en bon état de fonctionnement et que le serveur de licences cesse de répondre, l'instance continue de fonctionner avec la capacité actuelle pendant 30 jours. Si la connectivité au serveur de licences n'est pas rétablie après 30 jours, l'instance perd sa capacité et cesse de traiter le trafic.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gérer les paramètres système

Le tableau suivant décrit la liste des options disponibles sous **Paramètres** > **Administration** :

Configurations réseau

CONFIGURATIONS RÉSEAU	OPTIONS	DESCRIPTION
Adresse IP, deuxième carte réseau, nom d'hôte et serveur proxy	Adresse IP	Affiche les détails de l'adresse IP de configuration réseau de NetScaler Console qui sont utilisés pour déployer NetScaler Console
	Deuxième carte réseau	Permet de configurer une deuxième carte réseau pour isoler l'accès de gestion de NetScaler Console. Pour plus d'informations, consultez Configurer une double carte réseau pour accéder à NetScaler Console
	Nom d'hôte	Permet d'attribuer un nom d'hôte à NetScaler Console. Pour plus d'informations, consultez Attribuer un nom d'hôte à un serveur NetScaler Console
	Serveur proxy	Permet de configurer NetScaler Console en tant que serveur proxy. Pour plus d'informations, consultez NetScaler Console en tant que serveur proxy API
Routes statiques		Permet de configurer des routes statiques pour établir

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONFIGURATIONS RÉSEAU	OPTIONS	DESCRIPTION
		une connexion entre NetScaler Console et les instances NetScaler VPX
Serveurs NTP		Garantit que l'horloge de NetScaler Console a les mêmes paramètres de date et d'heure que les autres serveurs du réseau. Pour plus d'informations, consultez Configurer le serveur NTP
Informations sur les ports de NetScaler Console		Permet de comprendre quel port doit être ouvert pour la communication entre NetScaler Console et les instances NetScaler. Pour plus d'informations, consultez Ports pris en charge

Configurations système

CONFIGURATIONS SYSTÈME	OPTIONS	DESCRIPTION
Système, Fuseau horaire, URL autorisées et Message du jour	Paramètres de base	Permet de modifier les paramètres système tels que l'activation de la connexion `nsrecover`, l'activation du délai d'expiration de session, etc.
	Fuseau horaire	Permet de modifier le fuseau horaire à utiliser dans NetScaler Console. Le fuseau horaire par défaut est UTC
	Liste des URL autorisées	Permet de configurer des URL pour envoyer des requêtes ininterrompues à

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONFIGURATIONS SYSTÈME	OPTIONS	DESCRIPTION
		NetScaler Console. Vous pouvez le configurer avec la valeur « none » si aucune URL ne doit être ajoutée.
	Message du jour	Permet de créer un message de bienvenue dans NetScaler Console. Vous pouvez utiliser cette fonctionnalité pour définir des messages de rappel pour vous-même ou pour l'utilisateur qui se connecte à NetScaler Console. Cliquez sur **Activer le message**, saisissez le message dans la zone de message, puis cliquez sur **Enregistrer**.
Afficher l'empreinte digitale de NetScaler Console		Permet de copier l'ID d'empreinte digitale unique de NetScaler Console pour commencer avec le graphique de service.
Configurer l'identité du client		Permet de protéger les ressources réseau en autorisant uniquement les clients ou utilisateurs authentifiés à accéder à son réseau. Pour plus d'informations, consultez Gouvernance des données.
Paramètres CUXIP		Si vous cochez cette case, les statistiques d'utilisation sont collectées dans le seul but d'améliorer l'interface graphique. Les données reçues sont utilisées uniquement par les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CONFIGURATIONS SYSTÈME	OPTIONS	DESCRIPTION
		ingénieurs Citrix et ne sont partagées avec personne.

Maintenance du système

MAINTENANCE DU SYSTÈME	DESCRIPTION
Mettre à niveau NetScaler Console	Permet de mettre à niveau NetScaler Console via l'interface graphique. Pour plus d'informations, consultez Mise à niveau.
Redémarrer NetScaler Console	Permet de redémarrer NetScaler Console
Arrêter NetScaler Console	Permet d'arrêter NetScaler Console
Reprise après sinistre	Permet d'afficher les informations sur les nœuds de reprise après sinistre. Pour plus d'informations, consultez Configurer la reprise après sinistre

Élagage des données

ÉLAGAGE DES DONNÉES	OPTIONS	DESCRIPTION
Élagage des données système et d'instance	Système	Permet de limiter la quantité de données de rapport stockées dans la base de données du serveur NetScaler Console. Pour plus d'informations, consultez Configurer les paramètres d'élagage du système
	Événements d'instance	Permet de limiter les données de rapport des messages d'événement stockées dans NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÉLAGAGE DES DONNÉES	OPTIONS	DESCRIPTION
	Syslog d'instance	Permet de limiter la quantité de données syslog stockées dans la base de données. Pour plus d'informations, consultez Configurer les paramètres d'élagage du syslog d'instance
	Rapports réseau	Permet de limiter les données de rapports réseau stockées dans NetScaler Console

Sauvegarde

SAUVEGARDE	OPTIONS	DESCRIPTION
Configurer la sauvegarde du système et de l'instance	Système	Permet de configurer les paramètres de sauvegarde initiaux avant d'effectuer une sauvegarde du système. Pour plus d'informations, consultez Paramètres de sauvegarde du système
	Instance	Permet de configurer les paramètres dans NetScaler Console pour sauvegarder une instance NetScaler sélectionnée ou plusieurs instances. Pour plus d'informations, consultez Configurer les paramètres de sauvegarde d'instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Notifications d'événements

NOTIFICATIONS D'ÉVÉNEMENTS	OPTIONS	DESCRIPTION
Configurer la notification et le résumé des événements	Notification d'événement	Vous pouvez envoyer des notifications à des groupes d'utilisateurs sélectionnés pour plusieurs fonctions liées au système. Ces fonctions système sont organisées en catégories d'événements telles que SystemReboot, StatusPoll, SystemState, etc. Vous pouvez configurer NetScaler Console pour vous envoyer des notifications par e-mail, SMS ou Slack. Cela garantit que vous êtes informé de toute activité au niveau du système, telle que le dépassement du stockage de données ou l'échec de la sauvegarde.
	Résumé des événements	Permet d'obtenir un rapport consolidé des événements système et des fonctionnalités importants

Paramètres SSL

PARAMÈTRES SSL	DESCRIPTION
Installer le certificat SSL	Permet d'installer le certificat SSL et le fichier de clé SSL
Afficher le certificat SSL	Permet d'afficher les détails du certificat SSL
Configurer les paramètres SSL	Pour plus d'informations, consultez Configurer les paramètres SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES SSL	DESCRIPTION
Certificats SSL	Permet de téléverser, de télécharger ou de supprimer un certificat SSL ou un fichier de clé SSL
Groupes de chiffrement	Pour plus d'informations, consultez Configurer un groupe de chiffrement

Configurer les fonctionnalités

CONFIGURER LES FONCTIONNALITÉS	DESCRIPTION
Désactiver ou activer les fonctionnalités	Vous pouvez activer ou désactiver des fonctionnalités dans NetScaler Console. Pour plus d'informations, consultez Activer ou désactiver les fonctionnalités de NetScaler Console

Configurer les paramètres de sauvegarde du système

Définissez vos paramètres de sauvegarde système initiaux avant de devoir sauvegarder et restaurer la NetScaler Console.

1. Accédez à **Settings > Administration**. Sous **Backup**, cliquez sur **Configure System and Instance backup**.
2. Sur la page **Backup > System**, spécifiez les éléments suivants :

    - Sauvegardes précédentes à conserver. Vous ne pouvez conserver que jusqu'à 10 sauvegardes.
    - Sélectionnez **Encrypt Backup File** pour chiffrer les fichiers de sauvegarde.
    - Sélectionnez **Enable External Transfer** pour transférer une copie de votre fichier de sauvegarde vers un autre système. Lorsque vous souhaitez restaurer la configuration, vous devez d'abord télécharger le fichier sur le serveur NetScaler Console, puis effectuer l'opération de restauration. Spécifiez le serveur, le nom d'utilisateur et le mot de passe, le port, le protocole de transfert à utiliser et le chemin du répertoire. Pour en savoir plus sur le transfert externe, consultez Transférer un fichier de sauvegarde NetScaler Console vers un système externe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur **OK**.



Configurer les paramètres du serveur proxy

NetScaler Console® vous permet de configurer un serveur proxy pour la connectivité sortante. Vous pouvez également télécharger ses certificats CA pour les déploiements NetScaler Console où le proxy d'inspection SSL intercepte le trafic sortant. NetScaler Console ne fait confiance au certificat du proxy que lorsque son certificat CA est téléchargé. Cette fonctionnalité garantit que toutes les communications externes de NetScaler Console passent par un serveur proxy sécurisé et contrôlé.

Cette fonctionnalité offre les avantages suivants :

- Garantit que la communication est sécurisée lorsque les proxys effectuent une interception SSL.
- Prévient les problèmes de connectivité pour les téléchargements de télémétrie et la communication Cloud Connect.

Pour configurer un serveur proxy, accédez à **Paramètres > Administration** et cliquez sur **Serveur proxy**.



Points à noter

- Assurez-vous que le serveur proxy est accessible depuis NetScaler Console via l'adresse IP/le port spécifié.
- Si l'interception SSL est activée, importez dans NetScaler Console le certificat CA du proxy pour éviter les échecs de connectivité.
- Les modifications de la configuration du proxy peuvent avoir un impact sur le téléchargement automatique de télémétrie ou Cloud Connect jusqu'à ce que les nouvelles informations soient ajoutées.

Configuration du serveur proxy

Vous pouvez utiliser l'onglet **Configuration du serveur proxy** pour ajouter les détails et les informations d'identification du proxy.

Prérequis

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ajoutez `adm.cloud.com` à la liste d'autorisation.

Pour ajouter un serveur proxy afin de router tout le trafic sortant, effectuez les étapes suivantes :

1. Accédez à **Paramètres > Administration** et cliquez sur **Serveur proxy**.
2. Dans l'onglet **Configuration du serveur proxy**, sélectionnez **Activer le serveur proxy**.
3. Spécifiez l'**adresse IP/nom d'hôte** du serveur proxy et son **port** d'écoute.

   REMARQUE :

   - À partir de la version 14.1 build 56.x, NetScaler Console prend en charge l'utilisation de noms d'hôte DNS (FQDN) en plus des adresses IP pour la configuration du proxy.
   - L'utilisation de noms d'hôte est bénéfique dans les environnements qui :
     - Utilisent la redondance basée sur DNS (par exemple, GSLB) pour acheminer le trafic entre plusieurs serveurs proxy.
     - N'ont pas d'équilibreur de charge, mais s'appuient sur DNS pour gérer la haute disponibilité et le basculement.
     - Nécessitent des configurations de proxy évolutives et résilientes entre les centres de données.

     La prise en charge de l'utilisation des noms d'hôte DNS permet à NetScaler Console de résoudre dynamiquement le point de terminaison proxy le plus approprié, améliorant ainsi la fiabilité et simplifiant la gestion.

4. Fournissez un **Nom d'utilisateur** et le **Mot de passe** correspondant si le proxy nécessite des informations d'identification.

   REMARQUE :

   NetScaler Console prend actuellement en charge l'authentification de base pour le proxy.

5. Cliquez sur **Enregistrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gérer le certificat CA

Si le serveur proxy effectue une inspection SSL, utilisez l'onglet **Gérer les certificats CA** pour télécharger le certificat CA du serveur proxy. Vous pouvez ajouter ou supprimer le certificat selon vos besoins.

Pour télécharger le certificat CA du serveur proxy, effectuez les étapes suivantes :

1. Accédez à **Paramètres > Administration** et cliquez sur **Serveur proxy**.
2. Cliquez sur **Télécharger le certificat**.

Pour supprimer le certificat CA du serveur proxy, effectuez les étapes suivantes :

1. Accédez à **Paramètres > Administration** et cliquez sur **Serveur proxy**.
2. Sélectionnez le certificat à supprimer.
3. Cliquez sur **Supprimer le certificat**.



Prise en charge de la configuration proxy

NetScaler Console prend en charge les modèles de déploiement proxy suivants pour s'adapter aux différentes architectures de réseau d'entreprise. En fonction de votre environnement et de vos exigences de sécurité, vous pouvez choisir l'une des configurations proxy prises en charge suivantes :

- Aucun proxy
- Proxy explicite en avant
- Proxy SSL interceptant explicite
- Proxy SSL interceptant transparent

IMPORTANT

- Pour les déploiements de proxy SSL interceptant explicite et de proxy SSL interceptant transparent, le téléchargement du certificat CA du proxy est obligatoire. Si le certificat CA du proxy n'est pas téléchargé, le trafic sortant de NetScaler Console échoue.
- Ne configurez pas de proxy sur NetScaler Console sur site lors de l'utilisation d'un proxy SSL interceptant transparent.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pas de proxy (Accès Internet direct)

Dans ce modèle de déploiement, NetScaler Console sur site se connecte directement à Citrix Cloud sans utiliser de proxy.

- La communication utilise uniquement le trafic HTTPS sortant.
- Aucune configuration de proxy n'est requise sur NetScaler Console sur site.

Proxy explicite de transfert (Non interceptant)

Dans une configuration de proxy explicite de transfert, le trafic sortant de NetScaler Console sur site est explicitement acheminé via un serveur proxy.

- Le trafic de NetScaler Console est envoyé via un proxy de transfert configuré.
- Le proxy transfère le trafic HTTPS sans déchiffrer SSL/TLS.
- Obligatoire : Les détails du proxy doivent être configurés sur NetScaler Console sur site.
- Facultatif : L'authentification est facultative. Les utilisateurs peuvent fournir un nom d'utilisateur et un mot de passe pour s'authentifier lors de la configuration du proxy. Seule l'authentification de base est prise en charge.

Proxy SSL-interceptant explicite

Dans ce modèle de déploiement, le proxy inspecte le trafic chiffré en terminant et en rechiffrant les connexions SSL/TLS.

- Le proxy effectue le déchiffrement et le rechiffrement SSL.
- Obligatoire : La configuration du proxy est requise sur NetScaler Console.
- Obligatoire : Le certificat d'autorité de certification du proxy doit être téléchargé sur NetScaler Console. Pour plus d'informations, consultez Gérer le certificat d'autorité de certification.
- Facultatif : L'authentification est facultative. Les utilisateurs peuvent fournir un nom d'utilisateur et un mot de passe pour s'authentifier lors de la configuration du proxy. Seule l'authentification de base est prise en charge.

Proxy SSL-interceptant transparent

Dans une configuration de proxy transparent, le trafic est intercepté au niveau du réseau sans configuration de proxy explicite sur le client.

- L'inspection SSL se produit de manière transparente sans paramètres de proxy sur NetScaler Console.
- Les périphériques réseau redirigent automatiquement le trafic vers le proxy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Obligatoire : Le certificat d'autorité de certification du proxy doit être téléchargé sur NetScaler Console pour la validation SSL. Pour plus d'informations, consultez Gérer le certificat d'autorité de certification.
- Aucune configuration de proxy n'est requise sur NetScaler Console.

Configurer un serveur NTP

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans NetScaler Console pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge de NetScaler Console a les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

Pour configurer un serveur NTP sur NetScaler Console :

1. Accédez à **Paramètres > Serveurs NTP**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer un serveur NTP**, saisissez les détails suivants :
    - **Nom du serveur/Adresse IP** – Saisissez le nom de domaine ou l'adresse IP du serveur NTP. Le nom ou l'adresse IP ne peut pas être modifié après l'ajout du serveur NTP.
    - **Intervalle d'interrogation minimal** – Spécifiez la valeur minimale de l'intervalle entre les messages NTP transmis, en secondes sous forme de puissance de 2. Par exemple, si vous souhaitez que l'intervalle d'interrogation minimal soit de 64 secondes, ce qui peut être exprimé comme 2\^6, saisissez 6.
    - **Intervalle d'interrogation maximal** – Spécifiez la valeur maximale de l'intervalle entre les messages NTP transmis, en secondes sous forme de puissance de 2. Par exemple, si vous souhaitez que l'intervalle d'interrogation maximal soit de 256 secondes, ce qui peut être exprimé comme 2\^8, saisissez 8.
    - **Identifiant de clé** - Saisissez l'identifiant de clé qui peut être utilisé pour l'authentification par clé symétrique avec le serveur NTP. N'ajoutez pas d'identifiant de clé si vous choisissez de sélectionner Autokey.
    - **Autokey** - Sélectionnez **Autokey** si vous souhaitez utiliser l'authentification par clé publique avec le serveur NTP. Ne sélectionnez pas si vous souhaitez ajouter un identifiant de clé.
    - **Préféré** – Sélectionnez cette option si vous souhaitez spécifier ce serveur NTP comme serveur préféré pour la synchronisation de l'horloge. Cela s'applique uniquement si plusieurs serveurs sont configurés.
3. Cliquez sur **Créer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Pour activer la synchronisation NTP sur NetScaler Console :

1. Accédez à **Paramètres > Serveurs NTP**.
2. Cliquez sur **Synchronisation NTP** et cochez la case **Activer la synchronisation NTP**.
3. Cliquez sur **OK**.



Remarque

Vous pouvez trouver les messages des journaux NTP dans le répertoire /var/log, dans le fichier `/var/log/ntpd.log`.

Mettre à niveau NetScaler Console

IMPORTANT :

La licence basée sur fichier sera en fin de vie (EOL) à partir du April 15, 2026. Toutes les instances NetScaler (ADC, SVM) doivent être mises à niveau vers des versions conformes à LAS et passer à l'utilisation de licences basées sur LAS avant cette date. Les versions minimales requises de NetScaler compatibles avec LAS sont :

- NetScaler ADC : 14.1–51.80, 13.1-60.29, 13.1-37.247 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM : 14.1–51.83, 13.1-60.30

Après le April 15, 2026, dans les versions 14.1-66.x et ultérieures de NetScaler ADC et SVM, une vérification liée à la mise à niveau sera déclenchée avant la mise à niveau de NetScaler. Cette vérification valide si votre NetScaler (ADC, SVM) utilise toujours une licence basée sur fichier, et si c'est le cas, la mise à niveau serait bloquée avec l'erreur « NetScaler Upgrade Blocked: File-based licensing in use ». Cette précaution empêche vos instances NetScaler de procéder à la mise à niveau et de devenir sans licence après le April 15, 2026. Contactez le support Citrix ou votre représentant ATS pour comprendre comment débloquer la mise à niveau et les risques qui y sont associés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vérifications avant la mise à niveau

Avant de déclencher une mise à niveau depuis NetScaler Console, le système effectue automatiquement une vérification préalable à la mise à niveau pour valider la préparation du système et l'intégrité de l'image de mise à niveau. Cette vérification garantit que la mise à niveau se déroule sans problème et réduit la probabilité de rencontrer des échecs pendant le processus de mise à niveau.

REMARQUE :

La fonction de vérification préalable à la mise à niveau est disponible à partir de la version 14.1 build 56.x de NetScaler Console. La vérification s'exécute automatiquement avant chaque mise à niveau initiée via NetScaler Console sur site.

Si la vérification détecte des problèmes, NetScaler Console affiche des informations détaillées sur les écarts et vous invite à les résoudre avant de poursuivre la mise à niveau.

La vérification préalable à la mise à niveau comprend les validations suivantes :

- Vérification de la disponibilité de la mémoire – Vérifie que NetScaler Console dispose de suffisamment de RAM disponible pour effectuer la mise à niveau en toute sécurité.
- Vérification de l'espace disque – Garantit que l'espace disque libre requis est disponible pour l'extraction et l'installation de l'image de mise à niveau.
- Vérification des exigences des fichiers image – Confirme que tous les fichiers image obligatoires requis pour la mise à niveau sont disponibles.
- Vérification de l'intégrité du fichier image – Valide la somme de contrôle de l'image de mise à niveau pour s'assurer que le fichier est complet et non corrompu.
- Vérification de la transition LAS - Vérifie si NetScaler Console utilise toujours des licences basées sur des fichiers pour les types de licences groupées ou flexibles après le April 15, 2026.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

La vérification de la transition LAS prend effet le April 15, 2026 et s'applique aux types de licences groupées et flexibles. À partir de cette date, si vous tentez de mettre à niveau vers NetScaler Console 14.1-66.x ou une version ultérieure avec des licences basées sur des fichiers toujours utilisées, la mise à niveau ne sera pas autorisée. Cette vérification est effectuée pour éviter que votre NetScaler Console sur site ne procède à la mise à niveau après le April 15, 2026, et que les instances NetScaler ne deviennent sans licence après la mise à niveau. Si vous rencontrez cette restriction, vous devez contacter le support Citrix ou votre représentant ATS pour obtenir des conseils.

L'erreur suivante s'affiche lorsque la vérification préalable à la mise à niveau LAS échoue :



En plus des validations de ressources et de fichiers, NetScaler Console vérifie l'état et la connectivité du système pour garantir une mise à niveau sécurisée. La vérification comprend les contrôles suivants :

- Vérification de l'intégrité de la base de données – Détecte les fichiers de base de données manquants ou corrompus pour éviter les échecs de mise à niveau.
- État du canal de diffusion en continu de la base de données – Confirme que le canal de diffusion en continu est actif et opérationnel.
- Connectivité du nœud secondaire – Assure une communication appropriée avec le nœud secondaire pour la redondance.
- Vérification SSH sans mot de passe – Confirme que la connexion SSH sans mot de passe au nœud secondaire fonctionne.

La fonction de vérification préalable à la mise à niveau offre les avantages suivants :

- L'exécution de ces validations avant la mise à niveau permet d'éviter les échecs causés par des ressources insuffisantes ou des fichiers image corrompus.
- En identifiant les problèmes potentiels à l'avance, la vérification préalable à la mise à niveau améliore la fiabilité de la mise à niveau et minimise les temps d'arrêt dus aux efforts de récupération ou de réinstallation.

Pour mettre à niveau NetScaler Console :

1. Accédez à **Paramètres > Administration**. Sous **Maintenance du système**, cliquez sur **Mettre à niveau NetScaler Console**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Sur la page Mettre à niveau NetScaler Console, téléchargez un nouveau fichier image en sélectionnant **Local** (votre ordinateur local) ou **Appliance**.

   REMARQUE

   Lorsque vous sélectionnez **Appliance**, assurez-vous que l'image de mise à niveau est disponible à l'emplacement `/var/mps/mps_images` dans NetScaler Console.

   Par défaut, l'image logicielle est nettoyée après une mise à niveau réussie.

3. Cliquez sur **OK**.

Déblocage de la mise à niveau de NetScaler Console lorsque la vérification préalable à la mise à niveau LAS échoue

Utilisez cette option uniquement si vous devez procéder immédiatement à la mise à niveau de NetScaler Console et que vous comprenez et acceptez l'impact sur les licences décrit ci-dessous. Si votre objectif est de rester sous licence après la mise à niveau, contactez le support Citrix ou votre représentant ATS.

Conditions préalables : Vous devez disposer d'un accès shell à NetScaler Console ou à la VM et de privilèges suffisants pour créer des fichiers sous `/var/tmp`.

Pour débloquer la mise à niveau :

1. Connectez-vous au shell de NetScaler Console.
2. Créez le fichier d'indicateur de contournement.

   ```
   touch /var/tmp/skip_las_checks
   ```

3. Relancez la mise à niveau. NetScaler Console détecte l'indicateur `skip_las_checks` et ignore la validation LAS, ce qui permet au processus de mise à niveau de se poursuivre.

IMPORTANT :

Si vous ignorez la vérification préalable à la mise à niveau LAS et continuez alors que la licence groupée ou flexible basée sur des fichiers est toujours utilisée, toutes les instances NetScaler gérées devraient devenir sans licence après la mise à niveau de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après la mise à niveau sur site de NetScaler Console, effectuez la transition LAS pour la licence groupée ou flexible et confirmez que chaque instance NetScaler est correctement licenciée.

Si vous avez besoin d'une approche alternative ou d'une assistance pour la séquence de transition, contactez le support Citrix ou votre représentant ATS.

Comment réinitialiser le mot de passe de NetScaler Console

La procédure de réinitialisation du mot de passe de NetScaler Console peut différer selon les hyperviseurs sur lesquels il est hébergé. Si vous avez modifié votre mot de passe par défaut et souhaitez revenir au mot de passe par défaut, vous pouvez réinitialiser le mot de passe en redémarrant le nœud NetScaler Console.

Citrix Hypervisor™ à l'aide de XenCenter :

1. Connectez-vous à Citrix Hypervisor à l'aide de XenCenter.
2. Sélectionnez le nœud NetScaler Console, cliquez avec le bouton droit de la souris et sélectionnez **Redémarrer**.
3. Dans l'onglet **Console**, appuyez sur **CTL + C** pour interrompre la séquence de démarrage.

   
4. Exécutez la commande **boot -s** à l'invite OK.

   

   NetScaler Console redémarre et affiche le message suivant :

   
5. Appuyez sur **Entrée** pour obtenir l'invite /u@.

   
6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount /dev/ada0s1a /flash
   ```

   
7. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.
8. Exécutez la commande **Reboot** pour redémarrer NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Accédez à l'interface graphique de NetScaler Console et attendez que le redémarrage soit terminé.

   Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour vous connecter depuis l'interface graphique et *nsrecover/nsroot* pour vous connecter depuis l'hyperviseur.

   Remarque

   Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Ensuite, exécutez les commandes suivantes et redémarrez NetScaler Console :

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

Esx utilisant vSphere :

1. Connectez-vous à ESX à l'aide de vSphere.
2. Sélectionnez le nœud NetScaler Console, cliquez avec le bouton droit, puis sélectionnez **Redémarrer**.
3. Sous l'onglet **Console**, appuyez sur **CTL + C** pour interrompre la séquence de démarrage.
4. Exécutez la commande **boot -s** dans l'invite OK.

   La NetScaler Console redémarre.
5. Appuyez sur **Entrée** pour obtenir l'invite /u@.
6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount dev/da0s1a /flash
   ```
7. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.
8. Exécutez la commande **Redémarrer** pour redémarrer NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Accédez à l'interface graphique de NetScaler Console et attendez que le redémarrage soit terminé.

   

   Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour vous connecter depuis l'interface graphique et *nsrecover/nsroot* pour vous connecter depuis le serveur ESX.

   Remarque

   Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Ensuite, exécutez les commandes suivantes et redémarrez NetScaler Console :

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

Hyper-v à l'aide du gestionnaire Hyper-v :

1. Connectez-vous à Hyper-V à l'aide du gestionnaire Hyper-V.
2. Sélectionnez le nœud NetScaler Console, cliquez avec le bouton droit de la souris, puis sélectionnez **Redémarrer**.
3. Dans l'onglet **Console**, appuyez sur **CTL + C** pour interrompre la séquence de démarrage.

   

4. Exécutez la commande **boot -s** à l'invite OK.

   NetScaler Console redémarre.

5. Appuyez sur **Entrée** pour obtenir l'invite /u@.
6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount dev/ad0s1a /flash
   ```

7. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

8. Exécutez la commande **Reboot** pour redémarrer NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Accédez à l'interface graphique de NetScaler Console et attendez que le redémarrage soit terminé.

   Vous pouvez maintenant utiliser les identifiants *nsroot/nsroot* pour vous connecter depuis l'interface graphique et *nsrecover/nsroot* pour vous connecter depuis le gestionnaire Hyper-V.

   Remarque

   Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Ensuite, exécutez les commandes suivantes et redémarrez NetScaler Console :

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

Serveur KVM Linux (connexion SSH au serveur KVM à l'aide de n'importe quel client SSH) :

1. Connectez-vous à NetScaler Console à l'aide d'un client SSH au serveur KVM.
2. Redémarrez NetScaler Console.
3. Appuyez sur **CTL + C** pour interrompre la séquence de démarrage peu après l'affichage du message **Loading /boot/defaults/loader.conf**.
4. À l'invite OK, exécutez la commande suivante :

   ```
   set console='comconsole,vidconsole'
   ```

5. Exécutez la commande **boot -s** pour redémarrer NetScaler Console.
6. Une fois que le message **Enter full path of shell or RETURN for /bin/sh:** s'affiche, appuyez sur **Entrée** pour obtenir l'invite /u@.
7. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount dev/vtbd0s1a /flash
   ```

8. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.
9. Exécutez la commande **Reboot** pour redémarrer NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Accédez à l'interface graphique de NetScaler Console et attendez que le redémarrage soit terminé.

    Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour vous connecter depuis l'interface graphique et *nsrecover/nsroot* pour vous connecter depuis la console SSH.

    Remarque

    Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Ensuite, exécutez les commandes suivantes et redémarrez NetScaler Console :

    - `rm /flash/mpsconfig/master.passwd`
    - `rm –rf /etc/passwd`

Configurer une carte réseau secondaire pour accéder à NetScaler Console

Vous pouvez configurer une deuxième carte réseau pour isoler l'accès de gestion à NetScaler Console. Grâce à cette fonctionnalité de deuxième carte réseau, selon vos besoins, vous pouvez choisir comment isoler le trafic reçu et envoyé via NetScaler Console.

Considérez un scénario dans lequel vous souhaitez isoler le trafic pour :

- Avoir toutes les communications entre NetScaler Console et ses instances NetScaler gérées dans un seul réseau.
- Avoir l'accès de gestion à NetScaler Console dans un autre réseau.

Dans ce scénario, en tant qu'administrateur, vous pouvez :

- Configurer une adresse IP pour le trafic entre NetScaler Console et ses instances NetScaler gérées.
- Configurer une autre adresse IP pour gérer le logiciel NetScaler Console afin d'effectuer toutes les tâches administratives dans le logiciel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Si NetScaler Console est configuré en tant que paire HA, l'adresse IP de gestion configurée sur la deuxième carte réseau est associée au nœud principal.

Prérequis

- Assurez-vous d'avoir déployé et configuré **NetScaler Console 13.0 Build 47.x ou version ultérieure** sur l'hyperviseur (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM ou VMware ESXi).
- Assurez-vous d'avoir ajouté la deuxième carte réseau sur l'hyperviseur (Citrix Hypervisor™, Microsoft Hyper-V, Linux KVM ou VMware ESXi).

Pour attribuer une adresse IP à une carte réseau sur un Citrix Hypervisor et créer une interface secondaire, consultez Attribuer une adresse IP à une carte réseau.

Configurer une deuxième carte réseau dans NetScaler Console

1. Connectez-vous à l'interface graphique de NetScaler Console.
2. Accédez à **Paramètres > Administration**.
3. Sous **Configuration réseau**, cliquez sur **Adresse IP, deuxième carte réseau, nom d'hôte et serveur proxy**.

   

   La page **Configuration réseau** s'affiche.
4. Cliquez sur l'onglet Deuxième carte réseau et configurez les paramètres suivants :

   a. **Adresse IP de gestion de la livraison d'applications** – Entrez une adresse IP valide pour accéder à NetScaler Console. Vous pouvez utiliser cette adresse IP pour accéder à NetScaler Console, en plus de l'adresse IP de gestion existante.

   b. **Masque de sous-réseau** – Entrez l'adresse du masque de sous-réseau pour spécifier l'hôte réseau. L'adresse par défaut est 255.255.255.0.

   c. **Adresse réseau** – Entrez une adresse IP pour ajouter une entrée de routage pour NetScaler Console. Cliquez sur **+** pour ajouter d'autres adresses IP. Ce champ est facultatif.

   d. Cliquez sur **Enregistrer**.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer une carte réseau secondaire pour accéder à l'agent NetScaler®

Vous pouvez configurer deux cartes réseau sur un agent. Grâce à l'architecture Dual NIC, l'agent pourra :

- Établir la communication entre l'agent et les instances NetScaler - Vous pouvez utiliser la première carte réseau pour isoler le trafic reçu et envoyé via la console NetScaler et également pour communiquer entre la console NetScaler et ses instances NetScaler gérées dans un autre réseau.
- Établir la communication entre l'agent et la console NetScaler - Vous pouvez utiliser la deuxième carte réseau pour gérer la console NetScaler qui se trouve sur un réseau et effectuer des tâches administratives.

REMARQUE

Vous ne pouvez pas interchanger les fonctionnalités et la configuration des deux cartes réseau.



Dans ce scénario, en tant qu'administrateur, vous pouvez :

- Configurer l'adresse IP pour le trafic entre la console NetScaler et ses instances NetScaler gérées.
- Configurer l'adresse IP pour la gestion du logiciel NetScaler Console afin d'effectuer toutes les tâches administratives dans le logiciel.

REMARQUE

Il n'est pas obligatoire de configurer des cartes réseau doubles pour un agent. C'est facultatif et n'est requis que lorsque le trafic entre l'agent, la console NetScaler et les instances NetScaler doit être séparé.

Modifier les adresses réseau des cartes réseau IPV4 à l'aide de la CLI

1. Ouvrez une connexion SSH à la console de l'agent NetScaler à l'aide d'un client SSH, tel que PuTTY.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Connectez-vous en utilisant les informations d'identification **nsrecover/nsroot** et passez à l'invite de commande du shell.
3. Exécutez la commande **ifconfig**. Vous pouvez voir les détails des deux cartes réseau que vous avez configurées -

   - Carte réseau 1 – Pour la communication entre l'agent et NetScaler
   - Carte réseau 2 – Pour la communication entre l'agent et la console NetScaler

   
4. Exécutez la commande **networkconfig**. Un menu apparaît qui vous permet de définir ou de modifier les adresses réseau IPV4.

   

   REMARQUE

   L'adresse réseau de la deuxième carte réseau peut prendre plusieurs valeurs IP.
5. Sélectionnez un élément de menu à modifier. Enregistrez et quittez les paramètres.

Configurer l'intervalle de purge du syslog

Syslog est un protocole standard pour la journalisation. Il comporte deux composants : le module d'audit Syslog, qui s'exécute sur l'instance Citrix NetScaler, et le serveur Syslog, qui peut s'exécuter soit sur le système d'exploitation (OS) FreeBSD sous-jacent de l'instance NetScaler, soit sur un système distant. SYSLOG utilise le protocole UDP (User Datagram Protocol) pour le transfert de données.

Syslog permet d'isoler le système qui génère les informations et le système qui les stocke. Vous pouvez consolider les informations de journalisation et en tirer des enseignements à partir des données collectées. Vous pouvez également configurer syslog pour enregistrer différents types d'événements.

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données syslog suivantes seront supprimées de NetScaler Console :

- Données Syslog génériques
- Données AppFirewall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Données NetScaler Gateway

Vous pouvez également configurer l'intervalle de purge de NetScaler Gateway par type de syslog. Cet intervalle de purge a priorité sur l'intervalle de rétention configuré pour les données NetScaler Gateway.

Pour configurer les paramètres d'intervalle de purge syslog pour NetScaler Console :

1. Accédez à **Paramètres > Stockage des données > Stratégie de rétention des données**. La page **Purge des données** s'affiche. Cliquez sur **Syslog d'instance**.
2. Dans la page **Configurer les paramètres de purge du syslog d'instance**, spécifiez **Conserver les données génériques Syslog (jours)**. Saisissez le nombre de jours pendant lesquels NetScaler Console conserve les messages syslog génériques.



Configurer les paramètres de purge du système et des événements

Pour limiter la quantité de données de rapport stockées dans la base de données de votre logiciel NetScaler Console, vous pouvez les purger. Vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont purgées toutes les 24 heures (à 00h00).

REMARQUE

La valeur que vous spécifiez ne peut pas dépasser 30 jours ni être inférieure à 15 jours.

Pour configurer les paramètres de purge du système pour les rapports de performances :

1. Accédez à **Paramètres** > **Administration**. Sous **Purge des données**, cliquez sur **Purge des données système et d'instance**.
2. Dans la page **Configurer les paramètres de purge du système**, spécifiez les éléments suivants :
   - Nombre de jours pour conserver les données
   - Pourcentage d'espace disque (seuil de purge)
3. Cliquez sur **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez activer la purge automatique en cochant la case **Activer la purge automatique des données**. Une alarme est déclenchée et un e-mail est envoyé lorsque l'utilisation du disque dépasse la **valeur de seuil de purge des données** configurée.

REMARQUE

La purge commence lorsqu'un des critères est rempli – valeur de seuil de purge des données ou données à conserver (jours). Celui qui est atteint en premier a priorité sur l'autre.

Pour configurer et activer les paramètres d'alarme :

1. Accédez à **Paramètres** > **SNMP**. Cliquez sur **Alarmes** dans le coin supérieur droit.
2. Sélectionnez l'alarme que vous souhaitez configurer (par exemple, diskUtilizationHigh) et cliquez sur **Modifier**.
3. Dans la page **Configurer l'alarme**, spécifiez les éléments suivants :

- **Gravité**—Sélectionnez le niveau de gravité.
- **Seuil d'alarme**—Saisissez la valeur pour laquelle la gravité de l'événement est calculée.
- **Délai**—Saisissez le délai (en minutes) après lequel vous souhaitez déclencher l'alarme.

configurer la purge automatique des alarmes(/en-us/netscaler-application-delivery-management-software/media/configure-alarm-automatic-purging.png)

Configurer les paramètres de purge des événements à l'aide de NetScaler Console

Pour limiter la quantité de données de messages d'événements stockées dans votre base de données NetScaler Console, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapports réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont purgées toutes les 24 heures (à 00h00).

1. Accédez à **Paramètres > Administration > Purge des données** et cliquez sur **Purge des données système et d'instance**. Cliquez sur **Événements d'instance**.
2. Saisissez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler Console et cliquez sur **Enregistrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Activer l'accès shell pour les utilisateurs non par défaut

Vous pouvez activer l'accès shell pour les utilisateurs non par défaut dans NetScaler Console. Vous pouvez utiliser cette fonctionnalité pour activer et configurer le mode de communication avec les instances.

REMARQUE

Par défaut, l'accès shell est désactivé pour les utilisateurs non par défaut.

Pour activer l'accès shell pour les utilisateurs non par défaut dans NetScaler Console :

1. Dans NetScaler Console, accédez à **Paramètres > Administration**.
2. Dans **Configurations système**, cliquez sur **Système, Fuseau horaire, URL autorisées et Paramètres de l'agent**.
3. Sur la page **Configurations système**, configurez les paramètres suivants :

   - **Communication avec les instances** - Sélectionnez le protocole de communication.
   - **Accès sécurisé** - Activez l'accès sécurisé pour NetScaler Console.
   - **Activer le délai d'expiration de session** - Spécifiez la période pendant laquelle conserver une session inactive.
   - **Autoriser l'authentification de base** - Autorisez le service de gestion à accepter les informations d'identification fournies à l'aide du protocole d'authentification de base.
   - **Activer la connexion nsrecover** - Activez la connexion `nsrecover` sur le service de gestion.
   - **Activer le téléchargement de certificats** - Vous permet de télécharger des certificats à partir du NetScaler ajouté.
   - **Activer l'accès shell pour les utilisateurs non-nsroot** - Activez l'accès shell pour les utilisateurs non par défaut dans NetScaler Console.
   - **Demander les informations d'identification de l'utilisateur pour la connexion à l'instance** - Permet aux utilisateurs de saisir leurs informations d'identification lors de la connexion aux instances depuis NetScaler Console.

     - **Demander les informations d'identification pour les opérations Stylebooks** - Permet aux utilisateurs de saisir leurs informations d'identification lors de l'utilisation des opérations StyleBook et des packs de configuration sur les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Si **Demander les informations d'identification pour la connexion à l'instance** est sélectionné et que **Demander les informations d'identification pour les opérations Stylebook** est désactivé, les utilisateurs ne sont pas invités à fournir des informations d'identification pour les opérations StyleBook et les packs de configuration sur les instances NetScaler.

4. Cliquez sur **OK**.

Récupérer les serveurs NetScaler Console inaccessibles

NetScaler Console fournit désormais un outil de maintenance de base de données pour nettoyer la base de données système. Vous pouvez maintenant lancer l'outil utilitaire NetScaler Console pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible. Le script de récupération NetScaler Console est un outil qui aide à récupérer de l'espace dans le système de fichiers en supprimant les tables et fichiers de base de données anciens ou inutilisés. L'outil vous aide à naviguer à travers les tables et fichiers de la base de données par étapes successives et affiche l'espace actuellement occupé sur le système de fichiers par les éléments respectifs. Une fois que vous avez sélectionné les tables et fichiers de base de données à supprimer, l'outil les supprime du système de fichiers après confirmation.

Comment utiliser le script de récupération de base de données NetScaler Console pour un déploiement autonome de NetScaler Console

Utilisez la procédure suivante dans un déploiement NetScaler Console à serveur unique pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible, puis effectuer les opérations de récupération.

1. À l'aide d'un client SSH ou de la console de votre hyperviseur, connectez-vous à NetScaler Console et tapez la commande suivante :

   

2. Lorsque l'écran affiche un message d'avertissement pour l'arrêt de quelques processus NetScaler Console, tapez « y » et appuyez sur la touche **Entrée**.

   L'écran suivant apparaît pendant que le système détermine quels composants de la base de données vous pouvez supprimer sans affecter les fichiers principaux du système.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. L'écran affiche la liste des fichiers dans la base de données. Tapez « y » et appuyez sur la touche Entrée pour lancer le processus de nettoyage.

4. Vous pouvez sélectionner le composant de base de données spécifique à nettoyer et taper le numéro correspondant. Appuyez sur la touche **Entrée**.

   Par exemple, pour effectuer le nettoyage du catalogue système, sélectionnez l'option 8 dans le menu de sélection **Composant de base de données** et tapez « y » et appuyez sur la touche **Entrée** pour continuer le nettoyage du catalogue système.

   REMARQUE

   NetScaler Console inclut des tables utilisateur appelées catalogue système. Le catalogue système est un emplacement dans la base de données NetScaler Console où un système de gestion de base de données relationnelle stocke les métadonnées de schéma, telles que les informations sur les tables et les colonnes et les enregistrements internes. Les tables du catalogue système sont comme des tables normales qui peuvent accumuler des lignes gonflées et obsolètes au fil du temps et nécessitent donc un nettoyage périodique pour des performances optimales. Il est recommandé d'entretenir régulièrement ces tables. Cette activité libère non seulement de l'espace disque mais améliore également les performances globales de la base de données et donc de NetScaler Console.

   L'utilitaire de nettoyage vous offre la possibilité de nettoyer les composants de base de données et les composants de fichiers. Vous pouvez sélectionner n'importe quel composant de fichier en tapant un nombre entre "1" et "9", ou taper "11" et appuyer sur la touche Entrée pour nettoyer le composant de base de données.

   REMARQUE

   Le nombre "11" indique que vous n'avez sélectionné aucun composant de fichier à nettoyer et que vous allez procéder au nettoyage du composant de base de données précédemment sélectionné. Dans cet exemple, il s'agit du "catalogue système".

5. Tapez "y" et appuyez à nouveau sur la touche **Entrée** dans l'écran de confirmation finale.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Le catalogue système est nettoyé, ce qui peut prendre du temps en fonction de la taille de la table dans le catalogue système. Une fois le processus terminé, un écran récapitulatif s'affiche.

6. Tapez "y" et appuyez sur la touche **Entrée** pour redémarrer NetScaler Console.

   Assurez-vous de redémarrer NetScaler Console après le nettoyage du système. Attendez environ 30 minutes pour que les opérations internes de la base de données se terminent après le redémarrage de NetScaler Console. Vous devriez alors pouvoir vous connecter à la base de données NetScaler Console. Si ce n'est pas le cas, exécutez à nouveau le script de récupération pour libérer plus d'espace. Lorsque NetScaler Console est opérationnel, il devrait fonctionner comme prévu.

   REMARQUE

   La taille actuelle de la table du catalogue système n'est jamais égale à zéro après le nettoyage. Cela est dû au fait que seules les lignes vides sont supprimées de la table et que la table peut contenir des entrées valides même après leur nettoyage.

Comment utiliser le script de récupération de la base de données NetScaler Console pour un déploiement NetScaler Console à haute disponibilité

Le système de base de données des serveurs NetScaler Console dans un déploiement à haute disponibilité est en mode de synchronisation continue. Lors de l'utilisation du nouvel outil de récupération de base de données, vous n'avez pas besoin de reproduire la procédure sur les deux serveurs NetScaler Console.

1. À l'aide d'un client SSH ou de la console de l'hyperviseur, connectez-vous au nœud principal.
2. Exécutez la commande suivante :

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. Suivez la procédure à partir de l'étape 2 disponible pour NetScaler Console Standalone Deployment Recovery Script

Attribuer un nom d'hôte à un serveur NetScaler Console

Pour identifier un serveur NetScaler Console, vous pouvez lui attribuer un nom d'hôte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour attribuer un nom d'hôte à un serveur NetScaler Console :

1. Dans NetScaler Console, accédez à **Paramètres > Administration**.
2. Sous **Configurations réseau**, cliquez sur **Adresse IP, deuxième carte réseau, nom d'hôte et serveur proxy**.
3. Sélectionnez **Nom d'hôte**, entrez un nom d'hôte et un nom d'hôte d'hyperviseur, puis cliquez sur **Enregistrer**.

REMARQUE :

Vous pouvez également utiliser la commande `networkconfig` dans votre hyperviseur et modifier le nom d'hôte.

Sauvegarder et restaurer votre serveur NetScaler Console

Vous pouvez effectuer des sauvegardes périodiques de votre serveur NetScaler Console. Vous pouvez sauvegarder et restaurer les fichiers de configuration, les détails d'instance, les données système, etc.

IMPORTANT

Citrix vous recommande de restaurer le serveur NetScaler Console à l'aide d'une sauvegarde de la même version. Par exemple, si la version de NetScaler Console est 13.0, utilisez la sauvegarde NetScaler Console 13.0 pour restaurer le serveur.

L'accès utilisateur pour sauvegarder et restaurer le serveur NetScaler Console est limité. La page **Paramètres > Fichiers de sauvegarde** n'apparaît qu'aux utilisateurs ayant accès à toutes les fonctionnalités de NetScaler Console. Un utilisateur ne peut accéder à cette page que si sa politique d'accès dispose de toutes les autorisations. Généralement, les super-utilisateurs ont accès à toutes les fonctionnalités de NetScaler Console.

Pour plus d'informations, consultez Configurer les politiques d'accès.

Avant de procéder à la mise à niveau, sauvegardez les fichiers de configuration du serveur NetScaler Console par mesure de précaution.

La sauvegarde comprend les composants suivants :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Fichiers de configuration de NetScaler Console :
  - SNMP
  - Fichiers de configuration du serveur Syslog
  - Fichiers NTP
  - Certificats SSL
  - Fichiers Control Center
- Sauvegardes des instances NetScaler gérées par le serveur NetScaler Console.
- Modèles d'audit de configuration.
- Données système stockées dans la base de données :
  - Liste des locataires et des utilisateurs créés.
  - Configuration du serveur d'authentification externe (LDAP, RADIUS et autres).
  - Tâches de configuration et modèles de tâches créés.
- Données d'infrastructure et d'application stockées dans la base de données :
  - Données des instances NetScaler ajoutées et gérées.
  - Détails du profil d'instance, détails de version, détails du groupe d'instances, etc.
  - Une application statique (groupe de serveurs virtuels) créée par l'administrateur.
- Paramètres SNMP.

REMARQUE

Les données d'analyse, les événements, les licences NetScaler Console et les messages syslog sont exclus de la sauvegarde.

Sauvegarder la configuration de NetScaler Console

Par défaut, le serveur NetScaler Console sauvegarde la configuration toutes les 24 heures (à 00h30). Vous pouvez également planifier et sélectionner l'heure de la sauvegarde. De plus, vous pouvez déplacer une copie du fichier sauvegardé vers un autre système.

La sauvegarde est stockée sous forme de fichier TAR compressé qui peut également être chiffré. Par défaut, trois fichiers de sauvegarde sont conservés sur le serveur. Pour éviter tout problème d'espace disque insuffisant, vous pouvez stocker un maximum de 10 fichiers de sauvegarde sur

© 1997–2026 Citrix Systems, Inc. All rights reserved.

votre serveur NetScaler Console. Cependant, nous vous recommandons de stocker des copies de vos fichiers de sauvegarde sur le serveur ou de (#transfer-a-citrix-adm-backup-file-to-an-external-system) à titre de précaution.

Pour sauvegarder une configuration NetScaler Console :

1. Accédez à **Paramètres > Fichiers de sauvegarde**, puis cliquez sur **Sauvegarder**.
2. Pour chiffrer le fichier de sauvegarde, cochez la case **Protéger le fichier par mot de passe**, puis saisissez un mot de passe pour chiffrer le fichier.



Transférer un fichier de sauvegarde NetScaler Console vers un système externe

Vous pouvez transférer une copie du fichier de sauvegarde vers un autre système à titre de précaution. Lorsque vous souhaitez restaurer la configuration, téléchargez d'abord le fichier sur le serveur NetScaler Console, puis effectuez (#restore-the-citrix-adm-configuration-from-a-backup-file).

Pour transférer un fichier de sauvegarde NetScaler Console :

1. Accédez à **Paramètres > Fichiers de sauvegarde**.
2. Sélectionnez le fichier de sauvegarde que vous souhaitez déplacer vers un autre système, puis cliquez sur **Transférer**.
3. Sur la page **Fichiers de sauvegarde**, spécifiez les paramètres suivants :
    - **Serveur** - Adresse IP du système vers lequel vous souhaitez transférer le fichier sauvegardé.
    - **Nom d'utilisateur et mot de passe** - Informations d'identification de l'utilisateur du nouveau système où les fichiers sauvegardés sont copiés.
    - **Port** - Numéro de port du système vers lequel les fichiers sont transférés.
    - **Protocole de transfert** - Protocole utilisé pour effectuer le transfert du fichier de sauvegarde. Vous pouvez sélectionner les protocoles SCP, SFTP ou FTP pour transférer le fichier sauvegardé.
    - **Chemin du répertoire** - L'emplacement où le fichier de sauvegarde est transféré sur le nouveau système.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Vous pouvez supprimer le fichier de sauvegarde de NetScaler Console après le transfert en cochant la case **Supprimer le fichier d'Application Delivery Management après le transfert**.
5. Cliquez sur **OK** pour effectuer le transfert.



REMARQUE

Pour enregistrer une copie du fichier de sauvegarde sur votre système local, accédez à **Paramètres > Fichiers de sauvegarde**, sélectionnez le fichier que vous souhaitez copier, puis cliquez sur **Télécharger**.

Restaurer la configuration de NetScaler Console à partir d'un fichier de sauvegarde

Lorsque vous restaurez la configuration de NetScaler Console à partir d'un fichier précédemment sauvegardé, l'opération de restauration décompresse le fichier de sauvegarde, puis restaure la configuration. L'opération de restauration supprime la configuration existante et la remplace par la configuration du fichier de sauvegarde.

REMARQUE

- L'opération de restauration échoue si le fichier de sauvegarde est renommé ou si son contenu est modifié.
- Copiez les fichiers de licence dans le répertoire `/mpsconfig/license/` avant de lancer la restauration sur NetScaler Console. L'ID d'hôte du périphérique cible doit correspondre à l'ID d'hôte présent dans le fichier de licence copié.

Pour restaurer une configuration NetScaler Console à partir d'un fichier de sauvegarde :

1. Accédez à **Paramètres > Fichiers de sauvegarde**.
2. Sélectionnez le fichier de sauvegarde que vous souhaitez restaurer, puis cliquez sur **Restaurer**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

Pour restaurer la configuration à partir d'un fichier de sauvegarde stocké dans un système externe, téléchargez le fichier de sauvegarde sur le serveur NetScaler Console avant d'effectuer l'opération de restauration. Pour télécharger le fichier, accédez à **Paramètres > Fichiers de sauvegarde**, puis cliquez sur **Télécharger**.

Instantanés de VM de NetScaler Console dans un déploiement haute disponibilité

Vous pouvez prendre des instantanés des serveurs NetScaler Console dans le déploiement HA avant de commencer votre mise à niveau. Les instantanés capturent l'état complet de la machine virtuelle au moment où vous les prenez.

Prendre un instantané des serveurs NetScaler Console

Utilisez la séquence suivante pour prendre des instantanés des serveurs NetScaler Console :

1. Serveur secondaire NetScaler Console
2. Serveur principal NetScaler Console

Pour prendre un instantané des serveurs NetScaler Console :

1. Sur votre hyperviseur, sélectionnez le serveur secondaire NetScaler Console dans la liste des machines virtuelles.
2. Prenez un instantané de la VM.

   REMARQUE :

   Nous vous recommandons de sélectionner **Prendre la mémoire de la VM** lors de la prise de l'instantané.

3. Donnez un nom significatif à l'instantané et saisissez une description, si nécessaire.

   L'instantané est stocké dans le répertoire VM par défaut.
4. Répétez les mêmes étapes pour le serveur principal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE :

Vous n'avez pas besoin d'éteindre la VM lors de la prise d'un instantané.

Restaurer un instantané des serveurs NetScaler Console

Lorsque vous restaurez un instantané, vous ramenez la mémoire, les paramètres et l'état des disques de la machine virtuelle à l'état dans lequel ils se trouvaient au moment où vous avez pris l'instantané.

Utilisez la séquence suivante pour restaurer les instantanés des serveurs NetScaler Console :

1. Serveur principal NetScaler Console
2. Serveur secondaire NetScaler Console

Pour restaurer l'instantané des serveurs NetScaler Console :

1. Sur votre hyperviseur, sélectionnez le serveur principal NetScaler Console dans la liste des machines virtuelles.
2. Cliquez avec le bouton droit sur la VM et rétablissez l'instantané.

   La machine virtuelle est rétablie à l'instantané le plus récent.
3. Répétez les mêmes étapes pour le serveur secondaire NetScaler Console.

Afficher les informations d'audit

Les journaux d'audit contiennent des enregistrements avec certaines informations pour une durée spécifique, telles que les détails de l'utilisateur, les opérations et les actions effectuées. Vous pouvez afficher les messages syslog pour les scénarios d'exemple suivants :

- Si votre NetScaler® Console est une paire HA et s'il y a un problème de latence dans la réplication de la base de données entre les nœuds primaire et secondaire, vous pouvez afficher les détails sous forme d'événement.
- S'il y a des tentatives de connexion invalides (erreur de nom d'utilisateur ou de mot de passe) ou des connexions réussies, vous pouvez afficher les détails sous forme d'événement.

En tant qu'administrateur, vous pouvez utiliser ces journaux pour maintenir la sécurité et pour récupérer les transactions perdues.

Pour configurer un serveur syslog sur NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Paramètres > Messages du journal d'audit > Serveurs Syslog**.
2. Dans la page **Serveur Syslog**, cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur Syslog**, saisissez les valeurs suivantes :
   - **Nom** - Nom du serveur syslog.
   - **Adresse IP** - Adresse IP du serveur syslog.
   - **Port** - Port du serveur syslog.
4. Choisissez les niveaux de journalisation (Tous, Aucun ou Personnalisé).
5. Cliquez sur **Créer**.

Pour configurer le format de date et d'heure syslog sur NetScaler Console :

1. Accédez à **Paramètres > Messages du journal d'audit > Serveurs Syslog**.
2. Dans la page **Serveur Syslog**, sélectionnez un serveur syslog, puis cliquez sur **Paramètres Syslog**.
3. Sur la page **Configurer les paramètres Syslog**, spécifiez le format de date et d'heure.
4. Cliquez sur **OK**.

Pour afficher les messages syslog sur NetScaler Console :

Accédez à **Paramètres > Messages du journal d'audit**.

Vous pouvez également appliquer des filtres parmi les filtres suivants et afficher les messages du journal système :

- Événement
- Message
- Module
- Gravité
- Source

Pour plus d'informations, consultez Références des messages Syslog.

Configurer les paramètres SSL

SSL (Secure Socket layer) et TLS (Transport Layer Security) sont des protocoles de sécurité réseau couramment utilisés qui fournissent une communication chiffrée entre les utilisateurs et les

© 1997–2026 Citrix Systems, Inc. All rights reserved.

serveurs. Vous pouvez configurer les paramètres SSL sur NetScaler Console et spécifier le type de clients qui se connectent au système.

Pour configurer les paramètres SSL pour NetScaler Console :

1. Accédez à **Paramètres > Administration**. Sous **Paramètres SSL**, cliquez sur **Configurer les paramètres SSL**.
2. Sur la page **Paramètres SSL**, examinez les paramètres de protocole actuels et les suites de chiffrement appliquées au système.
3. Pour modifier les paramètres de protocole, cliquez sur l'icône **+** dans **Paramètres de protocole** sous **Modifier les paramètres**, et apportez les modifications souhaitées.
4. Pour modifier les suites de chiffrement appliquées, cliquez sur l'icône **+** dans **Suites de chiffrement** sous **Modifier les paramètres**, et apportez les modifications souhaitées.
5. Cliquez sur **OK**, puis cliquez sur **Fermer**.

Surveiller l'utilisation du CPU, de la mémoire et du disque

Vous pouvez utiliser les informations conservées dans les journaux et les statistiques. Ces informations sont également affichées dans des rapports qui vous aident à configurer et à maintenir NetScaler Console.

Pour surveiller l'utilisation du CPU, de la mémoire et du disque,

- **Déploiement autonome.** Accédez à **Système** \> **Statistiques**. Vous pouvez afficher les graphiques d'utilisation du CPU, de la mémoire et du disque en temps réel.

  

- **Déploiement haute disponibilité.** Accédez à **Paramètres > Déploiement**. Les statistiques relatives à la mémoire, au CPU, à l'espace disque et aux instances gérées sont affichées numériquement, comme illustré dans la figure suivante :

  

Configurer les paramètres de notification

Vous pouvez sélectionner un type de notification pour recevoir des notifications pour les fonctionnalités suivantes :

- **Événements** – Liste des événements générés pour les instances NetScaler. Pour plus d'informations, consultez Ajouter des actions de règle d'événement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Licences** – Liste des licences actuellement actives, sur le point d'expirer, etc. Pour plus d'informations, consultez L'expiration de la licence NetScaler Console.
- **Certificats SSL** – Liste des certificats SSL ajoutés aux instances NetScaler. Pour plus d'informations, consultez L'expiration du certificat SSL

NetScaler Console prend en charge les types de notification suivants :

- E-mail
- SMS
- Slack
- PagerDuty
- ServiceNow

Pour chaque type de notification, l'interface graphique de NetScaler Console affiche la liste de distribution ou le profil configuré. NetScaler Console envoie les notifications à la liste de distribution ou au profil sélectionné.

Créer une liste de distribution d'e-mails

Pour recevoir des notifications par e-mail pour les fonctions de NetScaler Console, vous devez ajouter un serveur de messagerie et une liste de distribution.

Effectuez les étapes suivantes pour créer une liste de distribution d'e-mails :

1. Accédez à **Paramètres > Notifications**.
2. Sous **E-mail**, cliquez sur **Ajouter**.
3. Dans **Créer une liste de distribution d'e-mails**, spécifiez les détails suivants :
    - **Nom** - Spécifiez le nom de la liste de distribution.
    - **Serveur de messagerie** - Sélectionnez le serveur de messagerie qui envoie la notification par e-mail. Si vous souhaitez ajouter un serveur de messagerie, cliquez sur **Ajouter**.
    - **De** - Spécifiez l'adresse e-mail à partir de laquelle NetScaler Console doit envoyer des messages.
    - **À** - Spécifiez les adresses e-mail auxquelles NetScaler Console doit envoyer des messages.
    - **Cc** - Spécifiez les adresses e-mail auxquelles NetScaler Console doit envoyer des copies de messages.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Cci** - Spécifiez les adresses e-mail auxquelles NetScaler Console doit envoyer des copies de messages sans afficher les adresses.



4. Cliquez sur **Créer**.

Répétez cette procédure pour créer plusieurs listes de distribution d'e-mails. L'onglet **E-mail** affiche toutes les listes de distribution d'e-mails présentes dans NetScaler Console.

Créer une liste de distribution SMS

Pour recevoir des notifications SMS pour les fonctions de NetScaler Console, vous devez ajouter un serveur SMS et des numéros de téléphone.

Effectuez les étapes suivantes pour configurer les paramètres de notification SMS :

1. Accédez à **Paramètres > Notifications**.
2. Dans **SMS**, cliquez sur **Ajouter**.
3. Dans **Créer une liste de distribution SMS**, spécifiez les détails suivants :
   - **Nom** - Spécifiez le nom de la liste de distribution.
   - **Serveur SMS** - Sélectionnez le serveur SMS qui envoie la notification SMS.
   - **À** - Spécifiez le numéro de téléphone auquel NetScaler Console doit envoyer des messages.
4. Cliquez sur **Créer**.

Répétez cette procédure pour créer plusieurs listes de distribution SMS. L'onglet **SMS** affiche toutes les listes de distribution SMS présentes dans NetScaler Console.

Créer un profil Slack

Pour recevoir des notifications Slack pour les fonctions de NetScaler Console, vous devez créer un profil Slack.

Effectuez les étapes suivantes pour créer un profil Slack :

1. Accédez à **Paramètres > Notifications**.
2. Dans **Slack**, cliquez sur **Ajouter**.
3. Dans **Créer un profil Slack**, spécifiez les détails suivants :
   - **Nom du profil** - Spécifiez le nom du profil. Ce nom apparaît dans la liste des profils Slack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Nom du canal** - Spécifiez le nom du canal Slack auquel NetScaler Console doit envoyer des notifications.
- **URL du webhook** - Spécifiez l'URL du webhook du canal. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom du canal. Et toutes les notifications d'événements envoyées à cette URL sont publiées sur le canal Slack désigné. Voici un exemple de webhook : `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

4. Cliquez sur **Créer**.

Répétez cette procédure pour créer plusieurs profils Slack. L'onglet **Slack** affiche tous les profils Slack présents dans NetScaler Console.

Créer un profil PagerDuty

Vous pouvez ajouter un profil PagerDuty pour surveiller les notifications d'incidents en fonction des configurations PagerDuty. PagerDuty vous permet de configurer des notifications par e-mail, SMS, notification push et appel téléphonique sur un numéro enregistré.

Avant d'ajouter un profil PagerDuty dans NetScaler Console, assurez-vous d'avoir effectué les configurations requises dans PagerDuty. Pour commencer avec PagerDuty, consultez la documentation PagerDuty.

Effectuez les étapes suivantes pour créer un profil PagerDuty :

1. Accédez à **Paramètres > Notifications**.
2. Dans **PagerDuty**, cliquez sur **Ajouter**.
3. Dans **Créer un profil PagerDuty**, spécifiez les détails suivants :
   - **Nom du profil** - Spécifiez un nom de profil de votre choix.
   - **Clé d'intégration** - Spécifiez la clé d'intégration. Vous pouvez obtenir cette clé depuis votre portail PagerDuty. Lors de la création d'un service dans PagerDuty pour l'intégration, utilisez l'option **Intégration d'API d'événements génériques**.
4. Cliquez sur **Créer**.

Pour plus d'informations, consultez Services and Integrations dans la documentation PagerDuty.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Répétez cette procédure pour créer plusieurs profils PagerDuty. L'onglet **PagerDuty** affiche tous les profils PagerDuty présents dans NetScaler Console.

Afficher le profil ServiceNow

Lorsque vous souhaitez activer les notifications ServiceNow pour les événements NetScaler et les événements NetScaler Console, vous devez intégrer NetScaler Console à ServiceNow à l'aide du connecteur ITSM. Pour plus d'informations, consultez Integrate NetScaler Console with the ServiceNow instance.

Effectuez les étapes suivantes pour afficher et vérifier le profil ServiceNow :

1. Accédez à **Settings > Notifications**.
2. Dans **ServiceNow**, sélectionnez le profil **Citrix_Workspace_SN** dans la liste.
3. Cliquez sur **Test** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

   Si vous souhaitez afficher les tickets ServiceNow dans l'interface graphique de NetScaler Console, sélectionnez **ServiceNow Tickets**.

Générer un fichier de support technique

Nous vous recommandons de générer une archive des données et des statistiques de NetScaler Console avant de contacter le support technique pour le débogage d'un problème. L'archive est un fichier TAR que vous pouvez envoyer à l'équipe du support technique.

REMARQUE

Pour les serveurs NetScaler Console en mode haute disponibilité, vous pouvez générer un fichier de support technique à partir de l'un ou l'autre des serveurs. Citrix vous conseille de ne pas utiliser l'adresse IP du serveur virtuel d'équilibrage de charge pour générer le fichier de support technique.

Pour configurer et envoyer un fichier de support technique depuis NetScaler Console :

1. Accédez à **Paramètres** \> **Diagnostics** \> **Support technique**, puis cliquez sur **Générer un fichier de support technique**.
2. Sur la page **Générer un fichier de support**, sélectionnez les options suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Collecter les journaux de débogage** – Sélectionnez cette option pour collecter les journaux `afdecoder`.
- **Durée** – Saisissez la durée pendant laquelle les journaux de débogage doivent être collectés. Cette option n'apparaîtra que si vous activez l'option **Collecter les journaux de débogage**.
- **Collecter la distribution des données** – Sélectionnez cette option pour collecter des journaux distincts et diversifiés à partir de la base de données.

```
 The archive file is created as a TAR file.



 For example, the archive file that is created might be named as
follows:
Citrix_ADM_&lt;ADM_IP_address>_&lt;DDMMYY>_&lt;time_stamp>.tar.gz
```

1. Vous pouvez envoyer les fichiers de support technique à l'équipe de support de deux manières :

   a. Vous pouvez télécharger le fichier depuis l'interface graphique de NetScaler Console vers votre stockage local, puis utiliser un navigateur web pour le télécharger vers Citrix Insight Services (CIS).

   b. Vous pouvez également télécharger les fichiers de support technique sur le site web de CIS en exécutant un script sur la Console.

      i. À l'aide de SSH, connectez-vous à la Console.

      ii. Passez à l'invite Shell et tapez :

      /mps/collector_upload.pl

La commande complète est donnée ci-dessous avec les attributs que vous devez fournir :

```
/mps/collector_upload.pl [-proxy
[<proxy_user>:<proxy_password>@]<proxy_host>:<proxy_port>] [-user <user>]
[-password <password>] [-sr <sr>] [-description <description>] [-debug]
<file>
```

L'avantage d'exécuter le script Perl est que vous n'avez pas à télécharger le fichier de support technique de NetScaler Console vers votre système local, puis à le télécharger vers CIS. En

© 1997–2026 Citrix Systems, Inc. All rights reserved.

option, vous pouvez télécharger le fichier directement vers CIS en utilisant un proxy depuis la console.

Assurez-vous d'avoir un compte sur CIS. Vous pouvez utiliser vos informations d'identification de compte Citrix pour télécharger des fichiers vers CIS.

Que faire si vous n'avez pas de serveur proxy ? Ou si vous rencontrez des problèmes avec les proxys de transfert SSL ? (Cela peut arriver si le script Perl ne fait pas confiance au certificat racine du serveur proxy.) Vous pouvez toujours télécharger le fichier directement depuis le shell de NetScaler Console vers CIS.

REMARQUE

Vous pouvez toujours télécharger le fichier et l'envoyer par e-mail à l'équipe de support technique de Citrix si NetScaler Console ne parvient pas à télécharger le fichier vers CIS depuis la console. Ou bien, vous pouvez télécharger le fichier de NetScaler Console vers votre stockage local, puis utiliser un navigateur web pour le télécharger vers CIS.

Configurer un groupe de chiffrements

Un groupe de chiffrements est un ensemble de suites de chiffrement que vous liez à un serveur virtuel SSL, un service ou un groupe de services sur l'instance Citrix NetScaler. Une suite de chiffrement comprend un protocole, un algorithme d'échange de clés (`Kx`), un algorithme d'authentification (`Au`), un algorithme de chiffrement (`Enc`) et un algorithme de code d'authentification de message (`Mac`).

Pour ajouter un groupe de chiffrements sur NetScaler Console :

1. Accédez à **Paramètres > Administration**
2. Sous **Paramètres SSL**, cliquez sur **Groupes de chiffrements**
3. Cliquez sur **Ajouter**
4. Sur la page **Créer un groupe de chiffrements**, entrez les détails suivants :
    - **Nom du groupe** - Nom du groupe de chiffrements.
    - **Description du groupe de chiffrements** – Fournissez une description pour votre groupe de chiffrements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Suites de chiffrement** – Cliquez sur Ajouter pour sélectionner les suites de chiffrement dans la liste Disponible, puis déplacez les suites de chiffrement sélectionnées (ou toutes) vers la liste Configuré.

5. Cliquez sur **Créer**.



Créer une destination de trap SNMP, une communauté de gestionnaires et des utilisateurs

Chaque fois qu'une condition anormale se produit sur la NetScaler Console, un trap SNMP est généré. Les traps sont ensuite envoyés à un périphérique distant appelé serveur de destination de trap ou *destination de trap SNMP*. Ici, NetScaler Console est configurée comme destination de trap. Vous pouvez interroger l'agent SNMP pour obtenir des informations spécifiques au système à partir d'un périphérique distant appelé *gestionnaire SNMP*. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et les envoie au gestionnaire SNMP.

Pour créer une destination de trap SNMP sur NetScaler Console :

1. Accédez à **Système** \> **SNMP** \> **Destinations de trap**.
2. Sous **Traps SNMP**, cliquez sur **Ajouter** pour créer un trap SNMP, puis spécifiez les détails suivants :
   - **Version.** Sélectionnez la version SNMP à utiliser.
   - **Serveur de destination.** Nom ou adresse IP de la destination de trap.
   - **Port.** Entrez le port de la destination de trap. Le port est défini sur 162 par défaut.
   - **Communauté.** Spécifiez la chaîne de communauté à utiliser lors de l'envoi d'un trap à l'écouteur de trap.
3. Cliquez sur **Créer**.

REMARQUE

Si vous créez une destination de trap SNMP v3, spécifiez les informations d'identification de l'utilisateur SNMP auxquelles vous souhaitez lier le trap. Pour ajouter une information d'identification d'utilisateur SNMP, cliquez sur **Insérer**, puis ajoutez l'utilisateur à partir de la liste des utilisateurs SNMP disponibles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour créer une communauté de gestionnaires SNMP :

1. Accédez à **Système** \> **SNMP** \> **Gestionnaires**.
2. Sous **Gestionnaire SNMP**, cliquez sur **Ajouter** pour créer une communauté de gestionnaires SNMP, puis spécifiez les détails suivants :
   - **Gestionnaire SNMP.** Saisissez le nom ou l'adresse IP du gestionnaire SNMP.
   - **Communauté.** Spécifiez la chaîne de communauté à utiliser lors de l'envoi de traps au récepteur de traps.
3. Vous pouvez éventuellement cocher la case **Activer le réseau de gestion** pour spécifier le **masque de sous-réseau** qui est le masque de sous-réseau du réseau du gestionnaire SNMP.
4. Cliquez sur **Créer**.

Pour créer un utilisateur SNMP :

1. Accédez à **Système** \> **SNMP** \> **Utilisateurs**.
2. Sous **Utilisateur SNMP**, cliquez sur **Ajouter**.
3. Saisissez le nom d'utilisateur et attribuez un niveau de sécurité à l'utilisateur à partir du menu.
4. En fonction du niveau de sécurité que vous avez attribué à l'utilisateur, fournissez des protocoles d'authentification supplémentaires, tels que des protocoles d'authentification, des mots de passe de confidentialité, et attribuez des vues SNMP.

Configurer et afficher les alarmes système

Vous pouvez activer et configurer un ensemble d'alarmes pour surveiller l'état de vos serveurs NetScaler Console. Vous devez configurer les alarmes système pour vous assurer d'être informé de tout problème système critique ou majeur. Par exemple, vous pourriez vouloir être averti si l'utilisation du CPU est élevée ou s'il y a plusieurs échecs de connexion au serveur. Pour certaines catégories d'alarmes, telles que cpuUsageHigh ou memoryUsageHigh, vous pouvez définir des seuils et la gravité (telle que Critique ou Majeure) pour chacune. Pour certaines catégories, telles que inventoryFailed ou loginFailure, vous ne pouvez définir que la gravité. Lorsque le seuil est dépassé pour une catégorie d'alarme (par exemple, memoryUsageHigh) ou lorsqu'un événement correspondant à la catégorie d'alarme se produit (par exemple, **loginFailure**), un message est enregistré dans le système et vous pouvez le consulter en tant que message syslog. Vous pouvez en outre configurer des notifications pour recevoir un e-mail ou un SMS correspondant à vos paramètres d'alarme.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez attribuer ou modifier la gravité d'une alarme. Les niveaux de gravité que vous pouvez attribuer sont Critique, Majeure, Mineure, Avertissement et Information.

Considérez un scénario où vous souhaitez surveiller chaque tentative de sauvegarde échouée. Vous pouvez activer l'alarme backupFailed et lui attribuer une gravité, telle que Majeure. Chaque fois que NetScaler Console tente de sauvegarder les fichiers système et que la tentative échoue, une alarme est déclenchée. Vous pouvez afficher le message sur la NetScaler Console ou recevoir des notifications par e-mail ou SMS.

Pour configurer l'alarme, vous devez sélectionner l'alarme backupFailed et spécifier le niveau de gravité comme Majeure. L'alarme est activée par défaut.

Pour configurer et afficher une alarme système à l'aide de NetScaler Console :

1. Accédez à **Paramètres > SNMP**. Cliquez sur **Alarmes** dans le coin supérieur droit.

   

2. Sélectionnez l'alarme que vous souhaitez configurer (par exemple, backupFailed) et cliquez sur **Modifier** pour modifier ses paramètres.
3. L'alarme est activée par défaut. Attribuez un niveau de gravité (exemple : Majeure), puis cliquez sur **OK**.

REMARQUE

Pour quelques alarmes, vous ne pouvez pas définir de seuil. Lorsque l'alarme est déclenchée, vous pouvez afficher l'événement généré en tant que message syslog.

Pour afficher l'événement généré par l'alarme backupFailed à l'aide de NetScaler Console :

1. Accédez à **Système** > **Audit**.
2. Dans la page **Audit**, sous **Messages d'audit**, sélectionnez **Messages Syslog**.
3. Dans le champ de recherche, saisissez le nom de l'alarme.Dans cet exemple, vous pouvez voir qu'un événement a été généré pour une tentative de sauvegarde échouée.

   

   Vous pouvez également configurer des notifications pour vous envoyer un e-mail ou un SMS (Short Message Service) lorsqu'une alarme est déclenchée. Pour plus d'informations sur la configuration des notifications système, consultez Comment configurer les paramètres de notification système de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter des limites de seuil aux alarmes d'utilisation du disque

Les alarmes d'utilisation du disque sont déclenchées lorsque la quantité d'espace disque utilisée sur le serveur NetScaler Console dépasse un seuil prédéfini.

En tant qu'administrateur, lorsque vous recevez des alertes, vous pouvez choisir de supprimer les données inutiles ou d'allouer des ressources de stockage supplémentaires pour éviter les interruptions de service ou la dégradation des performances.

À partir de la version 14.1-25.x, vous pouvez également ajouter un seuil de niveau inférieur pour les alarmes d'utilisation du disque. Avec cette valeur de seuil, vous pouvez définir une limite de niveau inférieur pour recevoir des alertes avant qu'une limite de seuil supérieur ne soit atteinte.

Pour configurer un seuil de niveau inférieur :

1. Accédez à **Paramètres > SNMP > Alarmes** et dans le champ de recherche, saisissez diskUtilizationHigh pour afficher les alarmes d'utilisation du disque.
2. Sélectionnez l'alarme et cliquez sur **Modifier**.
3. Dans la page **Configurer l'alarme**, sélectionnez **Configurer un seuil de niveau inférieur**. Saisissez la limite du seuil de niveau inférieur.



Par exemple, si vous définissez un seuil d'utilisation du disque inférieur de 60 et un seuil supérieur de 80, vous recevez une alerte lorsque l'utilisation du disque dépasse 60 % de la capacité du disque. Ce paramètre vous permet de prendre des mesures correctives avant que l'utilisation du disque n'atteigne 80 %.

Créer des gestionnaires et des utilisateurs SNMP pour l'agent NetScaler

Vous pouvez interroger l'agent SNMP pour obtenir des informations spécifiques au système à partir d'un périphérique distant appelé gestionnaire SNMP. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et envoie les données au gestionnaire SNMP.

Vous pouvez ajouter un gestionnaire SNMP pour interroger un agent NetScaler. Le gestionnaire est conforme à SNMP V2 et V3. Si vous spécifiez un ou plusieurs gestionnaires SNMP, l'agent NetScaler n'accepte pas les requêtes SNMP d'aucun hôte, à l'exception des gestionnaires SNMP spécifiés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ajouter un gestionnaire SNMP v2

Pour ajouter un gestionnaire SNMP v2 pour l'agent NetScaler :

1. Accédez à **Infrastructure > Agents**, sélectionnez un agent NetScaler, puis cliquez sur **Sélectionner l'action > Gérer SNMP**.
2. Dans l'onglet **SNMP > Gestionnaire SNMP**, cliquez sur **Ajouter**.
3. Dans la page **Créer un gestionnaire SNMP**, spécifiez les détails suivants :
   - **Gestionnaire SNMP**. Saisissez le nom ou l'adresse IP du gestionnaire SNMP.
   - **Version**. Sélectionnez v2.
   - **Communauté**. Saisissez un nom de communauté. Une configuration de communauté SNMP authentifie les requêtes SNMP provenant des gestionnaires SNMP.
   - **Activer le réseau de gestion** : Cochez cette case pour spécifier le masque de sous-réseau du réseau du gestionnaire SNMP.
   - **Masque de sous-réseau** : Saisissez le masque de sous-réseau associé à une adresse IP.
4. Cliquez sur **Créer**.

Ajouter un gestionnaire SNMP v3

Pour ajouter un gestionnaire SNMP v3 pour l'agent NetScaler :

1. Accédez à **Infrastructure > Agents**, sélectionnez un agent NetScaler, puis cliquez sur **Sélectionner une action > Gérer SNMP**.
2. Dans l'onglet **SNMP > Gestionnaire SNMP**, cliquez sur **Ajouter**.
3. Dans la page **Créer un gestionnaire SNMP**, spécifiez les détails suivants :
   - **Gestionnaire SNMP**. Entrez le nom ou l'adresse IP du gestionnaire SNMP.
   - **Version**. Sélectionnez v3.
   - **Activer le réseau de gestion** : Cochez cette case pour spécifier le masque de réseau du réseau du gestionnaire SNMP.
   - **Masque de réseau** : Entrez le masque de sous-réseau associé à une adresse IP.
4. Cliquez sur **Créer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Une boîte de dialogue apparaît, confirmant qu'un gestionnaire SNMP est créé et vous invitant à configurer un utilisateur SNMP.



REMARQUE

Vous devez configurer un utilisateur SNMP pour un gestionnaire SNMP v3. Pour configurer l'utilisateur SNMP, accédez à **SNMP > Utilisateur SNMP**.

Ajouter un utilisateur SNMP

Ajoutez un utilisateur SNMP pour répondre aux requêtes SNMP v3 d'un gestionnaire SNMP.

Pour ajouter un utilisateur SNMP pour l'agent NetScaler :

1. Accédez à **Infrastructure > Agents**, sélectionnez un agent NetScaler, puis cliquez sur **Sélectionner une action > Gérer SNMP**.
2. Dans l'onglet **SNMP > Utilisateur SNMP**, cliquez sur **Ajouter**.
3. Dans la page **Créer un utilisateur SNMP**, ajoutez les détails suivants :

   - **Nom**. Saisissez le nom d'utilisateur.
   - **Niveau de sécurité**. Niveau de sécurité requis pour la communication entre l'agent NetScaler et le gestionnaire SNMP.

     Sélectionnez l'un des niveaux de sécurité suivants :
   - **noAuthNoPriv**. Ne nécessite ni authentification ni chiffrement.



   - **authNoPriv**. Nécessite une authentification mais pas de chiffrement.



   - **authPriv**. Nécessite une authentification et un chiffrement.



   En fonction du niveau de sécurité que vous avez attribué à l'utilisateur, fournissez des protocoles d'authentification supplémentaires, tels que les protocoles d'authentification, les mots de passe de confidentialité, et attribuez des vues SNMP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion des vues SNMP

Les vues SNMP sont utilisées pour implémenter le contrôle d'accès pour un utilisateur SNMP. Les vues SNMP restreignent l'accès de l'utilisateur à des portions spécifiques de la MIB.

Pour autoriser ou restreindre un OID SNMP pour l'agent NetScaler :

1. Accédez à **Infrastructure > Agents > Gérer SNMP** et dans l'onglet **Vue SNMP**, cliquez sur **Ajouter**.
2. Dans **Créer une vue SNMP**, saisissez les détails suivants :
   - **Nom de la vue** : Un nom pour la vue SNMP. Une instance peut avoir plusieurs vues SNMP portant le même nom, différenciées par les paramètres du sous-arbre.
   - **Sous-arbre** : Une branche particulière (sous-arbre) de l'arborescence MIB que vous souhaitez associer à cette vue SNMP. Vous devez spécifier le sous-arbre comme un OID SNMP.
   - **Type** : Ce champ vous permet d'inclure ou d'exclure des sous-arbres d'une vue.
3. Cliquez sur **Créer**.



Configurer les paramètres de l'agent

Vous pouvez modifier l'intervalle de maintien en vie et les exigences de changement de mot de passe de l'agent NetScaler Console.

Définir l'intervalle de maintien en vie de l'agent

Le serveur et l'agent NetScaler Console maintiennent la même connexion TCP pendant l'intervalle de maintien en vie spécifié. Un agent utilise cette connexion pour envoyer les données des instances gérées au serveur NetScaler Console.

1. Accédez à **Paramètres > Administration**.
2. Sélectionnez **Système, Fuseau horaire, URL autorisées et Paramètres de l'agent** sous **Configurations système**.
3. Dans **Paramètres de base > Paramètres de l'agent**, spécifiez l'intervalle de maintien en vie entre 30 et 120 secondes.
4. Cliquez sur **Enregistrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modifier le mot de passe de l'agent sans le mot de passe actuel

Vous pouvez autoriser la modification des mots de passe de l'agent sans leur mot de passe actuel.

1. Accédez à **Paramètres > Administration**.
2. Sélectionnez **Système, Fuseau horaire, URL autorisées et Paramètres de l'agent** sous **Configurations système**.
3. Dans la case à cocher **Paramètres de base > Paramètres de l'agent > Supprimer la condition préalable du mot de passe actuel pour le changement de mot de passe de l'agent**, vous pouvez effectuer les opérations suivantes :
   - Cochez la case pour supprimer le champ **Mot de passe actuel** de la page **Modifier le mot de passe de l'agent**.
   - Décochez la case pour conserver le champ **Mot de passe actuel** dans la page **Modifier le mot de passe de l'agent**.
4. Cliquez sur **Enregistrer**.

REMARQUE

Pour afficher la page **Modifier le mot de passe de l'agent**, accédez à **Infrastructure > Instances > Agents**, sélectionnez un agent et cliquez sur **Sélectionner une action > Modifier le mot de passe**.

Utiliser le tableau de bord de gestion du stockage des données

Il est important de savoir quelles fonctionnalités sont utilisées dans NetScaler Console et l'utilisation des données de chacune de ces fonctionnalités. Le tableau de bord **Gestion du stockage des données** sert à cet effet et fonctionne comme votre outil de visualisation, vous permettant de comprendre le volume total de données stockées dans la base de données NetScaler Console pour les différentes fonctionnalités. Le tableau de bord indique également si le stockage consommé se situe dans les limites spécifiées ou s'il dépasse le stockage autorisé.

En tant qu'administrateur, vous pouvez effectuer les tâches suivantes dans le tableau de bord **Gestion du stockage des données** :

- Afficher la consommation de stockage des données des 30 derniers jours - Les tendances de stockage des données sont stockées dans la base de données NetScaler Console pour les 30

© 1997–2026 Citrix Systems, Inc. All rights reserved.

derniers jours. Ces tendances sont disponibles sous forme graphique ou tabulaire. Ces tendances indiquent la quantité de données entrantes et la quantité de données stockées après les cycles d'élagage planifiés dans NetScaler Console.

- Afficher l'état de l'ingestion des données - L'activité d'ingestion des données a lieu tant que le stockage consommé se situe dans les limites du stockage autorisé. Lorsque le stockage consommé dépasse le stockage autorisé, l'activité des données est suspendue.
- Envoyer des notifications - Vous pouvez configurer l'envoi de notifications lorsque le stockage consommé atteint 75 % ou 100 % du stockage autorisé, permettant aux utilisateurs de gérer leur stockage.
- Flexibilité pour gérer l'espace de stockage des données - Vous pouvez créer plus d'espace dans les données stockées en élaguant les données que vous jugez appropriées pour la suppression ou la réduction.

Accédez à **Paramètres > Stockage des données** pour afficher votre tableau de bord de stockage des données.

Les sections suivantes décrivent comment utiliser le tableau de bord **Gestion du stockage des données** pour une gestion efficace du stockage des données :

- Comprendre votre stockage de données - Cette section vous aide à comprendre comment utiliser le tableau de bord pour afficher des informations sur votre stockage de données.
- Gérer votre stockage de données - Cette section fournit des informations sur les actions que vous pouvez entreprendre dans le tableau de bord pour gérer votre stockage de données.

Comprendre votre stockage de données

Vous pouvez utiliser le tableau de bord **Gestion du stockage de données** dans NetScaler Console pour afficher les données et les graphiques qui vous aident à suivre votre utilisation du stockage de données.

Pour surveiller votre consommation de stockage de données, accédez à **Paramètres > Stockage de données**.



Le tableau de bord Gestion du stockage de données indique les informations suivantes :

- État de votre activité d'ingestion de données
- Consommation totale de stockage
- Tendances de consommation de stockage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Consommation de stockage par fonctionnalités

État de votre activité d'ingestion de données

L'ingestion de données fait référence au processus d'importation de données volumineuses et variées de toutes les instances NetScaler gérées, à travers diverses fonctionnalités telles que les événements, les Syslogs, les rapports réseau, etc., vers le stockage de NetScaler Console.

L'état de l'ingestion de données indique si NetScaler Console collecte des statistiques à partir des instances NetScaler. L'activité d'ingestion de données se poursuit tant que le stockage consommé est inférieur au stockage autorisé. Lorsque la consommation dépasse le stockage autorisé, l'ingestion de données est mise en pause.

Affichez la vignette **Ingestion de données** pour comprendre l'état actuel de l'ingestion de données. Cette vignette affiche l'un des deux états suivants :

- **Actif** - L'activité d'ingestion de données est en cours.



- **En pause** - L'activité d'ingestion de données est mise en pause car le stockage consommé dépasse le stockage autorisé.



Comment reprendre l'ingestion de données en pause

Pour reprendre votre activité d'ingestion de données, vous pouvez effectuer un élagage des données. Pour plus d'informations, consultez Effectuer l'élagage des données.

Consommation totale de stockage

Pour un aperçu rapide de votre stockage de données, consultez la vignette **Consommation de stockage**.



La vignette **Consommation de stockage** affiche le stockage total utilisé par toutes les fonctionnalités du déploiement.

Passez la souris sur le graphique en anneau pour afficher les éléments suivants :

Stockage autorisé

Le stockage autorisé est le stockage total dont vous disposez conformément à votre licence. Si vous disposez d'une licence Express, vous bénéficiez de 500 Mo de stockage autorisé. Si vous

© 1997–2026 Citrix Systems, Inc. All rights reserved.

disposez d'une licence Advanced, vous obtenez la somme de 500 Mo de stockage par VIP acheté et de tout stockage supplémentaire acheté directement sans acheter de VIP.

Considérez les scénarios suivants :

- Vous avez acheté 20 VIP. Vous obtenez 500 Mo de stockage gratuit pour chaque VIP. Votre stockage autorisé est de 20*500 = 10 Go.
- Vous avez acheté 20 VIP et un stockage additionnel de 5 Go. Vous obtenez 500 Mo de stockage gratuit pour chaque VIP. Votre stockage autorisé est de 20*500 + 5 = 15 Go.

Stockage consommé

Le stockage consommé est le stockage total utilisé par toutes les fonctionnalités du déploiement. Les critères de codage couleur suivants spécifient la quantité de stockage utilisée par les fonctionnalités :

- **Vert** - Le stockage consommé est inférieur à 75 % du stockage alloué.
- **Orange** - Le stockage consommé est compris entre 75 % et 99 % du stockage alloué.
- **Rouge** - La limite de stockage consommé a été atteinte ou est supérieure au stockage alloué actuel.

Tendances de consommation du stockage

Pour savoir comment les données sont consommées au cours des 30 derniers jours, consultez la section **Tendances de consommation du stockage**.

La section **Tendances de consommation du stockage** fournit des informations sur les fonctionnalités qui utilisent le plus ou le moins de stockage sur une période donnée et vous aide à gérer efficacement votre consommation de stockage de données.

Vous pouvez afficher les tendances des données de stockage sous l'une des formes suivantes :

- **Vue graphique** – Affiche la répartition du stockage de données entre les différentes fonctionnalités de NetScaler Console. Passez la souris sur la chronologie pour afficher les informations de stockage de données pour n'importe quel jour du mois.

  

  REMARQUE :

  La **Vue graphique** est la vue par défaut.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Vue tabulaire** – Cliquez sur **Vue tabulaire** pour afficher les informations de stockage de données sous forme de tableau.

  

  REMARQUE :

  L'affichage tabulaire vous permet de filtrer les données à l'aide du champ de recherche.

Le tableau suivant décrit les champs affichés dans la section **Tendance de consommation du stockage** :

FONCTIONNALITÉ	DESCRIPTION
Configuration	Inclut toutes les données configurables telles que les informations sur les instances, les tâches de configuration, l'audit de configuration, etc.
HDX Insight	Fournit une visibilité de bout en bout pour le trafic ICA passant par NetScaler.
Rapports réseau	Affiche les performances réseau de toutes les instances NetScaler.
Web Insight	Offre une visibilité sur les applications web d'entreprise et permet une surveillance intégrée et en temps réel des applications.
Security Insight	Aide à évaluer l'état de sécurité des applications et à prendre des mesures correctives pour sécuriser les applications.
Gateway Insight	Offre une visibilité sur les échecs rencontrés par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à NetScaler Gateway.
Événements	Surveille et gère les occurrences d'événements ou d'erreurs sur les instances NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉ	DESCRIPTION
Tableau de bord des applications	Permet de visualiser et de gérer les applications.
Bot Insight	Offre une visibilité sur les violations de bots et les actions entreprises à leur égard.
Syslog	Surveille les événements syslog générés sur les instances NetScaler si vous avez configuré votre appareil pour rediriger tous les messages syslog vers NetScaler Console.
Video Insight	Surveille les métriques des techniques d'optimisation vidéo utilisées par les instances NetScaler.
Transactions détaillées	Offre une visibilité sur les transactions web et affiche visuellement la métrique du temps de réponse répartie entre le client, NetScaler et le serveur.

Consommation de stockage par fonctionnalités

Pour en savoir plus sur la répartition du stockage des données entre les différentes fonctionnalités, consultez la section **Consommation de stockage par fonctionnalités au *jj mmm***.

Consommation de stockage par fonctionnalités au *jj mmm* vous aide à comprendre :

- L'espace de stockage utilisé par toutes les différentes fonctionnalités dans NetScaler Console
- Le pourcentage d'espace que les fonctionnalités consomment un jour donné

Pour trier les entrées du tableau, utilisez les en-têtes du tableau. NetScaler Console trie le tableau par ordre alphanumérique de haut en bas en fonction des données de la colonne choisie. Pour trier le tableau dans l'ordre inverse, cliquez à nouveau sur l'en-tête de colonne.

Pour plus d'informations sur l'élagage de vos données, l'historique d'élagage et les journaux d'événements de stockage, consultez Gérer votre stockage de données

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gérer votre espace de stockage

Vous pouvez utiliser le tableau de bord de la **Gestion du stockage des données** pour observer votre utilisation du stockage des données et prendre les mesures nécessaires pour libérer de l'espace ou augmenter le stockage lorsque votre stockage de données dépasse la limite sous licence.



La vignette **Actions** affiche la liste des étapes recommandées que vous pouvez suivre pour gérer votre capacité de stockage :

- Examiner la politique de rétention des données
- Effectuer l'élagage des données
- Notifier en cas de dépassement de la limite de stockage

Effectuer l'élagage des données

Élaguez vos données pour optimiser les ressources de stockage et obtenir plus d'espace de stockage. En plus de libérer de l'espace, l'élagage des données améliore la qualité des données et accélère les temps de traitement. Nous vous recommandons d'examiner et de purger les données inutiles à intervalles réguliers. Ce processus garantit que vos ressources sont utilisées judicieusement et que NetScaler Console est agile et réactif.

Pour élaguer vos données :

1. Dans la page **Gestion du stockage des données**, faites défiler jusqu'à la section ***Consommation de stockage par fonctionnalités au aaaa-mm-jj***.
2. Sélectionnez une ou plusieurs fonctionnalités et cliquez sur **Élaguer**. Vous ne pouvez pas sélectionner **Config** car elle inclut toutes les configurations système.

   Une fenêtre contextuelle vous invite à confirmer si vous souhaitez supprimer toutes les données pour les fonctionnalités sélectionnées. Cliquez sur **Oui, élaguer**.

   

Afficher l'historique d'élagage

Cliquez sur **Afficher l'historique d'élagage** pour obtenir des détails sur toutes les activités d'élagage que vous avez effectuées dans NetScaler Console.

Journaux des tâches(/en-us/netscaler-application-delivery-management-software/media/view-prune-history.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

La page **Journaux d'élagage : Journaux des tâches** affiche la liste de toutes les tâches d'élagage, y compris leurs statuts respectifs, l'heure de début et l'heure de fin.

Pour comprendre quelles fonctionnalités ont été supprimées lors de chaque opération d'élagage, sélectionnez une tâche et cliquez sur **Journal des fonctionnalités**.

Journaux des fonctionnalités(/en-us/netscaler-application-delivery-management-software/media/view-prune-history-feature.png)

Afficher les journaux d'événements de stockage

Cliquez sur **Journaux d'événements de stockage** pour obtenir des informations sur toutes les fois où vos données ont dépassé ou atteint 75 % de votre limite sous licence.

Journaux des fonctionnalités(/en-us/netscaler-application-delivery-management-software/media/data-ingestion-history.png)

Examiner la politique de rétention des données

La politique de rétention des données fait référence à un ensemble de règles et de configurations qui déterminent la manière dont NetScaler Console gère et maintient les données historiques au fil du temps. Cette politique décrit la durée de stockage des données avant qu'elles ne soient automatiquement supprimées.

Si vous souhaitez réduire l'espace de stockage utilisé par toutes les différentes fonctionnalités, vous pouvez modifier la durée de conservation des données dans NetScaler Console.

Utilisez la page **Politique de rétention des données** pour modifier les paramètres de stockage des données pour :

- Messages d'événement
- Messages Syslog
- Données de rapport réseau

Pour plus d'informations sur les paramètres de stockage des données, consultez Data Retention Policy.

Notifier en cas de dépassement de la limite de stockage

Vous pouvez configurer des notifications pour que NetScaler Console vous envoie des alertes lorsque votre capacité de stockage de données dépasse les limites spécifiées.

Pour afficher et configurer vos notifications système :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Dans la vignette **Actions**, cliquez sur **Notifier en cas de dépassement de la limite de stockage**.
2. Dans la page **Configurer les notifications système**, sous la **Catégorie d'événements système**, assurez-vous que la catégorie **DataStorageExceeded** est sélectionnée pour recevoir les notifications.

Vous pouvez spécifier divers paramètres liés à la manière et au moment où les notifications vous sont envoyées, à vous ou à d'autres utilisateurs. Sélectionnez la méthode de communication préférée (par exemple, les notifications par e-mail, Slack, PagerDuty et ServiceNow) et définissez les destinataires des notifications.

Pour plus d'informations sur la configuration des profils et l'envoi de notifications, consultez Configure Notifications.

Politique de rétention des données

Pour limiter la quantité de données de rapport stockées dans la base de données de votre serveur NetScaler Console, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont purgées toutes les 24 heures (à 00h00).

Configurer les paramètres de purge du système

Pour configurer les paramètres de purge du système :

1. Accédez à **Paramètres > Stockage des données > Politique de rétention des données**.
2. Dans la page **Purge des données**, cliquez sur **Système**.
3. Dans la page **Système**, saisissez les détails suivants :

    - **Données à conserver (jours)** - Saisissez le nombre de jours pendant lesquels les données doivent être conservées. Vous devez spécifier une valeur comprise entre 1 et 30.
    - **Valeur seuil de purge des données (%)** - Saisissez une limite de seuil (en pourcentage) à définir comme condition pour les processus de purge ou de nettoyage des données. Lorsque les données de la base de données atteignent ce pourcentage spécifié de capacité de stockage, les procédures de purge des données sont déclenchées pour supprimer les données et libérer de l'espace.
    - **Détails de la purge automatique** - Sélectionnez **Activer la purge automatique des données** si vous souhaitez que la purge des données démarre lorsque l'un des critères suivants est rempli :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- La valeur seuil des données spécifiée dans **Valeur seuil de purge des données (%)** est atteinte.
- Le nombre de jours spécifié dans **Données à conserver (jours)** est atteint.

- **Paramètre d'ingestion de données** - Saisissez une limite de seuil (en pourcentage) à définir comme condition pour l'ingestion de données. Lorsque les données de la base de données atteignent ce pourcentage spécifié, l'activité d'ingestion de données est suspendue. Vous devez spécifier une limite comprise entre 50 % et 80 %.

4. Cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configurer les paramètres de purge des événements d'instance

Pour limiter la quantité de données de messages d'événements stockées dans la base de données de votre serveur NetScaler Console, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler Console conserve les données de rapports réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont purgées toutes les 24 heures (à 00h00).

Pour configurer les paramètres de purge des événements d'instance :

1. Accédez à **Paramètres > Stockage des données > Stratégie de rétention des données**.
2. Dans la page **Purge des données**, cliquez sur **Événements d'instance**.
3. Dans le champ **Données à conserver (jours)**, entrez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler Console, puis cliquez sur **Enregistrer**.

Configurer les paramètres de purge des journaux système d'instance

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données syslog génériques sont supprimées de NetScaler Console.

Pour configurer les paramètres de purge des journaux système d'instance :

1. Accédez à **Paramètres > Stockage des données > Stratégie de rétention des données**.
2. Dans la page **Purge des données**, cliquez sur **Événements d'instance**.
3. Dans le champ **Conserver les données génériques Syslog**, spécifiez le nombre de jours entre 1 et 180.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Cliquez sur **Enregistrer**.

Configurer les paramètres de purge des rapports réseau

Pour limiter les données de rapports réseau stockées dans NetScaler Console, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez conserver les données historiques des rapports réseau.

Pour configurer les paramètres de purge des événements d'instance :

1. Accédez à **Paramètres > Stockage des données > Stratégie de rétention des données**.
2. Dans la page **Élagage des données**, cliquez sur **Rapports réseau**.
3. Dans le champ **Données à conserver (jours)**, spécifiez le nombre de jours entre 1 et 30.
4. Cliquez sur **Enregistrer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console en tant que serveur proxy d'API

En plus de pouvoir recevoir des requêtes d'API REST NITRO pour ses propres fonctionnalités de gestion et d'analyse, NetScaler Application Delivery Management (NetScaler Console) peut fonctionner comme un serveur proxy d'API REST pour ses instances gérées. Au lieu d'envoyer des requêtes d'API directement aux instances gérées, les clients d'API REST peuvent envoyer les requêtes d'API à NetScaler Console. NetScaler Console peut différencier les requêtes d'API auxquelles elle doit répondre et celles qu'elle doit transférer inchangées à une instance gérée.

En tant que serveur proxy d'API, NetScaler Console vous offre les avantages suivants :

- **Validation des requêtes d'API**. NetScaler Console valide toutes les requêtes d'API par rapport aux politiques de sécurité et de contrôle d'accès basé sur les rôles (RBAC) configurées. NetScaler Console est également sensible aux locataires et garantit que l'activité d'API ne dépasse pas les limites des locataires.
- **Audit centralisé**. NetScaler Console conserve un journal d'audit de toutes les activités d'API liées à ses instances gérées.
- **Gestion des sessions**. NetScaler Console libère les clients d'API de la tâche de devoir maintenir des sessions avec les instances gérées.

En tant que serveur proxy d'API, NetScaler Console prend en charge la partition d'administration.

Comment NetScaler Console fonctionne en tant que serveur proxy d'API

Lorsque vous souhaitez que NetScaler Console transfère une requête à une instance gérée, vous configurez le client d'API pour qu'il inclue l'un des en-têtes HTTP suivants dans la requête d'API :

VALEURS D'EN-TÊTE	DESCRIPTION
MPS-API-PROXY-MANAGED-INSTANCE-NAME	Nom de l'instance gérée.
MPS-API-PROXY-MANAGED-INSTANCE-IP	Adresse IP de l'instance gérée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VALEURS D'EN-TÊTE	DESCRIPTION
MPS-API-PROXY-MANAGED-INSTANCE-ID	ID de l'instance gérée.
MPS-API-PROXY-TIMEOUT	Valeur de délai d'expiration pour une requête API NITRO. Définissez la valeur de délai d'expiration en secondes. Lorsque vous définissez un délai d'expiration de proxy, NetScaler Console attend la durée spécifiée avant d'expirer la requête.
MPS-API-PROXY-MANAGED-INSTANCE-USERNAME	Nom d'utilisateur pour accéder à l'instance NetScaler gérée.
MPS-API-PROXY-MANAGED-INSTANCE-PASSWORD	Mot de passe pour accéder à l'instance NetScaler gérée.
MPS-API-PROXY-MANAGED-INSTANCE-SESSID	ID de session pour accéder à l'instance gérée.

REMARQUE

Dans **Paramètres > Administration >** Configurations système **> Paramètres de base**, si vous sélectionnez **Demander les informations d'identification pour la connexion à l'instance**, assurez-vous de configurer le nom d'utilisateur et le mot de passe d'une instance gérée. Vous pouvez également spécifier l'ID de session de l'instance.

La présence de l'un de ces en-têtes HTTP aide NetScaler Console à identifier une requête API comme une requête qu'elle doit transmettre à une instance gérée. La valeur de l'en-tête aide NetScaler Console à identifier l'instance gérée à laquelle elle doit transmettre la requête.

Ce flux est représenté dans la figure suivante :



Comme indiqué dans la figure ci-dessus, lorsqu'un de ces en-têtes HTTP apparaît dans une requête, NetScaler Console traite la requête comme suit :

1. Sans modifier la requête, NetScaler Console la transmet au moteur de proxy API de l'instance.
2. Le moteur de proxy API de l'instance transmet la requête API à un validateur et enregistre les détails de la requête API dans le journal d'audit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Le validateur s'assure que la requête ne viole pas les politiques de sécurité configurées, les politiques RBAC, les limites de locataires, etc. Il effectue des vérifications supplémentaires, telles qu'une vérification pour déterminer si l'instance gérée est disponible.

Si la requête API est valide et peut être transmise à l'instance gérée, NetScaler Console identifie une session maintenue par le gestionnaire de session de l'instance, puis envoie la requête à l'instance gérée.

REMARQUE

Assurez-vous que l'option **Demander les informations d'identification pour la connexion à l'instance** est désactivée. Pour ce faire :

1. Accédez à **Paramètres > Administration**.
2. Dans **Configurations système**, sélectionnez **Système, Fuseau horaire, URL autorisées et Message du jour**.

Comment utiliser NetScaler Console comme serveur proxy API

Les exemples suivants montrent des requêtes API REST qu'un client API envoie à un serveur NetScaler Console ayant l'adresse IP 192.0.2.5. NetScaler Console doit transmettre les requêtes, sans modification, à une instance gérée avec l'adresse IP 192.0.2.10. Tous les exemples utilisent l'en-tête MPS-API-PROXY-MANAGED-INSTANCE-IP.

Avant d'envoyer les requêtes API à NetScaler Console, le client API doit :

- Se connecter à NetScaler Console
- Obtenir un ID de session
- Inclure l'ID de session dans les requêtes API ultérieures.

La requête API de connexion est de la forme suivante :

```
POST /nitro/v1/config/login

Content-Type: application/json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    {
        "login": {
            "username":"nsroot",
            "password":"nsroot"
         }
    }
```

NetScaler Console répond à la requête de connexion avec une réponse qui inclut l'ID de session. L'exemple de corps de réponse suivant montre un ID de session :

```
{

  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"resourceName": "nsroot",

"login": [

  {

    "tenant_name": "Owner",

    "permission": "superuser",

    "session_timeout": "36000",

    "challenge_token": "",

    "username": "",

    "login_type": "",

    "challenge": "",

    "client_ip": "",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "client_port": "-1",


      "cert_verified": "false",


      "sessionid":
"##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",


      "token": "b2f3f935e93db6a"
    }


  ]


}
```

Exemple 1 : Récupérer les statistiques du serveur virtuel d'équilibrage de charge

Le client doit envoyer à NetScaler Console une requête API de la forme suivante :

```
GET /nitro/v1/stat/lbvserver

Content-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

Où la valeur de l'en-tête Cookie est l'ID de session renvoyé par l'appel API de connexion. Et la valeur de MPS-API-PROXY-MANAGED-INSTANCE-IP est l'adresse IP du NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exemple 2 : Créer un serveur virtuel d'équilibrage de charge

Le client doit envoyer à NetScaler Console une requête API de la forme suivante :

```
POST /nitro/v1/config/lbvserver/sample_lbvserver

Content-type: application/json

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

     "lbvserver":{

         "name":"sample_lbvserver",

         "servicetype":"HTTP",

         "ipv46":"10.102.1.11",

         "port":"80"

     }

}
```

Exemple 3 : Modifier un serveur virtuel d'équilibrage de charge

Le client doit envoyer à NetScaler Console une requête API de la forme suivante :

```
PUT /nitro/v1/config/lbvserver

Content-type: application/json

Accept-type: application/json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

   "lbvserver":{

        "name":"sample_lbvserver",

        "appflowlog":"DISABLED"

   }

}
```

Exemple 4 : Supprimer un serveur virtuel d'équilibrage de charge

Le client doit envoyer à NetScaler Console une requête API de la forme suivante :

```
DELETE /nitro/v1/config/lbvserver/sample_lbvserver

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

Exemple 5 : Télécharger la configuration CLI en cours d'exécution sur le NetScaler

Le client doit envoyer à NetScaler Console une requête API de la forme suivante :

```
GET /nitro/v1/config/nsrunningconfig

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQ

Cette section fournit la FAQ sur les fonctionnalités suivantes de NetScaler Application Delivery Management (NetScaler Console). Cliquez sur le nom d'une fonctionnalité dans le tableau suivant pour afficher la liste des FAQ pour cette fonctionnalité.

ANALYTIQUE	AUTHENTIFICATION	GESTION DE LA CONFIGURATION
Gestion des certificats	Déploiement	Déploiement (Reprise après sinistre)
Gestion des événements	Gestion des instances	StyleBooks
Gestion du système		

Analytique

Est-il nécessaire d'activer le canal virtuel EUEM sur les instances NetScaler Gateway déployées en mode à saut unique ?

Les données du canal virtuel EUEM font partie des données HDX Insight que NetScaler Console reçoit des instances Gateway. Le canal virtuel EUEM fournit les données concernant l'ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur NetScaler Console.

Le canal virtuel EUEM est un service par défaut exécuté sur les applications Citrix Virtual Desktop (VDA). S'il n'est pas en cours d'exécution, démarrez le processus « Citrix End User Experience Monitoring » dans les services VDA.

Comment activer NetScaler Console pour surveiller le trafic des applications web et des bureaux virtuels ?

1. Accédez à **Infrastructure** \> **Instances** \> **NetScaler**, et sélectionnez l'instance NetScaler sur laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Dans la page **Configurer l'analyse**, sélectionnez tous les serveurs virtuels sur lesquels vous souhaitez activer l'analyse, puis cliquez sur **Activer AppFlow**. Pour plus de détails, consultez Comment activer l'analyse sur les instances.

REMARQUE :

Pour les instances NetScaler de la version 11.0, build 65.30 et ultérieure, il n'y a pas d'option sur NetScaler Console pour activer explicitement Security Insight. Assurez-vous de configurer les paramètres AppFlow sur les instances NetScaler, afin que NetScaler Console commence à recevoir le trafic Security Insight ainsi que le trafic Web Insight. Pour plus d'informations sur la façon de définir les paramètres AppFlow sur les instances NetScaler, consultez Pour définir les paramètres AppFlow à l'aide de l'utilitaire de configuration.

Après avoir ajouté les instances NetScaler, NetScaler Console commence-t-il automatiquement à collecter des informations analytiques ?

Non. Activez l'analyse sur les serveurs virtuels hébergés dans les instances NetScaler gérées par NetScaler Console. Pour plus de détails, consultez Comment activer l'analyse sur les instances.

Est-il nécessaire d'accéder à l'appliance NetScaler individuelle pour activer l'analyse ?

Non. Toutes les configurations sont effectuées à partir de l'interface utilisateur de NetScaler Console, qui répertorie les serveurs virtuels hébergés sur l'instance NetScaler spécifique. Pour plus de détails, consultez Comment activer l'analyse sur les instances.

Quels sont les types de serveurs virtuels qui peuvent être répertoriés sur une instance NetScaler pour activer l'analyse ?

Actuellement, l'interface utilisateur de NetScaler Console répertorie les serveurs virtuels suivants pour l'activation de l'analyse :

- Serveur virtuel d'équilibrage de charge
- Serveur virtuel de commutation de contenu
- Serveur virtuel VPN
- Serveur virtuel de redirection de cache

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment attacher un disque supplémentaire à NetScaler Console ?

Pour attacher un disque supplémentaire à NetScaler Console :

1. Arrêtez la machine virtuelle NetScaler Console.
2. Dans l'hyperviseur, attachez un disque supplémentaire de la taille requise à la machine virtuelle NetScaler Console.

   Par exemple, considérons que vous souhaitez augmenter l'espace disque à 200 Go, sur une machine virtuelle NetScaler Console de 120 Go. Dans ce scénario, vous devez attacher un espace disque de 200 Go au lieu de 80 Go. Le nouvel espace disque de 200 Go sera utilisé pour stocker les données de la base de données et les fichiers journaux de NetScaler Console. L'espace disque existant de 120 Go est utilisé pour stocker les fichiers principaux, les fichiers journaux du système d'exploitation, etc.
3. Démarrez la machine virtuelle NetScaler Console.

Que signifie « les collecteurs ne sont pas configurés sur les instances NetScaler » ?

Un collecteur reçoit les enregistrements AppFlow générés par l'appliance NetScaler.

NetScaler Console reçoit le trafic Security Insight et Web Insight des instances NetScaler lorsque la fonctionnalité AppFlow est activée. Lorsque vous activez la fonctionnalité AppFlow sur une instance NetScaler, vous devez spécifier au moins un collecteur auquel les enregistrements AppFlow sont envoyés. Si les collecteurs ne sont pas configurés sur les instances NetScaler, NetScaler Console ne reçoit pas le trafic des instances.

Par exemple, cinq instances NetScaler sont ajoutées à NetScaler Console. Si les collecteurs ne sont pas spécifiés pour deux instances, aucun trafic ne transite vers NetScaler Console. Les diagnostics en libre-service détectent le problème et l'affichent comme « Les collecteurs ne sont pas configurés sur 2 instances. »

Pour plus d'informations sur la configuration de la fonctionnalité AppFlow, consultez Configuration de la fonctionnalité AppFlow.

À quoi sert l'activation des mesures côté client ?

Avec les mesures côté client activées, NetScaler Console capture les métriques de temps de chargement et de temps de rendu pour les pages HTML, via l'injection HTML. À l'aide de ces métriques, les administrateurs peuvent identifier les problèmes de latence L7.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentification

Qu'est-ce que l'équilibrage de charge des requêtes d'authentification ?

La fonctionnalité d'équilibrage de charge des serveurs d'authentification permet à NetScaler Console d'équilibrer la charge des requêtes d'authentification dirigées vers les serveurs d'authentification externes. L'équilibrage de charge des serveurs d'authentification garantit que la charge d'authentification est répartie sur plusieurs serveurs d'authentification, évitant ainsi qu'un serveur d'authentification ne soit surchargé. Vous pouvez créer un service d'authentification pour vous connecter et obtenir des informations utilisateur à partir de votre serveur d'authentification externe existant en utilisant des protocoles d'authentification tels que LDAP, RADIUS ou TACACS.

Pourquoi devons-nous cascader les serveurs d'authentification externes ?

Les serveurs d'authentification externes en cascade assurent un traitement d'authentification ininterrompu, permettant l'accès aux utilisateurs légitimes si un serveur d'authentification tombe en panne. Il n'y a aucune limitation quant aux types de serveurs d'authentification que vous pouvez cascader. Vous pouvez avoir tous des serveurs RADIUS, ou tous des serveurs LDAP, ou une combinaison de serveurs RADIUS et LDAP.

Combien de serveurs d'authentification externes puis-je cascader ?

Vous pouvez cascader jusqu'à 32 serveurs d'authentification externes dans NetScaler Console.

Ai-je une alternative lorsque l'authentification externe échoue ?

Il peut arriver que l'authentification externe échoue complètement, même si vous avez mis en cascade plusieurs serveurs. Par exemple, les serveurs externes peuvent devenir inaccessibles, ou les identifiants d'un nouvel utilisateur peuvent ne pas avoir été saisis dans l'un des serveurs d'authentification externes. Pour éviter de bloquer les utilisateurs dans une telle situation, vous pouvez activer l'authentification locale de secours. Pour plus de détails, consultez Authentification locale de secours.

Qu'est-ce que l'authentification locale de secours ?

L'authentification locale de secours est une option permettant d'authentifier vos utilisateurs localement lorsque l'authentification externe échoue. Si l'authentification externe échoue,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console accède à la base de données des utilisateurs locaux pour authentifier vos utilisateurs.

Dans NetScaler Console, accédez à **Paramètres > Authentification > Configuration de l'authentification**. Sur cette page, vous pouvez ajouter plusieurs serveurs d'authentification externes en cascade et sélectionner l'option **Activer l'authentification locale de secours**.

Qu'est-ce qu'une extraction de groupes d'utilisateurs externes ?

Si vous avez ajouté des serveurs externes pour authentifier les utilisateurs, vous pouvez importer (extraire) des groupes d'utilisateurs existants dans NetScaler Console. Vous devez importer les groupes d'utilisateurs une seule fois et attribuer une autorisation de groupe à un groupe d'utilisateurs plutôt que d'importer des utilisateurs individuels et de leur donner des autorisations individuelles. Vous n'avez pas besoin de recréer les utilisateurs sur NetScaler Console.

Pourquoi devons-nous attribuer des autorisations de groupe ?

Lorsque vous utilisez la fonctionnalité d'équilibrage de charge de NetScaler, vous pouvez intégrer NetScaler Console à des serveurs d'authentification externes et importer des informations de groupe d'utilisateurs à partir de ces serveurs. Connectez-vous à NetScaler Console et créez manuellement les mêmes informations de groupe dans NetScaler Console, puis attribuez des autorisations à ces groupes. Les autorisations des utilisateurs et des groupes d'utilisateurs sont gérées dans NetScaler Console et non sur le serveur externe. Les utilisateurs disposent de différentes autorisations d'accès basées sur les rôles sur les serveurs externes. Configurez les mêmes autorisations pour les utilisateurs dans NetScaler Console. Au lieu de configurer les autorisations individuellement pour chaque utilisateur, vous pouvez configurer une autorisation au niveau du groupe afin que les membres du groupe d'utilisateurs puissent accéder à des services spécifiques sur les serveurs virtuels à charge équilibrée. Les autorisations typiques que vous pouvez attribuer sont des autorisations de gestion des instances NetScaler, des instances NetScaler SDX, des serveurs virtuels, etc., afin que les utilisateurs de ce groupe puissent gérer uniquement ces instances ou serveurs virtuels. Vous pouvez ultérieurement modifier les autorisations accordées aux utilisateurs au niveau du groupe. Vous pouvez même supprimer un ou plusieurs groupes d'utilisateurs ; les utilisateurs des autres groupes continueront de fonctionner sur NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion de la configuration

Puis-je effectuer une configuration sur plusieurs instances NetScaler simultanément à l'aide de NetScaler Console ?

Oui, vous pouvez utiliser des tâches de configuration pour effectuer une configuration sur plusieurs instances NetScaler.

Que sont les tâches de configuration sur NetScaler Console ?

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une ou plusieurs instances gérées. Vous pouvez créer des tâches pour apporter des modifications de configuration à travers les instances, répliquer des configurations sur plusieurs instances de votre réseau, et enregistrer et rejouer des tâches de configuration à l'aide de l'interface graphique de NetScaler Console. Vous pouvez également convertir les tâches enregistrées en commandes CLI.

Vous pouvez utiliser la fonctionnalité Tâches de configuration de NetScaler Console pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

Puis-je planifier des tâches à l'aide de modèles intégrés dans NetScaler Console ?

Oui ! Vous pouvez planifier une tâche en utilisant l'option de modèle intégré. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégré pour planifier une tâche de configuration de serveurs syslog. Vous pouvez choisir d'exécuter la tâche immédiatement ou de la planifier pour une exécution ultérieure.

Vous pouvez enregistrer la configuration d'une tâche précédemment créée et l'exécuter à nouveau après avoir modifié les commandes, les paramètres, la source de configuration et les instances ciblées. Ceci est utile lorsque le même ensemble de commandes doit être exécuté sur une instance différente, ou lorsque la tâche rencontre une erreur et arrête son exécution.

Gestion des certificats

La suppression des certificats SSL de NetScaler Console entraîne-t-elle la suppression des certificats des instances NetScaler ?

Non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Déploiement

Quel est le nom d'utilisateur et le mot de passe par défaut ?

- Après avoir terminé la configuration réseau initiale, vous pouvez vous connecter à NetScaler Console depuis l'hyperviseur ou la console SSH, en utilisant le nom d'utilisateur et le mot de passe par défaut (nsrecover/nsroot).
- Le nom d'utilisateur et le mot de passe par défaut pour se connecter depuis l'interface graphique sont *nsroot/nsroot*.

Comment changer le mot de passe par défaut ?

REMARQUE :

À partir de la version 14.1-8x, après vous être connecté pour la première fois à l'interface graphique ou à l'API de NetScaler Console avec les informations d'identification par défaut, vous êtes invité à modifier le mot de passe par défaut.

Pour changer le mot de passe :

1. Dans NetScaler Console, accédez à **Paramètres > Administration des utilisateurs > Utilisateurs**.

   La page **Utilisateurs** s'affiche.
2. Sélectionnez le nom d'utilisateur **nsroot** et cliquez sur **Modifier**.

   

   La page **Configurer l'utilisateur système** s'affiche.
3. Sélectionnez **Changer le mot de passe** et créez un mot de passe de votre choix.

   
4. Cliquez sur **OK**.

   Vous pouvez maintenant utiliser le nouveau mot de passe pour vous connecter depuis l'interface graphique, l'hyperviseur ou la console SSH.

   REMARQUE :

   Vous ne pouvez pas modifier le nom d'utilisateur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment réinitialiser le mot de passe ?

Vous pouvez consulter cette documentation pour réinitialiser le mot de passe.

Dans une paire HA, si le mot de passe est modifié sur le nœud principal et si l'option « Rompre la paire HA » est sélectionnée ultérieurement, quel est le comportement ?

Vous pouvez vous connecter aux deux nœuds autonomes à l'aide de votre nouveau mot de passe.

Si deux serveurs autonomes ont des mots de passe différents, quel est l'impact lors du déploiement de ces deux serveurs en paire HA ?

Il est recommandé d'avoir un mot de passe par défaut pour les deux serveurs lorsque vous déployez deux serveurs autonomes en paire HA.

La configuration HA est terminée, mais l'interface graphique du nœud principal n'est pas accessible. Quelle peut en être la raison ?

La prise en compte de la configuration prend quelques minutes. Vous pouvez essayer d'y accéder à nouveau après quelques minutes.

La configuration HA est terminée, mais l'interface graphique de l'adresse IP flottante n'est pas accessible. Quelle peut en être la raison ?

Après la configuration HA, vous devez d'abord accéder à l'interface graphique du nœud principal et terminer le déploiement. Pour plus d'informations, consultez Déployer le nœud principal et secondaire en tant que paire haute disponibilité. Une fois le déploiement terminé, le serveur redémarre et est prêt pour le déploiement en haute disponibilité. Vous pouvez ensuite accéder à l'interface graphique de l'adresse IP flottante.

Quelle base de données est prise en charge dans NetScaler Console autonome et NetScaler Console HA ?

NetScaler Console autonome et NetScaler Console HA prennent tous deux en charge PostgreSQL.

Quelle est la perte de données potentielle pour le nœud secondaire ?

Le nœud secondaire écoute les messages de pulsation que le nœud principal envoie via la base de données NetScaler Console. Si le nœud secondaire ne reçoit pas les pulsations pendant plus

© 1997–2026 Citrix Systems, Inc. All rights reserved.

de 180 secondes, il effectue une vérification SSH sur le nœud principal. Si la pulsation et la vérification SSH échouent, le nœud principal est considéré comme étant hors service.

Dans ce scénario, le nœud secondaire prend le relais en tant que nœud principal et le délai de 180 secondes peut être considéré comme la perte de données possible pour le nœud secondaire.

Que se passe-t-il si le nœud principal est hors service ?

Le nœud secondaire prend le relais et devient le nœud principal.

Comment réinstaller le nœud défaillant ?

Il est recommandé d'installer une nouvelle machine virtuelle. Pour réinstaller :

1. Rompez la paire HA. Accédez à **Paramètres > Déploiement**

   La page de déploiement s'affiche. Cliquez sur **Rompre HA**
2. Supprimez le nœud défaillant de l'hyperviseur.
3. Importez le fichier image .XVA dans l'hyperviseur.
4. Depuis l'onglet Console, configurez NetScaler Console avec les configurations réseau initiales. Pour plus d'informations, consultez Enregistrer et déployer le premier serveur (nœud principal) et Enregistrer et déployer le deuxième serveur (nœud secondaire).
5. Redéployer la paire HA.

NetScaler Console prend-il en charge le stockage SAN ?

Nous vous recommandons d'héberger le VHD de NetScaler Console sur un stockage local. Lorsqu'il est hébergé sur des périphériques de stockage dans un SAN, NetScaler Console peut ne pas fonctionner comme prévu. Par conséquent, le déploiement de NetScaler Console sur SAN n'est pas pris en charge.

NetScaler Console prend-il en charge un disque supplémentaire ?

Oui. Une nouvelle installation d'une paire HA NetScaler Console alloue 120 Go de stockage par défaut. Pour plus de 120 Go de stockage, vous pouvez ajouter un disque supplémentaire pour un maximum de 3 To de stockage. L'ajout de plus d'un disque supplémentaire n'est pas pris en charge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir désactivé la paire HA, qu'advient-il de l'adresse IP flottante configurée ?

L'adresse IP flottante n'est plus accessible et vous devez redéployer la paire haute disponibilité.

Puis-je attribuer une adresse IP flottante différente lors du redéploiement ?

Oui. Vous pouvez configurer une nouvelle adresse IP flottante.

Pourquoi l'interface graphique du nœud secondaire n'est-elle pas accessible ?

Le nœud secondaire est uniquement un serveur de réplication en lecture et agit comme un nœud principal uniquement si le nœud principal est en panne pour une raison quelconque. Nous recommandons d'accéder soit à l'interface graphique du nœud principal, soit à l'interface graphique de l'adresse IP flottante.

Si le nœud principal est en panne pendant une longue période, les configurations peuvent-elles toujours être effectuées à l'aide de l'interface graphique de l'adresse IP flottante ?

Oui. Vous pouvez toujours continuer à effectuer des configurations et les configurations sont enregistrées dans le nœud secondaire. Une fois le nœud principal de retour, toutes les configurations sont synchronisées.

S'il est nécessaire de modifier l'adresse IP du nœud principal, l'adresse IP du nœud secondaire ou l'adresse IP flottante à l'avenir (par exemple, en la remplaçant par IPv6), quelles sont les solutions recommandées à suivre ?

La modification des adresses IP dans une paire HA n'est pas prise en charge sans rompre la paire HA.

Pour mettre à jour l'adresse IP du nœud principal ou du nœud secondaire :

1. Rompez la paire HA. Accédez à **Paramètres > Déploiement**.

   La page Déploiement s'affiche. Cliquez sur **Rompre HA**

   a. Connectez-vous au nœud principal à l'aide d'un client SSH ou depuis l'hyperviseur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Utilisez `nsrecover` comme nom d'utilisateur et saisissez le mot de passe que vous avez défini.

c. Saisissez **networkconfig**. Suivez la procédure à partir de l'**étape 3** disponible dans Enregistrer et déployer le premier serveur (nœud principal).

   Lors de la configuration réseau initiale, vous pouvez fournir une adresse IP différente.

d. Effectuez la même procédure pour le nœud secondaire et poursuivez la procédure à partir de l'**étape 3** disponible dans Enregistrer et déployer le deuxième serveur (nœud secondaire).

Pour mettre à jour l'adresse IP flottante :

1. Accédez à **Paramètres > Déploiement**.

   La page Déploiement s'affiche.

   a. Cliquez sur **Paramètres HA**.

   b. Cliquez sur **Configurer l'adresse IP flottante pour le mode haute disponibilité**.

   c. Saisissez l'adresse IP flottante et cliquez sur **OK**.

NetScaler Console prend-il en charge les processeurs AMD ?

Le processeur AMD est pris en charge dans :

- **NetScaler Console 13.1 build 4.43 ou version ultérieure**.
- **Agent NetScaler 13.1 build 17.42 ou version ultérieure**.

Déploiement (reprise après sinistre)

À quelle fréquence la réplication a-t-elle lieu entre le site principal et le site de reprise après sinistre ?

La réplication entre le site principal et le site de reprise après sinistre est en temps réel.

Après avoir initié le script de sauvegarde sur le site de reprise après sinistre, le site de reprise après sinistre devient-il le site principal temporaire, jusqu'à ce que le site principal soit récupéré et entièrement opérationnel ?

Non. Le site de reprise après sinistre deviendra désormais le site principal. Pour rétablir la paire HA en tant que site principal, consultez Rétablir les configurations sur le site principal d'origine

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si l'option Rompre la paire HA est sélectionnée, les deux nœuds fonctionnent comme un serveur autonome. Étant donné que la prise en charge de la reprise après sinistre n'est pas applicable pour un serveur autonome, qu'advient-il du site de reprise après sinistre si l'option Rompre la paire HA est sélectionnée ?

Si vous sélectionnez l'option Rompre la paire HA, la réplication entre le site principal et le site de reprise après sinistre est interrompue. Vous devez reconfigurer le site de reprise après sinistre dans le cadre du redéploiement de la paire HA.

Gestion des événements

Comment puis-je suivre tous les événements générés sur mes instances NetScaler gérées à l'aide de NetScaler Console ?

En tant qu'administrateur réseau, vous pouvez afficher des détails tels que les modifications de configuration, les conditions de connexion, les pannes matérielles, les violations de seuil et les modifications d'état d'entité sur vos instances NetScaler, ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements de NetScaler Console pour afficher les rapports générés pour les détails de gravité des événements critiques sur toutes vos instances NetScaler.

Que sont les règles d'événement ?

À l'aide de NetScaler Console, vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles d'événement facilitent la surveillance de nombreux événements générés dans votre infrastructure NetScaler Console.

Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en attribuant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée.

Les conditions pour lesquelles vous pouvez créer des filtres sont la gravité, les instances NetScaler, la catégorie et les objets de défaillance. Les actions que vous pouvez attribuer aux événements sont l'envoi d'une notification par e-mail, le transfert de traps SNMP des instances NetScaler gérées vers la NetScaler Console et l'envoi d'une notification par SMS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion des instances

Que se passe-t-il si une instance NetScaler ne peut pas se connecter à NetScaler Console après l'allocation de bande passante lorsque vous utilisez la licence de capacité groupée NetScaler ?

Si le battement de cœur entre l'instance NetScaler et NetScaler Console échoue, l'instance entre dans une période de grâce de 30 jours. Une fois la communication rétablie, la licence de capacité mutualisée commence à fonctionner. Pendant la période de grâce, les fonctions NetScaler ne sont pas affectées. Après 30 jours de période de grâce, l'instance NetScaler initie un redémarrage à chaud et n'est plus sous licence.

Que sont les centres de données dans NetScaler Console ?

Un centre de données NetScaler Console est un regroupement logique des instances NetScaler dans un emplacement géographique spécifique. Chaque serveur peut surveiller et gérer plusieurs instances NetScaler au sein d'un centre de données. Vous pouvez utiliser le serveur NetScaler Console pour gérer des données telles que les journaux système (syslog), le flux de trafic applicatif et les traps SNMP des instances gérées. Pour plus de détails sur la configuration des centres de données, consultez la section Comment configurer les centres de données pour les géocartes dans NetScaler Console.

Quels sont les différents dispositifs NetScaler pris en charge par NetScaler Console ?

Les instances sont les dispositifs NetScaler ou les dispositifs virtuels que vous souhaitez découvrir, gérer et surveiller depuis NetScaler Console. Vous devez ajouter ces instances au serveur NetScaler Console. Vous pouvez ajouter les dispositifs NetScaler et les dispositifs virtuels suivants à NetScaler Console :

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler Console ou ultérieurement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Qu'est-ce qu'un profil d'instance ?

Un profil d'instance est utilisé par NetScaler Console pour accéder à une instance.

Un profil d'instance contient le nom d'utilisateur et le mot de passe pour l'accès à une ou plusieurs instances. Un profil par défaut est disponible pour chaque type d'instance. Par exemple, le profil ns-root-profile est le profil par défaut pour les instances NetScaler. Il contient les informations d'identification de l'administrateur NetScaler par défaut. Lorsque vous modifiez les informations d'identification requises pour l'accès aux instances, vous pouvez définir des profils d'instance personnalisés pour ces instances.

Puis-je redécouvrir plusieurs instances NetScaler VPX dans NetScaler Console ?

Oui, vous pouvez redécouvrir plusieurs instances Citrix **VPX** dans NetScaler Console pour connaître les derniers états et configurations des instances.

Accédez à **Infrastructure > Instances > NetScaler > VPX**, sélectionnez les instances que vous souhaitez redécouvrir, puis dans la liste **Action**, cliquez sur **Redécouvrir**. Pour plus d'informations, consultez Comment redécouvrir plusieurs instances VPX.

NetScaler Console peut-il être installé sur NetScaler SDX ?

Non

Puis-je ajouter une instance NetScaler au logiciel NetScaler Console en utilisant une adresse IP publique ?

Oui, vous pouvez le faire en utilisant la traduction d'adresses réseau (NAT).

- Pour ajouter une seule instance : utilisez l'adresse IP NAT de l'adresse IP publique de l'instance NetScaler.
- Pour ajouter une paire HA NetScaler : ajoutez les adresses IP NAT de la paire HA dans ce format :

  `<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`
- Pour ajouter un cluster NetScaler : ajoutez toutes les adresses IP publiques NAT de toutes les instances du cluster, chacune séparée par une virgule, et ajoutez l'adresse IP NAT de l'adresse IP du CLUSTER entre parenthèses. Exemple de format : NAT1, NAT2, NAT3,(NATIP of CLUSTERIP).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour plus d'informations, consultez les rubriques suivantes :

- Ajouter des instances à NetScaler Console
- Configuration de la traduction d'adresses réseau

Comment enregistrer un nœud de reprise après sinistre si les informations d'identification du nœud DR sont modifiées ?

Réinitialisez les informations d'identification du nœud de reprise après sinistre (DR) sur `nsrecover` / `nsroot` à l'aide de la commande suivante :

```
./mps/change_freebsd_password.sh <username> <password>
```

Pour enregistrer un nœud DR, suivez les étapes de Déployer et enregistrer le nœud DR de NetScaler Console à l'aide de la console DR.

StyleBooks

Les StyleBooks peuvent-ils être utilisés pour configurer différentes instances NetScaler exécutant différentes versions du logiciel NetScaler ?

Oui, vous pouvez utiliser les StyleBooks pour configurer différentes instances NetScaler exécutant différentes versions s'il n'y a pas de divergence entre les commandes des différentes versions.

Lorsqu'un StyleBook est utilisé pour configurer plusieurs instances NetScaler simultanément, et que la configuration d'une instance NetScaler échoue, que se passe-t-il ?

Si l'application de la configuration à une instance NetScaler échoue, la configuration n'est plus appliquée à d'autres instances, et les configurations déjà appliquées sont annulées.

Les sauvegardes NetScaler effectuées via NetScaler incluent-elles les configurations appliquées via les StyleBooks ?

Oui

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gestion du système

Puis-je attribuer un nom d'hôte à mon serveur NetScaler Console ?

Oui, vous pouvez attribuer un nom d'hôte pour identifier votre serveur NetScaler Console. Pour attribuer un nom d'hôte, accédez à **Système**\> **Administration du système** \> **Paramètres système**, puis cliquez sur **Modifier le nom d'hôte**.

Le nom d'hôte est affiché sur la licence universelle de NetScaler Console. Pour plus d'informations, consultez Comment attribuer un nom d'hôte à un serveur NetScaler Console.

Puis-je sauvegarder et restaurer ma configuration NetScaler Console ?

Oui, vous pouvez sauvegarder les fichiers de configuration (fichiers NTP et certificats SSL), les données système, les données d'infrastructure et d'application, ainsi que tous vos paramètres **SNMP**. Si votre NetScaler Console devient instable, vous pouvez utiliser les fichiers sauvegardés pour restaurer votre NetScaler Console à un état stable.

Pour sauvegarder et restaurer votre configuration NetScaler Console, accédez à **Système** > **Paramètres avancés** > **Fichiers de sauvegarde**, puis cliquez sur **Sauvegarder** ou **Restaurer** selon le cas. Pour plus d'informations, consultez Comment sauvegarder et restaurer la configuration sur NetScaler Console.

Nous vous recommandons d'utiliser cette fonctionnalité avant d'effectuer une mise à niveau ou par mesure de précaution.

Que sont les seuils et les alertes sur NetScaler Console ?

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance NetScaler et surveiller les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, NetScaler Console génère une alerte pour signaler un problème lié aux performances. Lorsque la valeur du compteur revient à la valeur claire spécifiée dans le seuil, l'événement est effacé.

Puis-je générer un fichier de support technique pour NetScaler Console ?

Oui. Nous vous recommandons de générer une archive des données et des statistiques de NetScaler Console avant de contacter le support technique pour déboguer un problème. L'archive est un fichier TAR que vous pouvez envoyer à l'équipe de support technique.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez générer un fichier de support technique qui contient des journaux de débogage, la durée pendant laquelle les journaux de débogage ont été collectés, ainsi que des journaux distincts et divers provenant de la base de données NetScaler Console.

Pour configurer et envoyer un fichier de support technique, accédez à **Système** \> **Diagnostics** \> **Support technique**, puis cliquez sur **Générer un fichier de support technique**. Pour plus d'informations, consultez Comment générer un fichier de support technique pour NetScaler Console.

Qu'est-ce que la purge de syslog ?

Syslog est un protocole standard pour la journalisation. Syslog permet d'isoler le système qui génère les informations et le système qui les stocke. Vous pouvez consolider les informations de journalisation et en tirer des enseignements à partir des données collectées. Vous pouvez également configurer syslog pour enregistrer différents types d'événements.

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels toutes les données Syslog génériques, les données AppFirewall et les données NetScaler Gateway seront supprimées de NetScaler Console.

Puis-je configurer un serveur NTP sur NetScaler Console ?

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans NetScaler Console pour synchroniser l'horloge de NetScaler Console avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge de NetScaler Console a les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

Pour configurer un serveur NTP, accédez à **Système** \> **Serveurs NTP**, puis cliquez sur **Ajouter**. Pour plus d'informations, consultez Comment configurer un serveur NTP sur NetScaler Console.

À partir de quelle version le déploiement HA actif-passif de NetScaler Console est-il pris en charge ?

Le mode de déploiement HA actif-passif de NetScaler Console est pris en charge à partir de la version 12.0 build 51.24 de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

J'avais une configuration HA actif-actif de NetScaler Console et j'avais configuré une appliance NetScaler avec un serveur virtuel d'équilibrage de charge dessus pour un accès GUI unifié. Comment mettre à jour cette configuration ?

Après la mise à niveau de la paire HA NetScaler Console en mode actif-passif, vous devez exécuter la commande suivante sur l'appliance NetScaler pour mettre à jour la configuration d'équilibrage de charge :

Ajouter un moniteur d'équilibrage de charge MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\\r\\nAccept-Encoding: identity\\r\\nUser-Agent: NetScaler-Monitor\\r\\nConnection: close\\r\\n\\r\\n\\"" -recv "{\\"statuscode\\":0, \\"is_passive\\":0}" -LRTM DISABLED**

Puis-je configurer l'équilibrage de charge de la paire HA NetScaler Console sur une instance NetScaler en utilisant le port 443 ?

Non, vous ne pouvez pas configurer l'équilibrage de charge de la paire HA NetScaler Console sur une instance NetScaler en utilisant le port 443.

Lorsque vous configurez les moniteurs `http-ecv` et `https-ecv` sur NetScaler, il ne surveille pas correctement les nœuds HA de NetScaler Console.

Un fichier de sauvegarde de serveur NetScaler Console peut-il être utilisé pour restaurer la configuration d'un autre serveur NetScaler Console ?

Oui

Après que NetScaler Console a sauvegardé une instance NetScaler, ce fichier de sauvegarde peut-il être utilisé pour restaurer la configuration d'une autre instance NetScaler via NetScaler Console ?

Oui. Téléchargez le fichier de sauvegarde de NetScaler Console, téléchargez-le dans le référentiel de sauvegarde d'une autre instance NetScaler, et restaurez cette instance. Assurez-vous que les informations réseau et d'authentification ne sont pas en conflit. Par exemple, vérifiez les conflits d'adresses IP ou de ports, les profils de mot de passe non concordants. Assurez-vous également que l'instance VPX restaurée possède la même adresse NSIP et la même licence NetScaler que celle qui a été sauvegardée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Avant de restaurer une instance dans une paire haute disponibilité, assurez-vous que les adresses IP et l'état (principal ou secondaire) stockés dans le fichier de sauvegarde correspondent à ceux de la configuration HA d'origine. Vérifiez également que le nouveau principal et le nouveau secondaire ont le même type de licence NetScaler.

Pouvons-nous forcer NetScaler Console à utiliser une adresse SNIP pour communiquer avec les instances NetScaler, au lieu d'utiliser l'adresse NSIP du serveur NetScaler Console ?

Oui, vous pouvez ajouter une adresse SNIP (avec gestion activée) dans NetScaler Console pour la communication avec les instances NetScaler.

Lorsque je sauvegarde des instances NetScaler dans NetScaler Console, le résultat est-il une sauvegarde complète ou une sauvegarde de base ?

Les sauvegardes des instances NetScaler par NetScaler Console sont des sauvegardes complètes.

Existe-t-il un guide de dépannage pour NetScaler Console ?

Oui. Voir `<https://support.citrix.com/article/CTX224502>`.

Comment les instances NetScaler sont-elles gérées lorsqu'un basculement HA de NetScaler Console se produit ?

Si la vérification basée sur le heartbeat et SSH échoue, le nœud principal est considéré comme hors service et le nœud secondaire prend le relais en tant que nœud principal. Toutes les instances NetScaler sont mises à jour avec les détails du dernier nœud principal comme destination de leur trap SNMP par défaut.

Le nouveau nœud principal (actif) de NetScaler Console vérifie si le nœud précédemment actif était configuré comme collecteur AppFlow ou serveur syslog ; si c'était le cas, le nouveau nœud principal ajoute les détails du collecteur AppFlow ou du serveur syslog aux informations envoyées aux instances.

Pour syslog, il remplace les détails de l'ancien serveur.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Que se passe-t-il lorsque le nœud HA de NetScaler Console qui est tombé en panne redémarre ?

Après son retour en service, le nœud NetScaler Console reste passif à moins que le nœud actif ne bascule.

Comment les instances NetScaler sont-elles distribuées entre les nœuds HA de NetScaler Console ?

Toutes les instances NetScaler sont gérées par le nœud principal de NetScaler Console.

Comment les licences de serveur virtuel sont-elles gérées en cas de basculement HA de NetScaler Console ?

Si le nœud principal de NetScaler Console sur lequel les licences de serveur virtuel sont appliquées tombe en panne, le nouveau nœud principal gère les licences de serveur virtuel pendant une période de grâce de 30 jours. Réappliquez les licences sur le nouveau nœud principal avant la fin de la période de grâce. Pour des alternatives, contactez le support NetScaler.

Un équilibreur de charge est-il obligatoire pour une configuration HA de NetScaler Console ?

Non, mais s'il n'y a pas d'équilibreur de charge, les nœuds NetScaler Console doivent être accessibles via leurs propres adresses IP. Le nœud passif est marqué avec l'étiquette « Passive », et nous recommandons de ne créer aucune configuration sur le nœud passif.

Nœud passif(/en-us/netscaler-application-delivery-management-software/media/netscaler-mas-faq.png)

NetScaler Console prend-il en charge une base de données externe ?

Non

Une instance NetScaler gérée par NetScaler Console peut-elle être utilisée comme équilibreur de charge pour NetScaler Console HA ?

Oui

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quelles données sont synchronisées entre les nœuds HA de NetScaler Console ?

La base de données complète de NetScaler Console est synchronisée, et les dossiers suivants sont synchronisés :

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- Configurer les seuils adaptatifs
- Configurer la synthèse de base de données
- Configurer la gestion des SLA
- Créer des seuils et des alertes
- Désactiver la collecte de données d'URL
- Présentation de Logstream
- Tableaux de bord
- Toutes les violations
- Vue d'ensemble de l'application
- Détails de la violation réseau
- SSL Insight
- Résoudre les problèmes de Web Insight
- Afficher les analyses pour les transactions web
- Procédures détaillées pour configurer une topologie à deux niveaux ou de maillage de services léger
- Procédures détaillées pour configurer la topologie de maillage de services
- Gouvernance des données (pour NetScaler Console entre les versions 14.1-8.x et 14.1-21.x)
- Gouvernance des données (pour NetScaler ADM 14.1-4.42 ou versions antérieures)
- Données de télémétrie facultatives pour Cloud Connect
- Données de télémétrie facultatives pour le programme de télémétrie NetScaler®
- Données de télémétrie requises pour Cloud Connect
- Données de télémétrie requises pour le programme de télémétrie NetScaler®
- Licences
- Sauvegarder et restaurer une configuration NetScaler Console dans une paire HA
- Configurer les paramètres de notification système
- Configurer les sites pour les géocartes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer les seuils adaptatifs

La fonctionnalité de seuil adaptatif définit la valeur de seuil pour le nombre maximal de requêtes sur chaque URL. Si le nombre maximal de requêtes sur une URL est supérieur à la valeur de seuil définie pour cette URL, un message syslog est envoyé à un serveur syslog externe. L'intervalle de la valeur de seuil peut être en jours ou en semaines.

La valeur de seuil est calculée comme suit :

Valeur de seuil = **Nombre maximal de requêtes * Multiplicateur de seuil**

Où :

- Le nombre maximal de requêtes est le nombre maximal de requêtes sur une URL.
- Le multiplicateur de seuil est une valeur entière que vous définissez (par défaut : 2).

Pour créer un seuil adaptatif à l'aide de NetScaler Console

1. Accédez à **Système** \> **Paramètres d'analyse** \> **Seuils adaptatifs**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils adaptatifs**, spécifiez les paramètres suivants :
    - **Nom** - Nom du seuil
    - **Entité** - URL
    - **Durée** - Durée du seuil (jour ou semaine)
    - **Multiplicateur de seuil** - Un entier défini par l'utilisateur qui est multiplié par le nombre maximal de requêtes de l'URL spécifiée pour obtenir le seuil adaptatif de l'URL.

Configurer la synthèse de base de données

La configuration de la synthèse de base de données dans NetScaler Console vous permet de personnaliser la durée pendant laquelle vous souhaitez stocker les données historiques de vos données d'analyse NetScaler. Vous pouvez choisir les types de synthèse de base de données suivants pour les données historiques de vos analyses :

- Heures pour conserver les données par minute
- Jours pour conserver les données horaires
- Jours pour conserver les données quotidiennes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour configurer la synthèse de base de données

1. Accédez à **Système** \> **Paramètres d'analyse** \> **Synthèse de base de données**.
2. Cliquez sur le type d'Insight pour lequel vous souhaitez configurer la synthèse de base de données.

   
3. Spécifiez la durée pendant laquelle vous souhaitez conserver les données Insight sur NetScaler Console. Par exemple, pour Gateway Insight, vous pouvez stocker les données historiques par minute de vos analyses pendant 2 heures, ou les données horaires pendant 1 jour.

   

Configurer la gestion des SLA

La fonctionnalité de gestion des accords de niveau de service (SLA) vous aidera à gérer les SLA sur le temps de réponse du serveur, les requêtes/seconde et l'utilisation de la bande passante sur l'ensemble de votre domaine. La configuration des SLA sur diverses violations vous permet de surveiller facilement de nombreux événements générés dans votre infrastructure NetScaler.

Vous pouvez configurer la violation de SLA pour les éléments suivants :

- Temps de réponse du serveur
- Fréquence de violation de SLA pour la bande passante
- Fréquence de violation de SLA pour les requêtes
- Fréquence de violation de SLA pour le temps de réponse

Vous pouvez configurer des notifications pour chaque violation de SLA chaque fois que votre appliance la rencontre. Vous pouvez configurer le type de notification comme Mail, SMS ou Syslog et configurer les listes de distribution en conséquence.

Pour configurer la violation de SLA pour une instance NetScaler

1. Accédez à **Système** \> **Paramètres d'analyse** \> **Gestion des SLA**.
2. Dans la liste affichée, sélectionnez l'adresse IP NetScaler® d'une appliance sur laquelle vous souhaitez gérer le SLA.
3. Cliquez sur **Ajouter** si vous souhaitez ajouter un nouveau **groupe SLA** et y ajouter des définitions de violation. Vous pouvez également sélectionner un groupe SLA dans la liste si vous avez déjà ajouté un groupe SLA.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Dans le champ **Groupe SLA**, saisissez le nom du nouveau groupe SLA.
5. Cochez les cases appropriées pour activer ou désactiver les moniteurs SLA.
6. Sélectionnez les valeurs de violation appropriées pour les options sélectionnées. Par exemple, Temps de réponse maximal du serveur (ms)* = 22 ms.
7. Sélectionnez le type de notification et l'intervalle de notification dans les listes **Type de notification** et **Intervalle** correspondantes.
8. Vous pouvez sélectionner les listes de distribution pour envoyer les notifications dans le menu Liste de distribution de courrier/SMS/Syslog.
9. Cliquez sur **Créer** pour créer et ajouter un groupe SLA à votre appliance NetScaler.



Créer des seuils et des alertes

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance NetScaler. Vous pouvez définir des seuils sur les compteurs et surveiller les instances et les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, NetScaler Console génère un événement pour signaler un problème lié aux performances. Lorsque la valeur du compteur correspond à la valeur de suppression spécifiée dans le seuil, l'événement est effacé, ce qui signifie que ce seuil particulier est revenu à son état normal.

Vous pouvez également associer une action au seuil. Les actions incluent l'envoi d'une alerte, d'un e-mail ou d'une notification par SMS. Lorsque le seuil est dépassé, NetScaler Console exécute automatiquement l'action que vous définissez, comme l'activation d'une alerte et l'envoi d'un e-mail ou d'une notification par SMS.

Pour créer un seuil et une alerte à l'aide de NetScaler Console

1. Accédez à **Système** \> **Paramètres d'analyse** \> **Seuils**. Sous **Seuils**, cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils et des alertes**, spécifiez les détails suivants :

   - **Nom** – Nom pour la configuration du seuil.
   - **Type de trafic** – Type de trafic pour lequel vous souhaitez configurer le seuil.
   - **Entité** – Catégorie ou type de ressource pour lequel vous souhaitez configurer le seuil.
   - **Clé de référence** – Valeur générée automatiquement en fonction du type de trafic et de l'entité sélectionnés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Durée** - Intervalle pour lequel vous souhaitez configurer le seuil.
- **Communauté** – Chaîne de communauté pour chaque trap à envoyer à l'écouteur de trap.

3. Vous pouvez éventuellement configurer des actions telles que des alertes, des notifications par e-mail et des notifications par SMS.
4. Cliquez sur **Créer**.

Pour HDX™ insight, vous pouvez également définir plusieurs seuils pour lesquels une alerte est générée uniquement si toutes les entités du seuil configuré sont dépassées.

Désactiver la collecte de données d'URL

Vous pouvez désactiver la collecte de données d'URL si vous ne souhaitez pas que les rapports d'URL soient affichés sur le nœud Web Insight du tableau de bord dans NetScaler Console.

Pour désactiver la collecte de données d'URL depuis NetScaler Console

1. Accédez à **Système** \> **Paramètres d'analyse**, puis cliquez sur **Configurer les paramètres d'enregistrement des données**.
2. Dans la section **Paramètres de collecte de données d'URL Web Insight**, si l'option **Activer la collecte de données d'URL** est cochée, décochez la case.
3. Cliquez sur **OK**.



Présentation de Logstream

Les instances NetScaler génèrent des enregistrements AppFlow et constituent un point de contrôle central pour tout le trafic d'applications dans le centre de données. IPFIX et Logstream sont les protocoles qui transportent ces enregistrements AppFlow des instances NetScaler vers NetScaler Console. Pour plus d'informations, consultez (/fr-fr/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con.html).

- IPFIX est une norme ouverte de l'Internet Engineering Task Force (IETF) définie dans la RFC 5101. IPFIX utilise le protocole UDP, qui est un protocole de transport non fiable utilisé pour le flux de données dans une seule direction. Étant donné qu'IPFIX utilise le protocole UDP, le respect de la norme IPFIX entraîne le traitement de davantage de ressources dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Logstream est un protocole propriétaire de Citrix qui est utilisé comme l'un des modes de transport pour transférer efficacement les données de journal d'analyse des instances NetScaler vers NetScaler Console. Logstream utilise le protocole TCP fiable et nécessite moins de ressources pour le traitement des données.

Pour NetScaler entre les versions **11.1 Build 47.14 et 11.1 Build 62.8**, Logstream est le mode de transport par défaut pour l'activation de Web Insight (HTTP) et IPFIX est le seul mode de transport pour l'activation d'autres insights. Pour les versions de NetScaler à partir de la **12.0 jusqu'à la dernière version**, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.

Activer Logstream comme mode de transport

1. Accédez à **Infrastructure > Instances**, et sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.

   
3. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer l'analyse**.

   
4. Dans la fenêtre **Activer l'analyse** :

   a. Sélectionnez les types d'insights (Web Insight ou violations de sécurité WAF)

   b. Sélectionnez **Logstream** comme mode de transport

   REMARQUE

   Pour NetScaler entre **11.1 Build 47.14 et 11.1 Build 62.8**, Logstream est le mode de transport par défaut pour l'activation de Web Insight (HTTP) et IPFIX est le seul mode de transport pour l'activation d'autres insights. Pour les versions de NetScaler à partir de **12.0 jusqu'à la dernière version**, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.

   c. L'expression est vraie par défaut

   d. Cliquez sur **OK**

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REMARQUE

- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, NetScaler Console octroie d'abord une licence à ces serveurs virtuels, puis active l'analyse
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection de cache, l'authentification et le GSLB, vous ne pouvez pas activer l'analyse. Un message d'erreur s'affiche

Le tableau suivant décrit les fonctionnalités de NetScaler Console qui prennent en charge Logstream comme mode de transport :

FONCTIONNALITÉ	IPFIX	LOGSTREAM
Web Insight	•	•
Violations de sécurité WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Tableaux de bord

NetScaler Console fournit deux tableaux de bord : le **tableau de bord du trafic sortant** et le **tableau de bord utilisateur**. Ces tableaux de bord affichent plusieurs graphiques qui résument les sites Web ou les applications consultés depuis le réseau d'entreprise, ainsi que les activités effectuées par les utilisateurs de votre réseau.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau de bord du trafic sortant

Le **tableau de bord du trafic sortant** fournit un résumé des URL ou des domaines consultés depuis votre réseau. Il offre une vue d'ensemble de toutes les URL ou de tous les domaines par nombre de transactions ou par volume de données consommées par les URL ou les domaines. Il fournit également des détails tels que les suivants :

1. Quantité de bande passante consommée par les URL ou les domaines consultés depuis votre réseau.
2. Nombre de transactions effectuées lors de l'accès aux URL et aux domaines depuis votre réseau.
3. Nombre de connexions SSL interceptées par l'appliance NetScaler pendant les transactions.
4. Nombre de connexions SSL non interceptées par l'appliance NetScaler pendant les transactions.
5. Nombre de connexions SSL réinitialisées par l'appliance NetScaler pendant les transactions.
6. Quantité de trafic Web transmise, en fonction du port utilisé pour transmettre le trafic, du protocole utilisé par le trafic Web et des systèmes d'exploitation clients utilisés pour transmettre le trafic.

Pour accéder au tableau de bord du trafic sortant, accédez à **Applications \> Tableau de bord du trafic sortant**.



Afficher le trafic sortant du réseau

Le **tableau de bord du trafic sortant** comprend un volet **Vue d'ensemble du trafic sortant**. Dans le volet **Vue d'ensemble du trafic sortant**, NetScaler Console regroupe les URL ou les domaines consultés en catégories, telles que Shopping, Actualités, Réseaux sociaux, etc. Le volet **Vue d'ensemble du trafic sortant** affiche les URL ou les domaines consultés depuis votre réseau sous forme de nœuds dans les catégories d'URL. La taille des nœuds est proportionnelle au volume de données consommé lors de l'accès à l'URL ou au domaine. La couleur du nœud indique le nombre de transactions effectuées lors de l'accès à l'URL ou au domaine.



Vous pouvez cliquer sur une catégorie pour filtrer les graphiques afin d'afficher les détails liés à cette catégorie pour la période spécifiée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tableau de bord utilisateur

Le **Tableau de bord utilisateur** affiche un résumé des activités effectuées par les utilisateurs de votre entreprise. Il fournit des métriques clés que vous pouvez utiliser pour déterminer les éléments suivants :

1. Le comportement de navigation des utilisateurs de votre entreprise.
2. Les catégories d'URL consultées par les utilisateurs de votre entreprise.
3. Les cinq principaux utilisateurs, en fonction de leurs scores de risque et de la bande passante qu'ils consomment. Pour plus d'informations sur le score de risque, consultez Score de risque.
4. Les navigateurs utilisés pour accéder aux URL ou aux domaines.
5. La quantité de trafic web générée par les utilisateurs, en fonction du score de réputation du trafic.

Pour accéder au **Tableau de bord utilisateur**, accédez à **Utilisateurs \> Tableau de bord**.



Vous pouvez cliquer sur un utilisateur dans le volet **Principaux utilisateurs** pour filtrer les graphiques afin d'afficher les détails de l'activité web effectuée par l'utilisateur pendant la période spécifiée.

Investigateur d'activité utilisateur

Le **Tableau de bord utilisateur** comprend un volet **Investigateur d'activité utilisateur** affichant diverses activités web effectuées par les utilisateurs. Il indique les catégories d'URL consultées par les utilisateurs pendant la période sélectionnée, et divers événements déclenchés par catégorie d'URL. Vous pouvez cliquer sur les événements pour obtenir les détails au niveau de la transaction.

L'**Investigateur d'activité utilisateur** affiche des informations clés telles que le comportement de navigation de l'utilisateur, les activités à haut risque de l'utilisateur et les événements déclenchés, par catégorie d'URL. Les événements sont affichés sous forme de légendes rectangulaires sur le graphique. Chacune des légendes est agrégée par intervalles d'une minute si la durée sélectionnée est d'une heure, et par intervalles d'une heure si la durée sélectionnée est d'un jour.



Ces légendes sont agrégées et sont codées par couleur en fonction du nombre d'événements qui se sont produits. Vous pouvez survoler une légende avec le pointeur de votre souris pour afficher des détails tels que l'heure et le nombre d'événements agrégés pour la légende sélectionnée.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vous pouvez personnaliser la période du graphique en sélectionnant une heure dans la liste des périodes.

Vous pouvez cliquer sur les événements pour explorer davantage les détails des transactions.

Transactions utilisateur

La page Transactions utilisateur affiche les détails des transactions utilisateur dans votre réseau. Elle fournit des détails au niveau des transactions, tels que :

1. Heure à laquelle la transaction a eu lieu
2. Protocole utilisé pour la transaction
3. Nom d'utilisateur
4. Domaine accédé par l'utilisateur
5. Catégorie d'URL
6. Serveur proxy utilisé pour intercepter la transaction
7. Détails du port client
8. Octets entrants
9. Octets sortants



Panneau récapitulatif

Le **Panneau Récapitulatif** affiche toutes les métriques des transactions visibles dans le volet **Détails des transactions**. Ce panneau vous permet de trier et d'afficher les transactions dans le volet **Détails des transactions** en sélectionnant ou désélectionnant les métriques. Le **Panneau Récapitulatif** affiche les métriques suivantes :

MÉTRIQUES	DESCRIPTION
Protocoles	Protocoles utilisés dans les transactions
Ports	Ports utilisés pour les transactions
Réputation d'URL	Score de réputation d'URL
Navigateurs	Navigateurs utilisés pour les transactions
Système d'exploitation	Système d'exploitation utilisé pour les transactions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MÉTRIQUES	DESCRIPTION
Octets entrants	Quantité de données reçues via l'appliance NetScaler.
Octets sortants	Quantité de données envoyées via l'appliance NetScaler.

Score de risque

Le score de risque est un système de notation utilisé dans NetScaler Console pour déterminer les risques associés aux utilisateurs de votre entreprise. NetScaler Console attribue un score de risque basé sur le score de réputation d'URL attribué par l'appliance NetScaler pour les URL consultées par les utilisateurs de votre réseau. Pour plus d'informations sur le score de réputation d'URL, consultez Score de réputation d'URL. Le tableau suivant décrit les scores de risque attribués par NetScaler Console.

SCORE DE RISQUE	DESCRIPTION
1	L'activité web de l'utilisateur ne présente aucune menace perçue ou n'est pas anormale.
2	L'activité web de l'utilisateur ne présente aucune menace perçue ou n'est pas anormale, mais l'utilisateur accède à des « sites inconnus » qui n'ont pas de scores de réputation d'URL.
3	Aucune menace n'est détectée dans l'activité web de l'utilisateur, mais l'utilisateur a tenté d'accéder à des sites potentiellement vulnérables ou affiliés à des sites potentiellement vulnérables.
4	Utilisateur potentiellement compromis.
5	L'activité web de l'utilisateur est anormale et l'utilisateur a accédé à des sites malveillants connus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Toutes les violations

La page **Toutes les violations** affiche les détails des violations de sécurité des applications en fonction des catégories **Réseau**, **WAF** et **Bot**.

Catégories de violations

NetScaler Console vous permet d'afficher les violations suivantes. Sous **Détails de la violation**, vous pouvez cliquer sur chaque onglet de violation pour afficher les détails de la violation.

RÉSEAU	WAF	BOT
HTTP Slow Loris	Marquage de formulaire CSRF	Marketing
DNS Slow Loris	Refuser l'URL	Scraper
HTTP Slow Post	Cohérence des champs de formulaire	Créateur de captures d'écran
Attaque par inondation NXDomain	Formats de champ	Moteur de recherche
Attaque de désynchronisation HTTP	Détournement de cookie	Récupérateur de flux
Attaque de Bleichenbacher	Inférence du type de contenu XML	Vérificateur de liens
Attaque par claquement de segment	Dépassement de tampon	Agent de service
Attaque par inondation SYN	Type de contenu	Moniteur de site
Attaque par petite fenêtre	Cohérence des cookies	Testeur de vitesse
	Objet sécurisé	Outil
	Injection SQL HTML	Non classé
	URL de démarrage	Analyseur de virus
	Script intersites	Analyseur de vulnérabilités

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RÉSEAU	WAF	BOT
	DoS XML	Délai d'attente DeviceFP dépassé
	Format XML	DeviceFP invalide
	XML WSI	Réponse Captcha invalide
	XML SSL	Nombre de tentatives Captcha dépassé
	Pièce jointe XML	Réponse Captcha valide
	Erreur SOAP XML	Client Captcha mis en sourdine
	Validation XML	Temps d'attente Captcha dépassé
	Autres	Limite de taille de requête dépassée
	Réputation IP	Limite de débit dépassée
	HTTP DOS	Liste de blocage (IP, sous-réseau, expression de stratégie)
	Petite fenêtre TCP	Liste d'autorisation (IP, sous-réseau, expression de stratégie)
	Violation de signature	Requête zéro pixel
	Type de téléchargement de fichier	IP source
	Script inter-sites JSON	Hôte
	SQL JSON	Géolocalisation
	DOS JSON	URL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RÉSEAU	WAF	BOT
	Injection de commandes	Robot d'exploration
	Nombre maximal de téléchargements	
	En-tête Referrer	
	Commerce sécurisé	

Tableau de bord des violations de sécurité

Dans le tableau de bord des violations de sécurité, vous pouvez afficher :

- Nombre total de violations sur toutes les instances et applications NetScaler. Le nombre total de violations est affiché en fonction de la durée sélectionnée.
- Nombre total de violations.
- Nombre total d'instances NetScaler affectées, nombre total d'applications affectées et principales violations basées sur le nombre total d'occurrences et les applications affectées.

Détails de la violation

Pour chaque violation, NetScaler Console surveille le comportement pendant une durée spécifique et détecte les violations pour les comportements inhabituels. Cliquez sur chaque onglet pour afficher les détails de la violation. Vous pouvez afficher des détails tels que :

- Le nombre total d'occurrences, la dernière occurrence et le nombre total d'applications affectées.
- Sous les détails de l'événement, vous pouvez afficher :
  - L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par des violations.
  - Le graphique indiquant les violations.

    Faites glisser et sélectionnez sur le graphique qui répertorie les violations pour affiner la recherche de violations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAITES GLISSER ET SÉLECTIONNEZ SUR LE GRAPHIQUE	RÉSULTAT DE LA RECHERCHE
	

Cliquez sur **Réinitialiser le zoom** pour réinitialiser le résultat du zoom.

- **Actions recommandées** qui vous suggèrent de résoudre le problème.
- Autres détails de la violation, tels que l'heure d'occurrence de la violence et le message de détection.

Vue d'ensemble de l'application

La page **Vue d'ensemble de l'application** affiche les applications avec une visibilité complète sur les détails des menaces associées aux violations de sécurité WAF et aux violations de sécurité des bots. Vous pouvez également afficher des informations telles que le nombre total de violations, le nombre total de violations WAF et de bots, les violations par pays, etc.



1 – Affiche le nombre total d'applications affectées, le nombre total de violations, le nombre total de violations WAF et le nombre total de violations de bots pour la durée sélectionnée.

2 – Affiche les détails des violations WAF et de bots. Cliquez sur l'onglet **WAF** et **Bot** pour afficher les 5 principales applications en fonction du nombre total de violations survenues. Cliquez sur **Afficher tout** pour afficher tous les détails de l'application.

3 – Affiche les principales violations en fonction des occurrences et des actions appliquées.

4 – Affiche une vue cartographique géographique qui indique les emplacements d'où proviennent les violations.

5 – Fournit des informations basées sur les violations.

Catégories de violations

WAF	BOT
Détournement de cookie	Récupérateur de flux
Inférence du type de contenu XML	Vérificateur de liens
Marquage de formulaire CSRF	Marketing

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
URL refusée	Scraper
Cohérence des champs de formulaire	Créateur de captures d'écran
Formats de champ	Moteur de recherche
Nombre maximal de téléchargements	Agent de service
En-tête Referrer	Moniteur de site
Commerce sécurisé	Testeur de vitesse
Objet sécurisé	Outil
Injection SQL HTML	Non classé
URL de démarrage	Analyseur de virus
Script intersite	Analyseur de vulnérabilités
DoS XML	Délai d'attente DeviceFP dépassé
Format XML	DeviceFP invalide
WSI XML	Réponse Captcha invalide
SSL XML	Tentatives Captcha dépassées
Pièce jointe XML	Réponse Captcha valide
Erreur SOAP XML	Client Captcha désactivé
Validation XML	Délai d'attente Captcha dépassé
Autres	Limite de taille de requête dépassée
Réputation IP	Limite de débit dépassée
DOS HTTP	Liste de blocage (IP, sous-réseau, expression de stratégie)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
Fenêtre TCP petite	Liste d'autorisation (IP, sous-réseau, expression de stratégie)
Violation de signature	Requête zéro pixel
Type de téléchargement de fichier	Adresse IP source
Script intersite JSON	Hôte
SQL JSON	Géolocalisation
DOS JSON	URL
Injection de commande	Robot d'exploration
Dépassement de tampon	
Type de contenu	
Cohérence des cookies	

Afficher les détails de la violation WAF

Cliquez sur une application à partir de **Top Applications** ou de l'option **Afficher tout** pour afficher les détails WAF.

La page **Aperçu de la sécurité** de l'application sélectionnée s'affiche. Sous **WAF**, vous pouvez afficher :

- Une vue graphique qui indique le nombre total de violations, le score d'indice de menace et le score d'indice de sécurité pour l'application.

  Cliquez sur **Afficher les détails** pour afficher les détails de configuration du pare-feu d'application et de la sécurité du système NetScaler.

- Les violations basées sur les types, la gravité et les actions appliquées.

  Cliquez sur **Journaux** pour afficher les détails basés sur la gravité ou l'action entreprise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Les violations affectant l'application. Sous **Détails de la violation**, vous pouvez afficher les détails de la violation affectée. Cliquez sur chaque violation pour afficher des détails tels que :
  - **Ce qui s'est passé** – Indique le nombre total d'occurrences ainsi que la date et l'heure de la dernière occurrence.
  - **Détails de l'événement** – Affiche une carte géographique qui indique l'adresse IP du client et d'autres détails de violation tels que le type de violation, l'adresse IP du client, l'emplacement, et ainsi de suite.

Afficher les détails de la violation de bot

Dans l'onglet **Bot**, cliquez sur une application parmi les applications principales (Top Applications) ou sur l'option **Afficher tout** (View All) pour afficher les détails du bot.

La page **Aperçu de la sécurité** (Security Overview) de l'application sélectionnée s'affiche. Sous **Bot**, vous pouvez afficher :

- Un graphique indiquant le nombre total de bots, de mauvais bots, de bons bots, et le ratio total entre les utilisateurs humains et les bots accédant à l'application.
- Les violations basées sur les types de bots, la gravité et les actions appliquées.

  Cliquez sur **Journaux** (Logs) pour afficher les détails basés sur la gravité ou les actions entreprises. Si un bot détecté est un bot de type Signature, vous pouvez afficher plus de détails tels que le développeur du bot et l'ID de signature. L'ID de signature vous permet d'identifier si le bot détecté est un bon bot ou un mauvais bot.

  Remarque

  > Si un bot détecté est un type de bot autre qu'un bot de signature, l'ID de signature et le développeur du bot sont affichés comme N/A.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Les violations affectées sur l'application. Sous Détails de la violation (Violation Details), vous pouvez afficher les détails des violations affectées. Cliquez sur chaque violation pour afficher des détails tels que :
  - **Ce qui s'est passé** (What Happened) – Indique le nombre total d'occurrences et la date et l'heure de la dernière occurrence.
  - **Détails de l'événement** – Affiche une carte géographique qui indique l'adresse IP du client et d'autres détails de violation tels que le type de violation, l'adresse IP du client, l'emplacement, etc.



REMARQUE

Sous **WAF** et **Bot**, vous pouvez afficher les analyses pour le serveur virtuel de commutation de contenu lié aux serveurs virtuels d'équilibrage de charge. Cliquez sur le serveur virtuel de commutation de contenu et sous **Serveur d'équilibrage de charge lié**, vous pouvez afficher la liste des serveurs d'équilibrage de charge liés au serveur virtuel de commutation de contenu.



Afficher l'historique des événements

Cliquez sur l'onglet **Événements** pour afficher les événements de bot et WAF.

Détails de la violation réseau

HTTP Slow Loris

L'attaque **Slow Loris** est une attaque par déni de service qui peut envoyer des en-têtes HTTP à l'application cible aussi lentement que possible. L'application cible est forcée d'attendre l'arrivée des en-têtes et peut rapidement devenir indisponible pour traiter les requêtes si plusieurs connexions similaires sont ouvertes. Lorsqu'une instance NetScaler reçoit un volume élevé de requêtes HTTP, l'en-tête HTTP augmente et prend beaucoup de temps à compléter les requêtes. Ce processus peut épuiser les ressources du serveur d'applications et entraîner une attaque HTTP **Slow Loris**.

À l'aide de l'indicateur **HTTP Slow Loris**, vous pouvez analyser les requêtes qui ont abouti à une attaque **Slow Loris**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Les **actions recommandées** pour résoudre le problème :

- Envisagez de régler la configuration du délai d'en-tête incomplet (incompHdrDelay) sur une valeur plus petite.
- Par défaut, l'instance NetScaler supprime ces requêtes incomplètes.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par des violations.
- Le graphique indiquant toutes les violations
- L'heure de survenance de la violation
- Le message de détection indiquant le total des requêtes incomplètes comme attaque **Slow Loris**

DNS Slow Loris

L'indicateur **DNS Slow Loris** détecte lorsqu'un NetScaler reçoit un grand nombre de requêtes DNS s'étendant sur plus d'un paquet. Ce processus peut épuiser les ressources du serveur DNS et entraîner une attaque **DNS Slow Loris**. Par défaut, l'instance NetScaler supprime ces requêtes **DNS Slow Loris** et aucune autre action n'est requise pour résoudre ce problème.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par des violations.
- Le graphique indiquant toutes les violations
- L'heure de l'occurrence de la violation
- Le message de détection indiquant le total des requêtes DNS comme attaque **Slow Loris**

HTTP Slow Post

Le Slow Post est une attaque par déni de service qui peut envoyer des en-têtes HTTP POST à une application cible. Dans les en-têtes, les tailles des corps de message sont spécifiées correctement, mais le corps du message est envoyé à faible vitesse. L'application cible est forcée d'attendre et peut également devenir rapidement indisponible pour traiter les requêtes si plusieurs connexions similaires sont ouvertes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ce processus peut épuiser les ressources du serveur d'applications et entraîner une attaque HTTP Slow Post.

À l'aide de l'indicateur **HTTP Slow Post**, vous pouvez analyser les requêtes qui ont entraîné une attaque de type slow post.

L'**action recommandée** pour résoudre ce problème est d'activer et de configurer le délai d'expiration des requêtes (Request Timeout) dans le profil HTTP de NetScaler. Pour plus d'informations, consultez Configurations HTTP.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par des violations.
- Le graphique indiquant toutes les violations
- L'heure de l'occurrence de la violation
- Le message de détection indiquant le nombre total de requêtes POST comme attaque **Slow Loris**

Attaque par inondation NXDOMAIN

L'attaque par inondation NXDOMAIN est une attaque par déni de service distribué (DDoS) qui peut cibler un serveur DNS ou une instance NetScaler (configurée comme serveur proxy DNS) et envoyer un volume élevé de requêtes inexistantes ou invalides. Cette attaque peut impacter le serveur DNS ou l'instance NetScaler, entraînant un ralentissement ou l'absence de réponse aux requêtes.

À l'aide de l'indicateur **Attaque par inondation NXDOMAIN**, vous pouvez analyser les requêtes qui ont entraîné une attaque NXDOMAIN.

Les **Actions recommandées** pour résoudre le problème :

- Vérifiez la consommation de ressources anormalement élevée sur le serveur DNS et le serveur proxy DNS.
- Appliquez une limite de débit de requêtes sur l'instance NetScaler
- Isolez et bloquez les adresses IP clientes suspectes
- Si la plupart des noms aboutissent à NXDOMAIN, suivez un modèle identifiable et configurez des politiques DNS pour abandonner ces requêtes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pour économiser la mémoire pour les enregistrements DNS authentiques, configurez une limite pour les enregistrements négatifs sur l'instance NetScaler. Pour plus d'informations, consultez Atténuer les attaques DDoS DNS.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par des violations.
- Le graphique indiquant toutes les violations

Attaque de désynchronisation HTTP

Lors d'une attaque de désynchronisation HTTP, une seule requête HTTP est interprétée comme :

- Une seule requête vers le serveur frontal (serveur virtuel)
- 2 requêtes vers le serveur principal

Dans ce scénario, le serveur principal interprète la deuxième requête comme provenant d'un client différent. La connexion entre le serveur virtuel et le serveur principal est réutilisée pour différentes requêtes. Si la première requête client est traitée à partir d'un client malveillant avec des données malveillantes, la requête client suivante peut avoir une requête personnalisée. Cette activité peut provoquer une attaque en abusant de la combinaison de deux en-têtes : la longueur du contenu et l'encodage de transfert.

À l'aide de l'indicateur **Attaque de désynchronisation HTTP**, vous pouvez analyser si l'instance NetScaler est susceptible de subir une attaque de désynchronisation HTTP due à la présence de :

- En-têtes de longueur de contenu et d'encodage de transfert dans une seule transaction HTTP
- Plusieurs en-têtes de longueur de contenu avec des valeurs différentes dans une seule transaction HTTP



L'**Action recommandée** vous suggère d'envisager de supprimer les transactions HTTP non valides.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par cette violation.
- Le graphique indiquant les détails de la violation. Passez le pointeur de la souris sur le graphique à barres pour afficher le total des requêtes/réponses non valides.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Le message de détection de la violation, indiquant le total des requêtes/réponses :
  - Contenant plusieurs en-têtes de longueur de contenu avec des valeurs différentes
  - Contenant à la fois les en-têtes de longueur de contenu et de codage de transfert

Attaque Bleichenbacher

L'instance NetScaler détecte si une séquence d'octets donnée d'un message chiffré a le bon format de remplissage lors du déchiffrement.

À l'aide de l'indicateur **Attaque Bleichenbacher**, vous pouvez analyser si l'instance NetScaler reçoit des connexions d'établissement de liaison SSL/TLS avec des données chiffrées erronées.



L'**Action recommandée** indique qu'aucune autre action n'est requise car l'instance NetScaler met fin aux connexions d'établissement de liaison et atténue cette attaque.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par cette violation.
- Le graphique indiquant les détails de la violation. Passez le pointeur de la souris sur le graphique à barres pour afficher le nombre total de connexions d'établissement de liaison erronées détectées.
- Le message de détection de la violation, indiquant le nombre total de connexions d'établissement de liaison sur le serveur virtuel avec des données chiffrées erronées.

Attaque Segment Smack

Une **attaque Segment Smack** est une attaque par déni de service (DoS), au cours de laquelle l'attaquant peut envoyer des paquets de petite taille non ordonnés pendant une session TCP. Ces paquets TCP personnalisés peuvent affecter le CPU et la mémoire, et entraîner un déni de service sur l'instance NetScaler.

À l'aide de l'indicateur **Attaque Segment Smack**, vous pouvez analyser si une instance NetScaler a reçu un grand nombre de paquets TCP supérieur à la limite de file d'attente configurée. Pour plus d'informations, consultez configuration TCP.



En tant qu'administrateur, aucune autre action n'est requise car l'instance NetScaler atténue cette attaque en supprimant tous ces paquets TCP excédentaires.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'instance NetScaler affectée
- Le graphique indiquant les détails de la violation. Passez le pointeur de la souris sur le graphique à barres pour afficher le nombre total de mauvaises connexions client détectées.
- Le message de détection de la violation, indiquant le nombre total de connexions client abandonnées.



Attaque par inondation SYN

Une attaque par inondation SYN est une attaque par déni de service (DoS) qui peut affecter la machine cible en envoyant des milliers de requêtes de connexion à l'aide d'adresses IP usurpées. Lorsqu'une instance NetScaler est soumise à une attaque par inondation SYN, l'instance tente d'ouvrir une connexion pour chaque requête malveillante, puis attend un paquet d'accusé de réception qui n'arrive jamais.

Le **SYNCOOKIE** dans le profil TCP empêche les attaques SYN sur l'appliance NetScaler. Par défaut, le **SYNCOOKIE** sur l'instance NetScaler est activé. La probabilité qu'une instance NetScaler soit soumise à une attaque par inondation SYN est élevée uniquement lorsque le SYNCOOKIE est désactivé.

À l'aide de l'indicateur **Attaque par inondation SYN**, vous pouvez analyser si l'instance NetScaler est soumise à une attaque SYN.



En tant qu'administrateur, l'**Action recommandée** vous suggère d'activer le SYN COOKIE dans le profil TCP.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par cette violation.
- Le graphique indiquant les détails de l'attaque SYN
- Le message de détection, indiquant le nombre total de fois où l'application a été détectée avec une attaque SYN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Attaque par petite fenêtre

Une attaque par petite fenêtre est une attaque par déni de service (DoS) qui peut affecter la machine cible en envoyant des milliers de paquets TCP avec une fenêtre de taille plus petite ou une taille de fenêtre de 0. La taille de fenêtre 0 indique que la machine cible doit cesser d'envoyer des données jusqu'à nouvel ordre. En envoyant autant de connexions similaires à la machine cible, la mémoire de la machine cible est utilisée au maximum et celle-ci devient insensible.

À l'aide de l'indicateur **Attaque par petite fenêtre**, vous pouvez analyser si l'instance NetScaler est sous l'attaque sockstress.



Par défaut, l'instance NetScaler atténue cette attaque en abandonnant tous les paquets TCP de petite fenêtre. Par conséquent, en tant qu'administrateur, aucune autre action n'est requise.

Sous **Détails de l'événement**, vous pouvez afficher :

- L'application affectée. Vous pouvez également sélectionner l'application dans la liste si deux applications ou plus sont affectées par cette violation.
- Le graphique indiquant les détails de l'attaque. Passez le pointeur de la souris sur le graphique à barres pour afficher le nombre total de paquets TCP de petite fenêtre détectés.
- Le message de détection indiquant le nombre total de paquets TCP de petite fenêtre abandonnés.

SSL Insight

SSL Insight offre une visibilité sur les transactions web sécurisées (HTTPS) et permet aux administrateurs informatiques de surveiller toutes les applications web sécurisées servies par le NetScaler en fournissant une surveillance intégrée, en temps réel et historique des transactions web sécurisées. Grâce à cette visibilité, l'administrateur peut évaluer les points suivants :

- **Déterminer l'impact des changements de configuration sur l'utilisation par le client** : L'administrateur peut comprendre l'impact sur les clients d'un changement de configuration, comme la désactivation de SSLv3 ou la suppression d'un chiffrement comme RC4-MD5. Cela peut être fait en évaluant les données de transaction historiques sur ce protocole et ce chiffrement.
- **Quantifier les performances du client** : L'administrateur peut comprendre l'impact sur le temps de réponse de l'application en fonction des chiffrements/protocoles SSL utilisés ou des certificats négociés.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Sécurité des applications** : Évaluer si l'une des applications a des transactions exécutées sur des protocoles de faible sécurité, des chiffrements faibles ou une force de clé faible.

Lorsque SSL Analytics est activé sur une instance NetScaler, les statistiques SSL sont enregistrées et journalisées pour chaque transaction SSL. Les statistiques affichent les détails du flux SSL. De plus, chaque connexion réussie est journalisée et affichée par NetScaler Console Analytics.

SSL Insight fournit les informations critiques suivantes, qui sont affichées par NetScaler Console Analytics :

- Version du protocole SSL négociée
- Chiffrement négocié et force du chiffrement
- Algorithme de hachage de signature du certificat utilisé
- Type et taille du certificat
- Erreurs SSL front-end et back-end

REMARQUE

Pour les connexions SSL réussies, la journalisation SSL AppFlow® a lieu à la fin de chaque transaction.

Prérequis

- L'instance NetScaler sur laquelle vous avez l'intention de configurer SSL Insight doit exécuter la version logicielle NetScaler 11.1 51.21 ou supérieure. Exécutez les commandes suivantes sur l'instance ADC exécutant 11.1 51.21 pour activer Logstream comme type de transport pour SSL Insight.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the Console>`

   Pour les instances ADC exécutant la version 12.0 et supérieure, sélectionnez Logstream comme type de transport lors de l'activation d'AppFlow depuis NetScaler Console.

- La version et le build de NetScaler Console doivent être égaux ou supérieurs à la version et au build de NetScaler. Par exemple, si vous avez installé NetScaler Console 11.1 build 61.7, assurez-vous d'avoir installé NetScaler 11.1 build 60.14 ou une version antérieure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurer SSL Insight

Les métriques SSL Insight sont incluses dans les rapports Web Insight si vous activez les éléments suivants :

- Activez AppFlow pour Web Insight sur chaque instance NetScaler.
- Activez le mode ULFD sur chaque instance NetScaler.
- Activez les paramètres AppFlow requis sur chaque instance NetScaler.

Activer la fonctionnalité AppFlow

REMARQUE

Vous pouvez activer la fonctionnalité AppFlow soit depuis NetScaler Console, soit depuis chaque instance NetScaler.

Pour activer la fonctionnalité AppFlow depuis NetScaler Console :

Si votre NetScaler Console est **13.0 Build 41.x ou ultérieur** :

1. Accédez à **Infrastructure > Instances > NetScaler**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, cliquez sur **Configurer l'analyse**.
3. Sur la page **Configurer l'analyse sur les serveurs virtuels**, sélectionnez le serveur virtuel, puis cliquez sur **Activer l'analyse**.
4. Dans la fenêtre **Activer l'analyse** :
   a. Sélectionnez **Web Insight**
   b. Sélectionnez **Logstream** comme mode de transport

   REMARQUE

   Pour NetScaler 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour NetScaler 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.

   Pour plus d'informations sur IPFIX et Logstream, consultez Présentation de Logstream.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. L'expression est vraie par défaut

d. Cliquez sur **OK**



REMARQUE

- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, NetScaler Console attribue d'abord une licence à ces serveurs virtuels, puis active l'analyse.
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection de cache, l'authentification et le GSLB, vous ne pouvez pas activer l'analyse. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, NetScaler Console procède à l'activation de l'analyse sur les serveurs virtuels sélectionnés.

Si votre NetScaler Console est **13.0 Build 36.27 ou une version antérieure** :

1. Accédez à **Infrastructure > Instances > NetScaler**, et sélectionnez l'instance NetScaler sur laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer l'analyse**.



3. Sur la page **Configurer Insight** :

a. Sélectionnez la **Liste des applications** pour l'équilibrage de charge ou la commutation de contenu.



b. Sélectionnez le serveur virtuel et cliquez sur **Activer AppFlow**.



4. Dans la boîte de dialogue Activer AppFlow :

- Saisissez **true** dans la zone de texte
- Sélectionnez **Logstream** comme mode de transport

REMARQUE :

Nous vous recommandons de sélectionner Logstream comme mode de transport

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sélectionnez **Web Insight** et cliquez sur **OK**.



Pour activer la fonctionnalité AppFlow à l'aide de l'interface graphique de NetScaler :

Dans l'interface graphique d'une instance NetScaler, accédez à **Configuration** \> **Système** \> **Paramètres**, cliquez sur **Configurer les fonctionnalités avancées**, et sélectionnez **AppFlow**.

Activer les paramètres SSL Insight

Sur chaque instance NetScaler, vous devez activer certains paramètres HTTP pour afficher les enregistrements SSL Insight dans NetScaler Console.

Pour activer les paramètres SSL Insight à partir de l'utilitaire de configuration NetScaler :

1. Accédez à **Configuration** \> **Système** \> **AppFlow**, et cliquez sur **Modifier les paramètres AppFlow**.
2. Sélectionnez les cases à cocher suivantes : **HTTP Domain**, **HTTP Host**, **HTTP Method**, **HTTP URL**, **HTTP User-Agent**, **HTTP Content-Type**.
3. Cliquez sur **OK**.



Afficher les métriques SSL Insight

Les métriques SSL Insight dans NetScaler Console fournissent une vue détaillée des performances des transactions SSL servies par les instances NetScaler. Vous pouvez afficher les métriques SSL Insight au niveau du client, du serveur ou de l'application, ainsi que les métriques des transactions SSL réussies et échouées. À l'aide de ces métriques, vous pouvez analyser et optimiser vos paramètres **NetScaler HTTPS** et les paramètres de certificat SSL, et suivre les problèmes de performances.

REMARQUE

Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au niveau de l'application au groupe et attribuer des utilisateurs au groupe. L'analyse de NetScaler Console prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais consulter les rapports de toutes les informations pour les seules applications (serveurs virtuels) auxquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'attribution d'utilisateurs au groupe, consultez Configurer les groupes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pour surveiller les métriques SSL Insight dans NetScaler Console :

Vous pouvez afficher les métriques SSL pour :

- Une application. Accédez à **Applications > Tableau de bord**, cliquez sur une application et sélectionnez l'onglet **Web Insight** pour afficher les métriques détaillées. Pour plus d'informations, consultez Analyse de l'utilisation des applications.
- Toutes les applications. Accédez à **Applications > Web Insight** et cliquez sur les onglets **Applications** et **Clients** pour afficher les métriques SSL.

Cas d'utilisation : Obtenir un aperçu des transactions SSL

Le cas d'utilisation suivant décrit comment vous pouvez utiliser SSL Insight pour évaluer l'utilisation de divers paramètres SSL et améliorer les mesures de sécurité.

Considérez que vous disposez d'un ensemble d'applications qui utilisent des transactions SSL (HTTPS) pour la communication, et que vous avez configuré NetScaler Console pour surveiller les composants SSL. Vous devrez peut-être examiner fréquemment les applications afin de vous concentrer d'abord sur celles qui nécessitent le plus d'attention. Le tableau de bord **Web Insight** pour une application ou toutes les applications fournit un résumé des paramètres SSL suivants sous **Erreurs SSL** et **Utilisation SSL** :

- Certificats SSL
- Protocoles SSL
- Chiffrement SSL
- Force de la clé SSL
- Échec SSL – Front-end
- Échec SSL – Back-end



Vous pouvez cliquer sur chaque onglet pour afficher les détails.

Cas d'utilisation : Métriques SSL pour les clients

Vous pouvez voir la liste des clients (identifiés par leurs adresses IP) et le nombre total d'occurrences par client. Accédez à **Applications > Web Insight** et sélectionnez l'onglet **Clients** pour afficher les détails sous **Utilisation SSL**.

Cliquez sur une métrique pour afficher les détails et sous **Clients**, cliquez sur n'importe quelle adresse IP de client pour afficher les métriques SSL du client sélectionné.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Résoudre les problèmes de Web Insight

Dans le tableau de bord Web Insight, vous pouvez visualiser l'utilisation de vos applications et surveiller toutes les applications servies par les NetScaler. À l'aide de Web Insight, les NetScaler envoient des données de transaction HTTP et SSL à la NetScaler Console configurée comme collecteur AppFlow. AppFlow est la norme d'exportation de flux utilisée pour identifier et collecter les données d'application et de transaction dans l'infrastructure réseau.

Ce document vous aide à résoudre les problèmes courants de déploiement de Web Insight.

Diagnostics en cas d'absence de données

Si Web Insight n'affiche aucune donnée, assurez-vous que **Web Insight** est activé pour le serveur virtuel. Pour plus d'informations, consultez Gérer les licences et activer l'analyse sur les serveurs virtuels.

Une notification avec **Diagnostics en cas d'absence de données** est également visible s'il n'y a pas de données dans Web Insight. Vous pouvez cliquer pour afficher les détails de dépannage.

Problèmes liés aux rapports du tableau de bord Web Insight

Si le tableau de bord Web Insight de NetScaler Console (**Applications> Web Insight**) ne parvient pas à afficher les rapports, le problème peut être l'un des suivants :

- Problème de configuration de Web Insight
- Problème de connectivité entre NetScaler et NetScaler Console
- Les données AppFlow ne sont pas reçues de NetScaler
- Problème de licence
- Problème d'ID de point d'observation
- Problème de paramètres AppFlow® manquants

Problème de configuration

Suivez les étapes suivantes pour résoudre ce problème :

1. Assurez-vous que la fonctionnalité AppFlow est activée dans l'instance NetScaler. Pour plus de détails, consultez Activation d'AppFlow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Vérifiez la configuration de Web Insight dans le NetScaler :

    a. Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration de Web Insight sur la stratégie. Assurez-vous que le type de liaison est `REQUEST`. Par exemple : `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`

    b. Exécutez la commande `show appflow action` pour vérifier la configuration de Web Insight sur l'action. Assurez-vous que l'option `-webinsight` est activée.

    c. Vérifiez le paramètre `appflowlog` dans le serveur virtuel LB/CS/CR, ainsi que les services et groupes de services liés. Assurez-vous que ce paramètre est activé à la fois dans le serveur virtuel, et dans les services et groupes de services liés.

Problème de connectivité entre NetScaler et NetScaler Console

Suivez les étapes suivantes pour résoudre ce problème :

1. Vérifiez l'état du collecteur AppFlow dans NetScaler. Pour plus de détails, consultez Comment vérifier l'état de la connectivité entre NetScaler et le collecteur AppFlow.
2. Dans l'interface graphique de NetScaler, vérifiez si les stratégies AppFlow reçoivent des hits. Exécutez la commande `show appflow policy <policy_name>` pour vérifier les hits de stratégie AppFlow. Vous pouvez également naviguer vers **Paramètres > AppFlow > Stratégies** dans l'interface graphique pour vérifier les hits de stratégie AppFlow.
3. Assurez-vous que le pare-feu ne bloque pas les données AppFlow de NetScaler vers NetScaler Console.

Données AppFlow non reçues de NetScaler®

Suivez les étapes suivantes pour résoudre ce problème :

1. Assurez-vous qu'il n'y a pas de problèmes de configuration et de connectivité AppFlow. Pour plus d'informations, consultez les sections de solution de ce sujet pour problème de configuration et problème de connectivité entre NetScaler et NetScaler Console.
2. Sur le NetScaler, à l'invite de commande, exécutez la commande `nsconmsg -g appflow_tmpl -d current` et vérifiez les compteurs suivants :

    - `appflow_tmpl_v4_l7_clt2ns_complete`
    - `appflow_tmpl_v4_l7_srvr2ns_complete`
    - `appflow_tmpl_v46_ulfd_client_eot`
    - `appflow_tmpl_v46_ulfd_server_eot`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Si l'un des compteurs est manquant, effectuez une trace sur le NetScaler. Ensuite, confirmez que la transaction est terminée et que la réponse est servie par le serveur d'origine. Si la transaction est terminée et que certains compteurs sont manquants, contactez l'équipe de support.

Problème de licence

Avec ce problème, la licence du serveur virtuel particulier pour lequel vous souhaitez afficher le rapport Web Insight apparaît « Non » sous **Paramètres > Configuration des licences et de l'analyse > Configurer la licence**.

Suivez les étapes suivantes pour résoudre ce problème :

1. Dans le NetScaler, assurez-vous que les accès de la politique AppFlow augmentent et que l'instance envoie des enregistrements AppFlow à NetScaler Console.
2. Vérifiez si le serveur virtuel correspondant est sous licence. Si le serveur virtuel n'est pas sous licence, NetScaler Console supprime les enregistrements AppFlow. Par conséquent, les rapports Web Insight n'apparaissent pas.

Problème d'ID de point d'observation

Ce problème apparaît parce que l'ID du point d'observation n'est pas unique.

REMARQUE

Un ID de point d'observation est l'identifiant du NetScaler à partir duquel les enregistrements AppFlow sont exportés. Par défaut, l'adresse IP du NetScaler est l'ID du point d'observation.

Effectuez les étapes suivantes pour résoudre ce problème :

1. Dans le NetScaler, assurez-vous que les accès de la stratégie AppFlow augmentent et que l'instance envoie des enregistrements AppFlow à NetScaler Console.
2. Vérifiez si le serveur virtuel correspondant est sous licence.
3. Assurez-vous que la configuration n'est pas copiée d'un NetScaler à un autre. Lorsqu'elle est copiée, la configuration peut créer un problème d'ID d'exportateur qui empêche NetScaler Console de traiter les enregistrements AppFlow.
4. Connectez-vous au NetScaler et exécutez la commande `unset appflow param -observationpointId`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Problème de paramètres AppFlow manquants

Ce problème apparaît parce que NetScaler Console supprime les enregistrements AppFlow en raison de données manquantes.

Effectuez les étapes suivantes pour résoudre ce problème :

1. Assurez-vous dans le NetScaler que les accès de la stratégie AppFlow augmentent et que l'instance envoie les enregistrements AppFlow à NetScaler Console.
2. Vérifiez si le serveur virtuel correspondant est sous licence.
3. Assurez-vous que la configuration n'est pas copiée d'un NetScaler à un autre. Lorsqu'elle est copiée, la configuration peut créer un problème d'ID d'exportateur qui empêche NetScaler Console de traiter les enregistrements AppFlow.
4. Assurez-vous que les paramètres AppFlow suivants sont activés sur le NetScaler :
   - `HTTP method logging`
   - `HTTP domain name logging`
   - `HTTP URL logging`
   - `HTTP host logging`
   - `HTTP Content-Type header logging`

Dépanner à l'aide de compteurs

Vérifiez les compteurs AppFlow suivants pour tout problème lié à AppFlow ou Web Insight.

COMPTEUR	DESCRIPTION
`appflow_tot_record_drop`	Enregistrements AppFlow abandonnés en raison d'un collecteur non valide. Cela se produit généralement lorsque la configuration du collecteur change et que les connexions existantes utilisent l'ancienne configuration du collecteur.
`lstream_tot_trans_written`	Ce compteur doit s'incrémenter pour chaque transaction à enregistrer.
`lstream_sent`	Ce compteur s'incrémente pour chaque journal de transaction envoyé.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Afficher les analyses pour les transactions web

L'analyse des transactions web vous permet d'afficher les transactions détaillées pour :

- Temps de réponse > 500 ms
- Erreurs 5xx

Remarque :

> Vous ne pouvez afficher que quelques exemples de transactions 2xx pour l'application sélectionnée.

Prérequis :

Pour afficher l'analyse des transactions web, vous devez :

- Activer l'analyse.
- Modifiez les **Paramètres des transactions web** pour afficher les 2xx. Accédez à **Paramètres** > **Paramètres d'analyse**, sélectionnez **Activer les fonctionnalités pour l'analyse**, puis sélectionnez **Tout**.



Transactions web détaillées

Cette fonctionnalité vous permet non seulement d'examiner les transactions détaillées, mais aussi de comprendre visuellement la métrique du temps de réponse répartie entre le client, NetScaler et le serveur.

Remarque

> Dans certains scénarios, NetScaler pourrait ne pas être en mesure de calculer les valeurs RTT pour certaines transactions. Pour ces transactions, NetScaler Console affiche les valeurs RTT comme

- **NA** – S'affiche lorsque l'instance NetScaler ne peut pas calculer le RTT.
- **< 1ms** – S'affiche lorsque l'instance NetScaler calcule le RTT en décimales entre 0 ms et 1 ms. Par exemple, 0,22 ms.

Vous pouvez accéder au **Résumé des transactions** pour :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Applications** - Accédez à **Applications** > **Tableau de bord**, sélectionnez une application et cliquez sur **Journal des transactions**.

  

- **Applications Kubernetes** - Accédez à **Applications** > **Graphe de services**, cliquez sur un service et sélectionnez **Journaux des transactions**.

  

  La page **Résumé des transactions** s'affiche pour l'application sélectionnée.

  

Passez le pointeur de la souris sur **Réponse de l'application** pour afficher des détails tels que le RTT et le temps de traitement de l'instance NetScaler et du serveur.

L'exemple suivant vous aide à analyser que le problème provient du serveur. Le temps de réponse du serveur indique 10 secondes.



Vous pouvez également faire glisser et sélectionner pour afficher les transactions pour une durée spécifique.



Afficher les événements

Vous pouvez afficher les informations détaillées sur un événement particulier. Dans le panneau **Résumé des transactions**, vous pouvez filtrer les résultats en sélectionnant les options de chaque métrique.

Par exemple, supposons que vous souhaitiez afficher les transactions 4xx.

Dans le panneau **Résumé des transactions**, cliquez sur **Code de réponse**, puis sélectionnez **404** pour afficher le résultat.



Cliquez sur une transaction pour afficher les détails qui présentent les informations de métriques du client au serveur.



Pour les transactions présentant des erreurs SSL, les détails sont affichés pour le client et le serveur. Les métriques SSL suivantes sont affichées :

- Version du protocole SSL
- Échec frontal SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Force du chiffrement SSL
- Force de la clé SSL
- Type de certificat SSL

Vous pouvez également cliquer sur les **métriques SSL Frontend** et **SSL Backend** dans le panneau **Résumé des transactions** pour filtrer les résultats.

Pour filtrer les résultats, sélectionnez les options disponibles sous **Résumé des transactions**.

- **Navigateur** : Les types de navigateurs utilisés par les clients. Par exemple : Chrome, Firefox.
- **Système d'exploitation client** : Le système d'exploitation client basé sur les détails de l'agent utilisateur du navigateur. Par exemple : Windows
- **Appareil** : Les appareils basés sur les détails de l'agent utilisateur du navigateur. Par exemple : Tablette, Mobile.
- **Type de requête** : Le type de requête de transaction. Par exemple : GET.
- **Code de réponse** : Le code de réponse reçu du serveur. Par exemple : 501, 404, 200.
- **Type de contenu de réponse** : Le type de contenu de la transaction. Si la requête du client est pour text/html, alors la réponse du serveur doit être text/html.
- **Version du protocole SSL frontal** : La version du protocole SSL utilisée par les clients. Par exemple : SSLv3.
- **Force du chiffrement SSL frontal** : La force du chiffrement basée sur la taille de la clé du certificat SSL, telle que élevée, moyenne et faible.
- **Force de la clé SSL frontale** : La force du chiffrement SSL est calculée à partir de la taille de la clé du certificat SSL. La longueur de la clé définit la sécurité de l'algorithme SSL. Par exemple : 2048
- **Échec SSL frontal** : Le message d'erreur de la poignée de main SSL frontale. Par exemple : SSL CLIENTAUTH FAILURE
- **Type de certificat SSL frontal** : Le type de certificat utilisé par le client. Par exemple : RSA, DSA, ECDSA, DH.
- **Version du protocole SSL dorsal** : Les protocoles SSL utilisés par le serveur. Par exemple : SSLv3
- **Force du chiffrement SSL dorsal** : La force du chiffrement basée sur la taille de la clé du certificat SSL, telle que élevée, moyenne et faible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Force de la clé SSL dorsale** : La force du chiffrement SSL est calculée à partir de la taille de la clé du certificat SSL. La longueur de la clé définit la sécurité de l'algorithme SSL. Par exemple : 2048
- **Type de certificat SSL de backend** : Le type de certificat utilisé par le serveur. Par exemple : RSA, DSA, ECDSA, DH.

Ajouter des colonnes dans la liste des événements

Vous pouvez cliquer sur le bouton

pour choisir la liste des options et cliquer sur **Ajouter des colonnes** pour afficher les détails.

Recherche avancée

Le résumé des transactions comporte également une zone de texte de recherche et une liste de durées, où vous pouvez afficher les événements selon vos besoins. Lorsque vous placez le curseur dans la zone de recherche, celle-ci vous propose une liste de suggestions de recherche. Vous pouvez également utiliser des opérateurs dans vos requêtes de recherche pour affiner votre recherche.

Voici les opérateurs que vous pouvez utiliser pour vos requêtes de recherche :

OPÉRATEURS	DESCRIPTION	EXEMPLE	SORTIE
=	Égal à une certaine valeur	Serveur virtuel = test	Affiche l'événement pour le serveur virtuel nommé « test ».
>	Supérieur à une certaine valeur	App-Response-Time > 500	Affiche les événements pour les applications dont le temps de réponse est supérieur à 500 ms
<	Inférieur à une certaine valeur	App-Response-Time < 300	Affiche les événements pour les applications dont le temps de réponse

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPÉRATEURS	DESCRIPTION	EXEMPLE	SORTIE
			est inférieur à 300 ms
>=	Supérieur ou égal à une certaine valeur	Total-Bytes >= 1024	Affiche les événements pour les transactions supérieures ou égales à 1 Ko
<=	Inférieur ou égal à une certaine valeur	Total-Bytes <= 1024	Affiche les événements pour les transactions inférieures ou égales à 1 Ko
!=	Différent d'une certaine valeur	Response-code != 200	Affiche les événements avec toutes les transactions, à l'exception des transactions échouées.
~	Contient une certaine valeur	Serveur virtuel ~ mas	Affiche les événements pour les serveurs virtuels dont le nom est mas.

Par exemple, considérons un scénario où vous souhaitez générer des événements pour un total d'octets inférieur à 300 octets. Vous devez spécifier les requêtes de recherche comme suit :

1. Spécifiez le mot requis dans la zone de recherche pour obtenir les suggestions associées.

   

2. Sélectionnez **Total-Bytes**, cliquez à nouveau sur la zone de texte de recherche, puis sélectionnez **<**.

   

3. Saisissez la valeur 300.

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Sélectionnez la période et cliquez sur **Rechercher** pour afficher les événements en fonction de votre requête de recherche.

   Le résultat de la recherche s'affiche.

   

Enregistrer la recherche

Après avoir utilisé les suggestions et les opérateurs, vous pouvez enregistrer la requête de recherche. Vous pourrez ensuite l'utiliser ultérieurement à partir de la liste, au lieu d'utiliser à nouveau les suggestions et les opérateurs.

- Pour enregistrer une requête de recherche, cliquez sur l'icône de signet, spécifiez un nom de votre choix, puis cliquez sur **Enregistrer**.

  

- Pour utiliser la requête de recherche de la liste, cliquez sur l'icône et sélectionnez la requête de recherche dans la liste pour afficher les résultats.

  

- Pour supprimer la requête de recherche, cliquez sur l'icône, passez le pointeur de la souris sur la requête de recherche enregistrée, cliquez sur **Supprimer**.

  

  Vous pouvez également cliquer sur l'icône de signet et cliquer sur **Supprimer**.

  

Exporter les données

Vous pouvez exporter les données d'analyse des transactions web pour la durée sélectionnée en cliquant sur l'icône **Exporter**. Vous pouvez exporter aux formats PDF, PNG, JPEG et CSV. L'option **Exporter** vous permet d'effectuer l'une des opérations suivantes :

- Sélectionnez **Exporter maintenant** pour afficher et exporter le rapport au format PDF, JPEG, PNG ou CSV.
- Sélectionnez l'onglet **Planifier l'exportation** pour planifier le rapport quotidiennement, hebdomadairement ou mensuellement et envoyer le rapport par e-mail ou par message Slack.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Procédures détaillées pour configurer une topologie à deux niveaux ou de maillage de services léger

Exigences logicielles

DISTRIBUTION KUBERNETES	VERSION DE KUBERNETES	INTERFACES RÉSEAU DE CONTENEUR (CNI)	VERSION DE CPX	VERSION DE CIC	VERSION DE NETSCALER CONSOLE	VERSION DE L'AGENT NETSCALER
Code source ouvert	v1.16.3	Flannel	13.0–41.28	1.5.25	13.0–47.22	13.0–47.22

Avant de commencer

Vous pouvez afficher le graphique de service à l'aide des scénarios suivants :

- NetScaler Console et cluster Kubernetes sur le même réseau (par exemple, NetScaler Console et cluster Kubernetes hébergés sur Citrix Hypervisor).
- NetScaler Console et cluster Kubernetes sur un réseau différent. Dans ce scénario, vous devez configurer un agent sur site et enregistrer l'agent sur le réseau où le cluster Kubernetes est hébergé.

Pour utiliser le graphique de service dans NetScaler Console, assurez-vous d'avoir :

- Un cluster Kubernetes avec NetScaler CPX comme proxy. Pour plus d'informations, consultez NetScaler Ingress Controller.
- Configuré des routes statiques sur NetScaler Console pour permettre la communication entre NetScaler Console et NetScaler CPX
- Téléchargé les exemples de fichiers de déploiement depuis le référentiel GitHub.
- Ajouté les paramètres requis dans le fichier YAML CPX pour assurer l'enregistrement réussi du CPX auprès de NetScaler Console.
- Ajouté un cluster Kubernetes dans NetScaler Console.
- Déployé une application de microservice exemple.
- Déployé NetScaler CPX et enregistré le CPX auprès de NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Activé **Sélection automatique des serveurs virtuels** pour licencier les serveurs virtuels.
- Modifié les **Paramètres de transaction Web** à **Tous** pour que l'agent NetScaler obtienne les transactions HTTP.
- Mis à jour le fichier **lstream.conf** et modifié le paramètre TCP sur **All** pour que l'agent NetScaler obtienne les métriques TCP.

Exigences logicielles

DISTRIBUTION KUBERNETES	VERSION DE KUBERNETES	INTERFACES RÉSEAU DE CONTENEUR (CNI)	VERSION DE CPX	VERSION DE CIC	VERSION DE NETSCALER CONSOLE	VERSION DE L'AGENT NETSCALER
Source ouverte	v1.16.3	Flannel	13.0–41.28	1.5.25	13.0–47.22	13.0–47.22

Avant de commencer

Vous pouvez afficher le graphique de service à l'aide des scénarios suivants :

- NetScaler Console et cluster Kubernetes sur le même réseau (par exemple, NetScaler Console et cluster Kubernetes hébergés sur Citrix Hypervisor).
- NetScaler Console et cluster Kubernetes sur un réseau différent. Dans ce scénario, vous devez configurer un agent sur site et enregistrer l'agent sur le réseau où le cluster Kubernetes est hébergé.

Pour utiliser le graphique de service dans NetScaler Console, assurez-vous d'avoir :

- Un cluster Kubernetes avec NetScaler CPX comme proxy. Pour plus d'informations, consultez NetScaler Ingress Controller.
- Configuré des routes statiques sur NetScaler Console pour permettre la communication entre NetScaler Console et NetScaler CPX
- Téléchargé les fichiers de déploiement d'exemple depuis le référentiel GitHub.
- Ajouté les paramètres requis dans le fichier YAML CPX pour assurer l'enregistrement réussi de CPX auprès de NetScaler Console.
- Ajouté le cluster Kubernetes dans NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Déployé une application de microservice d'exemple.
- Déployé NetScaler CPX et enregistré CPX dans NetScaler Console.
- Activé la **Sélection automatique des serveurs virtuels** pour licencier les serveurs virtuels.
- Modifié les **Paramètres de transaction Web** en **Tous** pour que l'agent NetScaler obtienne les transactions HTTP.
- Mis à jour le fichier **lstream.conf** et modifié le paramètre TCP sur **All** pour que l'agent NetScaler obtienne les métriques TCP.

Configurer les routes statiques dans NetScaler Console

À l'intérieur du cluster Kubernetes, tous les pods conteneurisés utilisent un réseau superposé. Il n'est pas possible d'établir la communication directement à l'aide de ces adresses IP privées. Pour permettre la communication entre NetScaler Console et le cluster Kubernetes, vous devez configurer le routage statique dans NetScaler Console.

Remarque

> Si vous utilisez un agent sur site, assurez-vous de configurer les routes statiques sur l'agent. À l'aide d'un client SSH, connectez-vous à l'agent NetScaler et configurez les routes statiques.

Considérez que vous avez les adresses IP suivantes pour votre cluster Kubernetes :

- Maître Kubernetes – 101.xx.xx.112
- Nœud de travail Kubernetes 1 – 101.xx.xx.111
- Nœud de travail Kubernetes 2 – 101.xx.xx.110

Sur le maître Kubernetes, exécutez la commande suivante pour identifier le réseau de pods afin d'effectuer le routage statique :

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

Voici un exemple de sortie après l'exécution de la commande :

1. À l'aide d'un client SSH, connectez-vous à NetScaler Console
2. Configurez le routage statique à l'aide de la commande `route add -net <public IP address range> <Kubernetes IP address>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Par exemple :

```
route add -net 192.168.0.0/24 101.xx.xx.112
```

```
route add -net 192.168.1.0/24 101.xx.xx.111
```

```
route add -net 192.168.2.0/24 101.xx.xx.110
```

3. Vérifiez la configuration à l'aide de `netstat -rn`



4. Ajoutez ces commandes de routage dans le fichier `/mpsconfig/svm.conf`.

   a. Dans NetScaler Console, accédez au fichier **svm.conf** à l'aide de la commande suivante :

   ```
   vim /mpsconfig/svm.conf
   ```

   b. Ajoutez les routes statiques dans le fichier **svm.conf**.

   Par exemple, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Télécharger les fichiers de déploiement d'exemple depuis GitHub

1. Utilisez la commande **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git` pour cloner le référentiel GitHub sur le nœud maître.
2. Pour accéder aux fichiers YAML :

   ```
   cd citrix-k8s-ingress-controller/example/servicegraph-demo/
   ```

Ajouter des paramètres dans le fichier YAML CPX

REMARQUE

Si vous utilisez CPX 58.x ou version ultérieure, vous devez utiliser le mot de passe non-nsroot lors de l'enregistrement auprès de l'agent. Pour garantir la sécurité, les versions 61.x ou ultérieures de l'agent NetScaler nécessitent un changement de mot de passe obligatoire. Si votre agent NetScaler est mis à niveau vers la version 61.x ou la dernière version, vous devez vous assurer d'utiliser la version **CPX 58.x ou ultérieure**.

Vous devez inclure les paramètres suivants dans le fichier `cpx.yaml` pour garantir l'enregistrement de CPX auprès de NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"

  value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

- name: "NS_HTTP_PORT"

  value: "9080"

- name: "NS_HTTPS_PORT"

  value: 9443"

- name: "NS_MGMT_USER"

  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – Indique l'adresse IP de NetScaler Console

  REMARQUE

  Si un agent est utilisé, cela indique l'adresse IP de l'agent.

- **NS_MGMT_FINGER_PRINT** – Indique l'authentification pour CPX dans NetScaler Console. Pour obtenir l'empreinte numérique :

  a. Dans NetScaler Console, accédez à **Paramètres > Administration**

  b. Sous **Configurations système**, cliquez sur **Afficher l'empreinte numérique ADM**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque :

> Si vous avez configuré un agent sur site, accédez à **Infrastructure > Instances > Agents**, sélectionnez l'agent, puis cliquez sur **Afficher l'empreinte numérique**.

- **NS_HTTP_PORT** – Indique le port HTTP pour la communication
- **NS_HTTPS_PORT** – Indique le port HTTPS pour la communication
- **NS_MGMT_USER** - Indique le nom d'utilisateur
- **NS_MGMT_PASS** - Indique le mot de passe. Spécifiez un mot de passe de votre choix
- **LOGSTREAM_COLLECTOR_IP** – Indique l'adresse IP de l'agent NetScaler, où le protocole **Logstream** doit être activé pour transférer les données de journal de CPX vers NetScaler Console

Ajouter une instance VPX, SDX, MPX ou BLX dans NetScaler Console

Pour obtenir les analyses de l'instance NetScaler de niveau 1 dans le graphique de service, vous devez ajouter l'instance VPX/SDX/MPX/BLX dans NetScaler Console et activer **Web Insight**.

1. Accédez à **Infrastructure > Instances > NetScaler**
2. Cliquez sur l'option **Ajouter** pour ajouter l'instance. Pour plus d'informations, consultez Ajouter des instances dans NetScaler Console
3. Après avoir ajouté l'instance, sélectionnez le serveur virtuel et activez **Web Insight**. Pour plus d'informations, consultez Gérer les licences et activer les analyses sur les serveurs virtuels

Ajouter un cluster Kubernetes dans NetScaler Console

Pour ajouter le cluster Kubernetes :

1. Connectez-vous à NetScaler Console avec les informations d'identification de l'administrateur.
2. Accédez à **Orchestration** > **Kubernetes** > **Cluster**. La page Clusters s'affiche.
3. Cliquez sur **Ajouter**.
4. Dans la page **Ajouter un cluster**, spécifiez les paramètres suivants :
    a. **Nom** - Spécifiez un nom de votre choix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **URL du serveur API** - Vous pouvez obtenir les détails de l'URL du serveur API à partir du nœud maître Kubernetes.

   i. Sur le nœud maître Kubernetes, exécutez la commande `kubectl cluster-info`.

   ii. Saisissez l'URL qui s'affiche pour **« Le maître Kubernetes est en cours d'exécution à l'adresse. »**

c. **Jeton d'authentification** - Spécifiez le jeton d'authentification. Le jeton d'authentification est requis pour valider l'accès à la communication entre le cluster Kubernetes et NetScaler Console. Pour générer un jeton d'authentification :

   Sur le nœud maître Kubernetes :

   i. Utilisez le fichier YAML suivant pour créer un compte de service :

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

   ii. Exécutez `kubectl create -f <yaml file>`.

   Le compte de service est créé.

   iii. Exécutez `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` pour lier le rôle de cluster au compte de service.

   Le compte de service dispose désormais d'un accès à l'échelle du cluster.

   Un jeton est automatiquement généré lors de la création du compte de service.

   iv. Exécutez `kubectl describe sa <name>` pour afficher le jeton.

   v. Pour obtenir la chaîne secrète, exécutez `kubectl describe secret <token-name>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Sélectionnez l'agent dans la liste.

Remarque

> Si vous utilisez un agent sur site, assurez-vous de sélectionner le même agent que celui que vous avez ajouté dans le fichier YAML du CPX.

e. Cliquez sur **Créer**.



Déployer un exemple d'application de microservice

Sur le nœud maître :

1. Exécutez `kubectl create -f namespace.yaml` pour créer un espace de noms.
2. Déployez les microservices `hotdrink`, l'entrée et les secrets à l'aide des commandes suivantes :

```
kubectl create -f team_hotdrink.yaml -n sg-demo
```

```
kubectl create -f hotdrink-secret.yaml -n sg-demo
```

Déployer CPX et enregistrer CPX dans NetScaler Console

1. Exécutez `kubectl create -f rbac.yaml` pour déployer le rôle de cluster et la liaison de cluster.
2. Exécutez `kubectl create -f cpx.yaml -n sg-demo` pour déployer CPX.

Après le déploiement, l'enregistrement CPX est effectué automatiquement.

Activer la sélection automatique des serveurs virtuels pour la gestion des licences

Remarque

> Assurez-vous de disposer de licences de serveur virtuel suffisantes. Pour plus d'informations, consultez Licences

Après avoir ajouté un cluster Kubernetes dans NetScaler Console, vous devez vous assurer de sélectionner automatiquement les serveurs virtuels pour la gestion des licences. Les serveurs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

virtuels doivent être sous licence pour afficher les données dans Service Graph. Pour sélectionner automatiquement les serveurs virtuels :

1. Accédez à **Paramètres > Configuration des licences et de l'analyse**.
2. Sous **Résumé des licences de serveur virtuel**, activez **Sélection automatique des serveurs virtuels** et **Sélection automatique des serveurs virtuels non adressables**.



Activer les paramètres de transaction Web et de transaction TCP

Après avoir ajouté le cluster Kubernetes et activé la sélection automatique des serveurs virtuels, définissez les **Paramètres de transaction Web** et les **Paramètres de transaction TCP** sur **Tous**.

1. Accédez à **Paramètres > Paramètres d'analyse**.

   La page **Paramètres d'analyse** s'affiche.
2. Cliquez sur **Activer les fonctionnalités pour l'analyse**.
3. Sous **Paramètres de transaction Web**, sélectionnez **Tous**.
4. Sous **Paramètres de transaction TCP**, sélectionnez **Tous**.



5. Cliquez sur **OK**.

Envoyer du trafic vers les microservices

Ensuite, vous devez envoyer du trafic vers les microservices pour que le graphique de service soit renseigné dans NetScaler Console.

1. Exécutez `kubectl get svc -n sg-demo` pour exposer CPX via NodePort.



2. Modifiez le fichier **etc/host** et créez une entrée IP de domaine pour `hotdrink.beverages.com`

   Vous pouvez maintenant accéder au microservice en utilisant `https://hotdrink.beverages.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Procédures détaillées pour configurer la topologie de maillage de services

Les prérequis pour déployer la topologie de maillage de services sont disponibles à l'adresse Configuration du graphe de services.

Configurer les routes statiques dans NetScaler Console

À l'intérieur du cluster Kubernetes, tous les pods conteneurisés utilisent un réseau superposé. Il n'est pas possible d'établir directement la communication à l'aide de ces adresses IP privées. Pour permettre la communication entre NetScaler Console et le cluster Kubernetes, vous devez configurer le routage statique dans NetScaler Console.

Remarque

> Si vous utilisez un agent sur site, assurez-vous de configurer les routes statiques sur l'agent. À l'aide d'un client SSH, connectez-vous à l'agent NetScaler et configurez les routes statiques.

Considérez que vous avez les adresses IP suivantes pour votre cluster Kubernetes :

- Maître Kubernetes – 101.xx.xx.112
- Travailleur Kubernetes 1 – 101.xx.xx.111
- Travailleur Kubernetes 2 – 101.xx.xx.110

Sur le maître Kubernetes, exécutez la commande suivante pour identifier le réseau de pods afin d'effectuer le routage statique :

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

Voici un exemple de sortie après l'exécution de la commande :

1. À l'aide d'un client SSH, connectez-vous à NetScaler Console
2. Configurez le routage statique à l'aide de la commande `route add -net <public IP address range> <Kubernetes IP address>`

   Par exemple :

   ```
   route add -net 192.168.0.0/24 101.xx.xx.112
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`route add -net 192.168.1.0/24 101.xx.xx.111`

`route add -net 192.168.2.0/24 101.xx.xx.110`

3. Vérifiez la configuration à l'aide de `netstat -rn`



4. Ajoutez ces commandes de routage dans le fichier `/mpsconfig/svm.conf`.

   a. Dans NetScaler Console, accédez au fichier **svm.conf** à l'aide de la commande suivante :

      `vim /mpsconfig/svm.conf`

   b. Ajoutez les routes statiques dans le fichier **svm.conf**.

      Par exemple, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Configurez les paramètres requis

Dans le maître Kubernetes :

1. Créez un secret avec les identifiants de l'agent dans chaque espace de noms où CPX est déployé en tant que passerelle d'entrée / sidecar.

   `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>`

2. `helm repo add citrix https://citrix.github.io/citrix-helm-charts/`

3. Déployer le NetScaler CPX en tant que passerelle d'entrée

   `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   Le tableau suivant répertorie les paramètres configurables dans le chart Helm et ses valeurs par défaut :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRE	DESCRIPTION	PAR DÉFAUT	FACULTATIF/ OBLIGATOIRE (HELM)
citrixCPX	NetScaler CPX	FALSE	Obligatoire pour NetScaler CPX
xDSAdaptor.image	Image du conteneur d'adaptateur Citrix xDS	quay.io/citrix/citrix-istio-adaptor:1.2.1	Obligatoire
ADMSettings.ADMIP	Adresse IP de NetScaler Console	vide	Obligatoire pour NetScaler CPX
ADMSettings.ADMFingerPrint	L'empreinte digitale de NetScaler Console. Accédez à **Paramètres > Administration**, puis cliquez sur **Afficher l'empreinte digitale** sous **Configurations système**	vide	Facultatif
ingressGateway.EULA	Conditions générales du contrat de licence utilisateur final (CLUF). Si oui, l'utilisateur accepte les conditions générales du CLUF.	NON	Obligatoire pour NetScaler CPX
ingressGateway.image	Image de NetScaler CPX désignée pour fonctionner comme passerelle d'entrée (Ingress Gateway)	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30	Obligatoire pour NetScaler CPX

4. Déployer l'injecteur SideCar Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --version 1.2.1 --namespace <namespace> set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<xx.xx.xx.xx> citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30
```

Le tableau suivant répertorie les paramètres configurables dans le graphique Helm et ses valeurs par défaut :

PARAMÈTRE	DESCRIPTION	VALEUR PAR DÉFAUT
ADMSettings.ADMIP	L'adresse IP de la console NetScaler	NUL
cpxProxy.image	Image NetScaler CPX utilisée comme proxy sidecar	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30
cpxProxy.imagePullPolicy	Politique de tirage d'image pour NetScaler	IfNotPresent
cpxProxy.EULA	Conditions générales du Contrat de Licence Utilisateur Final (CLUF). Si oui, l'utilisateur accepte les conditions générales du CLUF.	NON
cpxProxy.cpxSidecarMode	Variable d'environnement pour NetScaler CPX. Elle indique si NetScaler CPX fonctionne en mode sidecar ou non.	OUI

5. Définissez l'étiquette sur tout espace de noms nécessitant l'injection de sidecar CPX.

```
kubectl label namespace <app-namespace> cpx-injection=enabled
```

Après avoir effectué les étapes 3 et 5, vous pouvez voir que le NetScaler CPX est enregistré dans NetScaler Console.

Déployer une application exemple

Considérez que vous souhaitez déployer les applications suivantes :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Effectuez la procédure suivante pour déployer une application exemple :

1. `kubectl create namespace citrix-system`
2. `kubectl create namespace bookinfo`
3. `kubectl label namespace bookinfo cpx-injection=enabled`
4. `kubectl create secret generic admlogin --from-literal=username=<uername> --from-literal=password=<password> -n citrix-system`

   Remarque

   Vous pouvez donner un nom d'utilisateur et un mot de passe de votre choix.

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   Remarque

   Vous pouvez donner un nom d'utilisateur et un mot de passe de votre choix.

6. `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace citrix-system --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSetting IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   Remarque

   Vous devez fournir l'empreinte de votre console et l'adresse IP de l'agent ou de la console

7. `helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --namespace citrix-system --set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<ADM agent IP address>,cpxProxy.image=quay.io/citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remarque

Vous devez fournir l'empreinte digitale de votre console et l'adresse IP de l'agent ou de la console

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

Ajouter un cluster Kubernetes dans NetScaler Console

Pour ajouter le cluster Kubernetes :

1. Connectez-vous à NetScaler Console avec les informations d'identification de l'administrateur.
2. Accédez à **Orchestration** > **Kubernetes** > **Cluster**. La page Clusters s'affiche.
3. Cliquez sur **Ajouter**.
4. Dans la page **Ajouter un cluster**, spécifiez les paramètres suivants :
   a. **Nom** - Spécifiez un nom de votre choix.
   b. **URL du serveur API** - Vous pouvez obtenir les détails de l'URL du serveur API à partir du nœud maître Kubernetes.
      i. Sur le nœud maître Kubernetes, exécutez la commande `kubectl cluster-info`.
      ii. Saisissez l'URL qui s'affiche pour **« Le maître Kubernetes est en cours d'exécution à. »**
   c. **Jeton d'authentification** - Spécifiez le jeton d'authentification. Le jeton d'authentification est requis pour valider l'accès à la communication entre le cluster Kubernetes et NetScaler Console. Pour générer un jeton d'authentification :

      Sur le nœud maître Kubernetes :

      i. Utilisez le fichier YAML suivant pour créer un compte de service :

```
apiVersion: v1

kind: ServiceAccount

metadata:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: <name>

namespace: <namespace>
```

ii. Exécutez `kubectl create -f <yaml file>`.

Le compte de service est créé.

iii. Exécutez `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` pour lier le rôle de cluster au compte de service.

Le compte de service dispose désormais d'un accès à l'échelle du cluster.

Un jeton est automatiquement généré lors de la création du compte de service.

iv. Exécutez `kubectl describe sa <name>` pour afficher le jeton.

v. Pour obtenir la chaîne secrète, exécutez `kubectl describe secret <token-name>`.

d. Sélectionnez l'agent dans la liste.

Remarque

> Si vous utilisez un agent, assurez-vous de sélectionner le même agent que celui que vous avez ajouté dans le fichier YAML CPX.

e. Cliquez sur **Créer**.

Activer la sélection automatique des serveurs virtuels pour la licence

Remarque

> Assurez-vous de disposer de licences de serveur virtuel suffisantes. Pour plus d'informations, consultez Licences

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Après avoir ajouté un cluster Kubernetes dans NetScaler Console, vous devez vous assurer de sélectionner automatiquement les serveurs virtuels pour l'octroi de licences. Les serveurs virtuels doivent être sous licence pour afficher les données dans Service Graph. Pour sélectionner automatiquement les serveurs virtuels :

1. Accédez à **Paramètres > Configuration des licences et de l'analyse**.
2. Sous **Résumé des licences de serveur virtuel**, activez **Sélection automatique des serveurs virtuels** et **Sélection automatique des serveurs virtuels non adressables**.



Activer les paramètres de transaction Web et de transaction TCP

Après avoir ajouté le cluster Kubernetes et activé la sélection automatique des serveurs virtuels, définissez les **Paramètres de transaction Web** et les **Paramètres de transaction TCP** sur **Tous**.

1. Accédez à **Paramètres > Paramètres d'analyse**.

   La page **Paramètres d'analyse** s'affiche.
2. Cliquez sur **Activer les fonctionnalités pour l'analyse**.
3. Sous **Paramètres de transaction Web**, sélectionnez **Tous**.
4. Sous **Paramètres de transaction TCP**, sélectionnez **Tous**.



5. Cliquez sur **OK**.

Envoyer du trafic aux microservices

Ensuite, vous devez envoyer du trafic aux microservices pour que le graphique de service soit renseigné dans NetScaler Console.

1. Déterminer l'adresse IP et le port Ingress

```
export INGRESS_HOST=$(kubectl get pods -l app=citrix-ingressgateway -n citrix-system -o 'jsonpath={.items[0].status.hostIP}')
```

```
export INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')
```

```
export SECURE_INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Accédez à l'application front-end Bookinfo à l'aide de cURL. Le service `productpage` doit renvoyer une réponse 200 OK.

   ```
   curl -kv https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage
   ```

   ```
   curl -v http://$INGRESS_HOST:$INGRESS_PORT/productpage
   ```

3. Visitez `https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage` depuis un navigateur.

   La page **Bookinfo** s'affiche.

4. Assurez-vous que $INGRESS_HOST et $SECURE_INGRESS_PORT sont remplacés par une adresse IP et une valeur de port.

Après avoir envoyé du trafic aux microservices, le graphique de service est renseigné en 10 minutes environ.

À l'aide du graphique de service, vous pouvez analyser divers détails de service tels que les métriques, les erreurs, etc. Pour plus d'informations, consultez Graphique de service.

Gouvernance des données (pour NetScaler Console entre les versions 14.1-8.x et 14.1-21.x)

Cloud Connect permet à Citrix Cloud de collecter les données de licence, de configuration et d'utilisation pour la conformité des licences, et de gérer, mesurer et améliorer le service. À partir de la version 14.1-8.x ou ultérieure, vous pouvez configurer Cloud Connect pour établir une connexion entre le service NetScaler Console et NetScaler Console sur site. En activant Cloud Connect :

- Les données obligatoires de licence et d'utilisation pour la conformité des licences flexibles sont collectées.
- Vous pouvez obtenir la fonctionnalité **Security Advisory** dans NetScaler Console sur site. Pour plus d'informations, consultez Cloud Connect.

Catégories de données

Le tableau suivant fournit les détails des paramètres collectés après l'activation de Cloud Connect :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIES	DESCRIPTION	À QUOI SERT-IL ?	OBLIGATOIRE/ FACULTATIF
Données de télémétrie de licence	Informations sur les droits de licence, l'utilisation, les données de déploiement NetScaler de haut niveau et les données d'utilisation des fonctionnalités NetScaler.	Conformité des licences et gestion, mesure et amélioration du service.	Obligatoire
Données d'utilisation des fonctionnalités	Informations sur le déploiement de la Console et les données d'utilisation des fonctionnalités de la Console.	Pour gérer, mesurer et améliorer le service.	Facultatif

Gouvernance des données (pour NetScaler ADM 14.1-4.42 ou versions antérieures)

Si votre NetScaler ADM est en version 14.1-4.x ou inférieure, vous pouvez créer une identité client sur Citrix Cloud pour envoyer des statistiques importantes sur la santé, l'état et d'autres métriques de l'ADM depuis le déploiement sur site vers le compte Citrix Cloud. Citrix collecte des statistiques pour comprendre l'utilisation de NetScaler ADM.

- **Créer une identité client sur Citrix Cloud™** - Pour envoyer des statistiques importantes sur la santé, l'état et d'autres métriques de l'ADM depuis le déploiement sur site vers le compte Citrix Cloud.

  Après avoir créé une identité client, le « Cloud Connect » établit la connexion entre ADM sur site et le service NetScaler® Console en créant un compte Citrix Cloud. Voir, Configurer l'identité client.
- **Configurer les scripts de maintenance** - Pour optimiser la base de données. L'optimisation de la base de données peut créer des tables, modifier des colonnes, et plus encore. La même fonctionnalité « Cloud Connect » est utilisée pour configurer les scripts de maintenance. Voir Optimisation de la base de données à l'aide de scripts de maintenance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Programme d'amélioration de l'expérience utilisateur client (CUXIP)** - Ce programme est activé par défaut. Il collecte les données d'utilisation de NetScaler ADM. Ces données permettent d'optimiser l'expérience ADM grâce à des flux de travail guidés, des articles de recherche, des notifications de produits, des commentaires, des enquêtes, etc. Voir, Programme d'amélioration de l'expérience utilisateur client.

Configurer l'identité client

NetScaler Console exige que vous vous authentifiiez sur l'interface graphique d'ADM avant de commencer à accéder aux informations. Il est impératif de vous inscrire aux services Citrix Cloud avant de vous authentifier sur ADM. Fournissez les informations d'identification de l'utilisateur Citrix Cloud sur l'interface graphique d'ADM. Pour plus d'informations, consultez S'inscrire à Citrix Cloud.

Il existe différentes manières de vous authentifier sur NetScaler ADM. Les sections suivantes décrivent les flux de travail si vous êtes un nouvel utilisateur ou un utilisateur existant sur ADM.

Flux de travail 1 - Si vous êtes un nouvel utilisateur

1. Terminez l'installation de NetScaler ADM sur l'hyperviseur sélectionné.
2. Configurez les différentes adresses IP requises.
3. Dans un navigateur Web, saisissez l'adresse IP de NetScaler ADM.
4. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.

   La page **Configurer l'identité client** s'ouvre, où vous devez vous identifier avec vos informations d'identification Citrix Cloud.

   Si vous n'avez pas créé de compte sur Citrix Cloud, cliquez sur Citrix Cloud pour vous inscrire.
5. Cliquez sur **Authentifier** et indiquez l'adresse e-mail que vous avez utilisée pour vous inscrire à Citrix Cloud.
6. Cochez la case en regard de **J'accepte de partager les données** pour la télémétrie et cliquez sur **Soumettre**.

Flux de travail 2 - si vous êtes un utilisateur existant effectuant une mise à niveau vers la dernière version d'ADM

1. Après la mise à niveau de NetScaler ADM vers la dernière version, dans un navigateur Web, saisissez l'adresse IP de NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification de l'administrateur.
3. La page **Configurer l'identité du client** s'ouvre, où vous devez vous identifier avec vos informations d'identification Citrix Cloud.

   Si vous n'avez pas créé de compte sur Citrix Cloud, cliquez sur Citrix Cloud pour vous inscrire.
4. Cliquez sur **Authentifier** et indiquez l'adresse e-mail que vous avez utilisée pour vous inscrire à Citrix Cloud.
5. Cochez la case en regard de « J'accepte de partager les données pour la télémétrie » et cliquez sur Soumettre.

En tant qu'utilisateur existant, vous pouvez également configurer votre identité sur ADM ultérieurement de l'une des deux manières suivantes :

- Accédez à **Paramètres > Administration système**, puis cliquez sur **Authentification**.
- Cliquez sur le symbole du cloud en haut à droite de l'interface graphique d'ADM. Après une authentification réussie, le `X` se transforme en coche verte.

REMARQUE

Assurez-vous que les domaines suivants sont mis sur liste blanche :

- `*.citrixnetworkapi.net`
- `*.blob.core.windows.net`

En téléchargeant vos données sur NetScaler ADM et en utilisant les fonctionnalités de NetScaler ADM, vous acceptez et consentez à ce que Citrix puisse collecter, stocker, transmettre, maintenir, traiter et utiliser des informations techniques, utilisateur ou connexes concernant vos produits et services NetScaler.

Les informations reçues par Citrix sont toujours traitées conformément à la Politique de confidentialité de Citrix.com.

Diagnostics et collecte de données

NetScaler ADM collecte les données de télémétrie suivantes en utilisant l'identité du client :

- **Actions effectuées dans ADM** :
  - Actions effectuées à l'aide de l'interface UI/API de NetScaler ADM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Actions effectuées à l'aide de l'interface SDK de NetScaler ADM.
- Nombre d'opérations en une seule journée. Ce nombre inclut toute requête non-GET provenant de l'API ou de l'interface utilisateur.
- Nombre de mises à niveau NetScaler effectuées par ADM.

- **Informations sur la licence NetScaler ADM** : Nombre de serveurs virtuels autorisés.
- **Statistiques clés** :
  - Nombre total de règles d'événement.
  - Nombre total de StyleBooks définis par l'utilisateur.
  - Nombre d'applications gérées et personnalisées.
  - Nombre d'agents enregistrés.
  - Débit global sur le NetScaler (Rx+Tx).
  - Nombre d'instances gérées. Ce nombre inclut également les partitions d'administration.
  - Nombre d'administrateurs utilisant NetScaler ADM SaaS.
- **Géolocalisation de NetScaler ADM**
- **Informations de déploiement** : Ces informations incluent les types de déploiement tels que la haute disponibilité, la reprise après sinistre et les agents ADM.

Pourquoi les données sont-elles collectées ?

Les données de télémétrie collectées aident à :

- Recommander le dimensionnement et le déploiement corrects de NetScaler ADM.
- Résoudre les problèmes de manière proactive sur les déploiements ADM sur site.

Qui peut utiliser ces données ?

Citrix est le seul propriétaire des informations collectées. Citrix a accès/collecte les informations que vous nous fournissez volontairement. Nous ne vendons ni ne louons ces informations à quiconque. Nous ne partageons pas vos informations avec des tiers extérieurs à notre organisation, sauf si cela est nécessaire pour répondre à votre demande. Exemple : Pour expédier une commande ou pour résoudre des problèmes de manière proactive.

Combien de temps conservons-nous vos données ?

Généralement, nous stockons les données personnelles/d'utilisation tant que l'utilisateur utilise nos Services. Ou, nous avons un autre objectif pour le faire. Par la suite, les données ne sont plus

© 1997–2026 Citrix Systems, Inc. All rights reserved.

stockées au-delà de ce qui est requis ou permis par la loi ou nécessaire à des fins de rapports internes et de rapprochement.

Toutes les données de télémétrie sont stockées pendant une période ne dépassant pas 13 mois ou 396 jours.

Optimisation de la base de données à l'aide de scripts de maintenance

Les scripts de maintenance sont utilisés pour résoudre les problèmes liés à la base de données sur les déploiements ADM sur site. Le logiciel ADM télécharge automatiquement les scripts de maintenance de la base de données à partir du service ADM, offrant une résolution plus rapide des problèmes liés à la base de données. Auparavant, ces problèmes étaient résolus en exécutant manuellement les scripts.

Grâce à cette fonctionnalité, le déploiement ADM sur site télécharge périodiquement les scripts de maintenance de la base de données à partir du service ADM. Pour ce faire, assurez-vous de configurer l'identité du client.

Les scripts de maintenance s'exécutent quotidiennement et hebdomadairement. De plus, les scripts peuvent créer des tables ou ajouter ou supprimer des colonnes pour améliorer les performances de la base de données.

Programme d'amélioration de l'expérience utilisateur client

Chez Citrix Systems, notre objectif est d'offrir à nos utilisateurs une expérience produit engageante. Le **Programme d'amélioration de l'expérience utilisateur client (CUXIP)** utilise Pendo pour guider les utilisateurs à travers certaines tâches courantes mais détaillées en fournissant des articles de recherche, des guides intégrés à l'application, etc. Nous aidons également nos utilisateurs à rester informés de toutes les annonces récentes.

Quelles données d'utilisation sont collectées via CUXIP ?

Les données d'utilisation concernent toutes les actions de l'utilisateur. Également appelées données au niveau de l'événement, les données d'utilisation incluent tout, des pages que nos utilisateurs visitent sur un site Web au nombre de clics sur une certaine fonctionnalité. Les données d'utilisation sont des informations précieuses sur la façon dont les utilisateurs se déplacent dans nos applications. Ces données permettent d'optimiser l'expérience de nos utilisateurs.

Voici quelques-unes des données d'utilisation que nous collectons :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Détails des pages vues, temps passé sur chaque page.
- L'ID de visiteur est un identifiant anonymisé unique pour aider à identifier le nombre de visiteurs uniques sur une page.
- Statistiques d'enquête – score, vues, nombre de soumissions, etc.

Comment CUXIP vous aide-t-il ?

Nous utilisons les données d'utilisation pour améliorer votre expérience avec ADM. Voici quelques-unes des façons dont nous avons l'intention d'améliorer l'expérience utilisateur client :

- Workflows guidés intégrés à l'application et possibilité de rechercher des articles pertinents.
- Participez à une enquête depuis l'application pour aider à améliorer le produit.
- Restez informé des annonces récentes et autres notifications.
- Posez une question ou envoyez des commentaires à l'équipe produit.

Comment fonctionne CUXIP ?

L'appliance NetScaler ADM peut se trouver dans le réseau interne. Le navigateur doit disposer d'une connectivité Internet pour bénéficier de l'assistance guidée sur CUXIP.

Comment désactiver CUXIP sur mon ADM ?

Pour désactiver CUXIP, procédez comme suit dans l'interface graphique d'ADM :

1. Accédez à **Paramètres > Administration système**.
2. Dans **Paramètres CUXIP**, désactivez CUXIP.

Modifications de notre politique de confidentialité

Nous pouvons mettre à jour notre politique de confidentialité de temps à autre. Nous vous informerons des modifications en publiant la nouvelle politique de confidentialité sur cette page. Nous vous en informerons par e-mail et/ou par un avis bien visible sur notre Service, avant que le changement ne prenne effet, et nous mettrons à jour la « date d'entrée en vigueur » en haut de cette politique de confidentialité.

Il vous est conseillé de consulter régulièrement cette politique de confidentialité pour prendre connaissance des modifications. Les modifications apportées à cette politique de confidentialité prennent effet dès leur publication sur la page Politique de confidentialité de Citrix.

Références

Politique de confidentialité de Citrix : `<https://www.citrix.com/about/legal/privacy/>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Données de télémétrie facultatives pour Cloud Connect

Le tableau suivant affiche la liste des données facultatives collectées après l'activation de Cloud Connect :

PARAMÈTRES	DESCRIPTION
t_ten	Le nombre total de locataires connectés à NetScaler Console
déployer	Vérifie si le type de déploiement de NetScaler Console est autonome ou une paire HA
is_dr	Vérifie si le nœud de reprise après sinistre est configuré ou non
is_agt	Vérifie si l'agent est configuré ou non
is_cloud	Vérifie si le déploiement de NetScaler Console est un service NetScaler Console ou NetScaler Console sur site
is_cntr	Vérifie si le déploiement de NetScaler Console se trouve dans un cluster Kubernetes
plateforme	La plateforme où NetScaler Console est hébergé. Par exemple, Citrix Hypervisor
security_advisory_enabled	Vérifie si l'avis de sécurité est activé dans NetScaler Console sur site
total_users	Le nombre total d'utilisateurs locaux de NetScaler Console
total_gui_requests	Le nombre total d'utilisateurs connectés à l'interface graphique de NetScaler Console au cours des dernières 24 heures
total_api_requests	Le nombre total de requêtes via l'API vers NetScaler Console au cours des dernières 24 heures. Cela inclut également les utilisateurs de proxy distant (requêtes de l'agent).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_api_external_requests	Le nombre total de requêtes via l'API vers NetScaler Console qui excluent les requêtes de l'agent
total_success_preauth_requests	Le nombre total de requêtes réussies pour générer les jetons de pré-authentification
total_custom_apps	Le nombre total d'applications personnalisées dans NetScaler Console
total_managed_apps	Le nombre total d'applications gérées dans NetScaler Console
total_apps	Le nombre total d'applications dans NetScaler Console
total_custom_sites	Le nombre total de sites personnalisés configurés dans NetScaler Console
total_agents	Le nombre total d'agents configurés
total_active_agents	Le nombre total d'agents en état ACTIF
total_custom_event_rules	Le nombre total de règles d'événements personnalisées créées dans NetScaler Console
total_event_rules	Le nombre total de règles d'événement créées dans NetScaler Console
total_stylebook_config_store_count	Le nombre total de packs de configuration créés dans NetScaler Console
total_user_sb_stylebook_count	Le nombre total de packs de configuration personnalisés créés dans NetScaler Console
total_config_audit	Le nombre total de modèles d'audit de configuration configurés dans NetScaler Console
total_config_job	Le nombre total de tâches de configuration créées dans NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_ssl_certs	Le nombre total de certifications SSL créées/ modifiées/supprimées depuis NetScaler Console
total_network_report	Le nombre total de rapports réseau créés dans NetScaler Console
total_k8s	La NetScaler Console hébergée sur le cluster Kubernetes. Le nombre total de clusters Kubernetes.
total_ipam	Le nombre total de fournisseurs IPAM ajoutés dans NetScaler Console
total_rbac_groups	Le nombre total de groupes RBAC configurés dans NetScaler Console
total_ingress_deployed	Le nombre total de contrôleurs d'entrée dans Kubernetes.
total_ipam_configured	Le nombre total de réseaux IPAM ajoutés dans NetScaler Console
total_web_transaction_analytics	Le nombre total d'instances NetScaler activées avec l'analyse des transactions Web
total_pager_duty_profile	Le nombre total de profils PagerDuty ajoutés dans NetScaler Console
total_slack_profile	Le nombre total de profils Slack ajoutés dans NetScaler Console
total_api_discovery	Le nombre total d'instances NetScaler recevant des requêtes API
t_radius_svr	Le nombre total de serveurs d'authentification RADIUS configurés dans NetScaler Console
t_ldap_svr	Le nombre total de serveurs d'authentification LDAP configurés dans NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
t_tacacs_svr	Le nombre total de serveurs d'authentification TACACS configurés dans NetScaler Console
t_att	Le nombre total de requêtes provenant d'un appareil sur lequel Security Insight est activé
nombre	Le nombre total de requêtes provenant d'un appareil sur lequel HDX Insight est activé
nombre	Le nombre total d'utilisateurs se connectant via le VPN
nombre	Le nombre total d'utilisateurs se connectant via le Bureau virtuel
agent_id	L'ID unique de l'agent déployé
plateforme	La plateforme où l'agent est hébergé. Par exemple, Citrix Hypervisor
Version	La version de l'agent
ville	La ville où l'agent est déployé
pays	Le pays où l'agent est déployé
région	La région où l'agent est déployé
racine	Les détails d'utilisation du disque de NetScaler Console dans les répertoires /var, /root, /flash, /var/mps
Total	L'espace disque total de NetScaler Console (Unité : Octets)
utilisé	L'espace disque total utilisé de NetScaler Console
libre	L'espace disque total disponible de NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
Adm_analt_dx - Fonctionnalité	Le type d'analyse (Bot, WAF, Web Insight, Service Graph, etc.) pour lequel les problèmes sont identifiés
Adm_analt_dx - type_de_problème	La catégorie de problème à laquelle appartient le problème identifié. Par exemple, licences, configuration
Adm_analt_dx - type_de_sous-problème	La catégorie de sous-problème pour le problème identifié. Le sous-problème peut être NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_COLLECTORS_PRESENT, APPFLOWPARAM_DISABLED, ICA_APPFLOW_POLICY_BINDING, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_PRESENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
Production	Le nom du produit
isCloud	Qu'il soit sur site ou dans le cloud
isContainer	Indique s'il s'agit du déploiement de conteneurs
mas_platform	La plateforme NetScaler Console
fonctionnalité	La fonctionnalité d'analyse activée sur les serveurs virtuels d'équilibrage de charge/de commutation de contenu
total_lbvserver_ft_enabled	Le nombre total de serveurs virtuels d'équilibrage de charge sur lesquels au moins une fonctionnalité d'analyse est activée

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_csvserver_ft_enabled	Le nombre total de serveurs virtuels de commutation de contenu sur lesquels au moins une fonctionnalité d'analyse est activée
feature_enabled_on_vpn	La fonctionnalité d'analyse activée sur les serveurs virtuels VPN
total_vpnvserver_ft_enabled	Le nombre total de serveurs virtuels VPN sur lesquels au moins une fonctionnalité d'analyse est activée

Données de télémétrie facultatives pour le programme de télémétrie NetScaler®

Utilisation des fonctionnalités de NetScaler Console

Le tableau suivant affiche la liste des données facultatives collectées dans le cadre du programme de télémétrie NetScaler :

PARAMÈTRES	DESCRIPTION
plateforme	La plateforme sur laquelle NetScaler Console est hébergée. Par exemple, Citrix Hypervisor
déploiement	Vérifie si le type de déploiement de NetScaler Console est autonome ou une paire HA
is_agt	Vérifie si l'agent est configuré ou non
is_cloud	Vérifie si le déploiement de NetScaler Console est un service NetScaler Console ou NetScaler Console sur site
is_cntr	Vérifie si le déploiement de NetScaler Console se trouve dans un cluster Kubernetes
is_dr	Vérifie si le nœud de reprise après sinistre est configuré ou non

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
t_ten	Le nombre total de locataires connectés à NetScaler Console
num_of_ns_upgrade_jobs	Le nombre total de tâches de mise à niveau utilisées
security_advisory_enabled	Si Security Advisory est activé dans NetScaler Console sur site
Web Insight	Si Web Insight est activé dans le serveur virtuel lb ou cs
webinisight_usage	S'il y a des sessions HDX actives (oui ou non)
adm_analyt_hdx_apps	Le nombre total de requêtes provenant de l'appareil sur lequel HDX Insight est activé
adm_analyt_hdx_users	Le nombre d'utilisateurs connectés via le Bureau Virtuel
adm_analyt_sec_insight	Le nombre total de requêtes provenant de l'appareil sur lequel Security Insight est activé
adm_analyt_vpn_users	Le nombre total d'utilisateurs se connectant via VPN
adm_analyt_webinsight	Le nombre total de requêtes provenant de l'appareil sur lequel Web Insight est activé
Analyse des anomalies	Indique si la fonctionnalité de requête est activée sur le serveur virtuel lb ou cs
nombre	Le nombre total de problèmes liés à l'analyse
fonctionnalité	La catégorie de fonctionnalité pour le problème identifié. La fonctionnalité peut être BOT_INSIGHT, DEVICE, GATEWAY_INSIGHT, HDX_INSIGHT, SECURITY_INSIGHT, SERVICE_GRAPH, SWG_INSIGHT, WEB_INSIGHT, WEB_SECURITY_BOT_INSIGHT

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
fonctionnalité	La fonctionnalité d'analyse activée sur les serveurs virtuels d'équilibrage de charge
fonctionnalité	La fonctionnalité d'analyse activée sur les serveurs virtuels de commutation de contenu
fonctionnalité	La fonctionnalité d'analyse activée sur les serveurs virtuels VPN
aperçu gw	Indique si la fonctionnalité ICA_REQUEST est activée sur un serveur virtuel VPN
gwinsight_usage	Indique s'il y a eu des utilisateurs HDX au cours du dernier jour (oui ou non)
gw_hdx_insights	L'exportation de HDX insight et Gateway insight est activée
aperçu hdx	Indique si la fonctionnalité ICA_Request est activée sur un serveur VPN
hdxinsight_usage	Indique s'il y a eu des utilisateurs HDX au cours du dernier jour
issue_type	La catégorie de problème à laquelle appartient le problème identifié. Par exemple, la licence, la configuration.
aperçu de sécurité	Indique si le security insight est activé dans le serveur virtuel lb ou cs
secinsight_usage	Indique si des attaques de sécurité ont été détectées au cours de la dernière journée (oui ou non)
sub_issue_type	La sous-catégorie de problème pour le problème identifié. La sous-catégorie peut être NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_COLLECTORS_PRESENT,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
	APPFLOWPARAM_DISABLED, ICA_APPFLOW_POLICY_BINDING, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_PRESENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
total_api_discovery	Le nombre total d'instances NetScaler recevant des requêtes API
total_csvserver_ft_enabled	Le nombre total de serveurs virtuels de commutation de contenu où au moins une fonctionnalité d'analyse est activée
total_lbvserver_ft_enabled	Le nombre total de serveurs virtuels d'équilibrage de charge où au moins une fonctionnalité d'analyse est activée
total_vpnserver_ft_enabled	Le nombre total de serveurs virtuels VPN où au moins un serveur d'analyse est activé
total_web_transaction_analytics	Le nombre total d'instances NetScaler activées avec l'analyse des transactions Web
t_radius_svr	Le nombre total de serveurs d'authentification RADIUS configurés dans NetScaler Console
t_ldap_svr	Le nombre total de serveurs d'authentification LDAP configurés dans NetScaler Console
t_tacacs_svr	Le nombre total de serveurs d'authentification TACACS configurés dans NetScaler Console
agt_pl_azure	Le type de plateforme de l'agent
agt_pl_citrix_hypervisor	Le type de plateforme de l'agent
agt_pl_docker	Le type de plateforme de l'agent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
agt_pl_esx	Le type de plateforme de l'agent
agt_pl_hyper_v	Le type de plateforme de l'agent
agt_pl_gcp	Le type de plateforme de l'agent
agt_pl_kvm	Le type de plateforme de l'agent
agt_pl_kubernetes	Le type de plateforme de l'agent
agt_pl_unknown	Le type de plateforme de l'agent
agt_pl_aws	Le type de plateforme de l'agent
agent_id	L'ID unique de l'agent déployé
ville	La ville où l'agent est déployé
pays	Le pays où l'agent est déployé
plateforme	La plateforme où NetScaler Console est hébergé. Par exemple, Citrix Hypervisor
région	La région où l'agent est déployé
total_active_agents	Le nombre total d'agents en état ACTIF
total_agents	Le nombre total d'agents configurés
Version	La version de l'agent
ville	La ville du centre de données
isCloud	Qu'il soit sur site ou dans le cloud
mas_platform	La plateforme NetScaler Console
production	Le nom du produit
prodVer	La version de build de la Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_k8s	La NetScaler Console hébergée sur le cluster Kubernetes. Le nombre total de clusters Kubernetes
total_apps	Le nombre total d'applications dans NetScaler Console
total_custom_sites	Le nombre total de sites personnalisés configurés dans NetScaler Console
total_managed_apps	Le nombre total d'applications gérées dans NetScaler Console
total_custom_apps	Le nombre total d'applications personnalisées dans NetScaler Console
racine	Les détails d'utilisation du disque de NetScaler Console dans les répertoires /var, /root, /flash, /var/mps
Total	L'espace disque total de NetScaler Console (Unité : octets)
utilisé	L'espace disque total utilisé de NetScaler Console
libre	L'espace disque total disponible de NetScaler Console
total_api_requests	Le nombre total de requêtes via l'API vers NetScaler Console au cours des dernières 24 heures. Cela inclut également les utilisateurs de proxy distant (requêtes de l'agent).
total_api_external_requests	Le nombre total de requêtes via l'API vers NetScaler Console qui excluent les requêtes de l'agent
total_gui_requests	Le nombre total d'utilisateurs connectés à l'interface graphique de NetScaler Console au cours des dernières 24 heures

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_users	Le nombre total d'utilisateurs locaux de NetScaler Console
total_config_audit	Le nombre total de modèles d'audit de configuration configurés dans NetScaler Console
total_config_job	Le nombre total de tâches de configuration créées dans NetScaler Console
total_ssl_certs	Le nombre total de certifications SSL créées/ modifiées/supprimées depuis NetScaler Console
total_custom_event_rules	Le nombre total de règles d'événements personnalisées créées dans NetScaler Console
total_event_rules	Le nombre total de règles d'événements créées dans NetScaler Console
total_ingress_deployed	Le nombre total de contrôleurs d'entrée dans Kubernetes.
total_ipam	Le nombre total de fournisseurs IPAM ajoutés dans NetScaler Console
total_ipam_configured	Le nombre total de réseaux IPAM ajoutés dans NetScaler Console
total_network_report	Le nombre total de rapports réseau créés dans NetScaler Console
total_pager_duty_profile	Le nombre total de profils PagerDuty ajoutés dans NetScaler Console
gw_hdx_insights	Si l'exportation de HDX Insight et Gateway Insight est activée
total_rbac_groups	Le nombre total de groupes RBAC configurés dans NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_slack_profile	Le nombre total de profils Slack ajoutés dans NetScaler Console
total_ssl_certs	Le nombre total de certifications SSL créées/ modifiées/supprimées depuis NetScaler Console
total_stylebook_config_store_count	Le nombre total de packs de configuration créés dans NetScaler Console
total_user_sb_stylebook_count	Le nombre total de packs de configuration personnalisés créés dans NetScaler Console
pack de configuration	Le nombre total de packs de configuration stockés à partir des StyleBooks
isContainer	Si NetScaler Console est déployé sur une plateforme de conteneurs
pourcentage	L'espace disque total utilisé pour var_mps, root, flash, var

Données de télémétrie requises pour Cloud Connect

Le tableau suivant affiche la liste des données requises collectées après l'activation de Cloud Connect :

PARAMÈTRES	DESCRIPTION
onprem_ip	L'adresse IP de la console NetScaler
onprem_customer_id	L'ID Citrix Cloud
onprem_time_stamp	La date et l'heure de téléchargement des données
on_prem_version	La version sur site de NetScaler Console
total_blx_device	Le nombre total d'instances BLX gérées dans NetScaler Console sur site

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_managed_devices	Le nombre total d'instances NetScaler gérées dans NetScaler Console
total_active_managed_devices	Le nombre total d'instances NetScaler qui sont à l'état UP
total_ns_device	Le nombre total d'instances MPX gérées dans NetScaler Console
total_ng_device	Le nombre total d'instances Gateway gérées dans NetScaler Console
total_ngvpx_device	Le nombre total d'instances Gateway VPX gérées dans NetScaler Console
total_nswg_device	Le nombre total d'instances Web Gateway gérées dans NetScaler Console
total_nswgvpx_device	Le nombre total d'instances Web Gateway VPX gérées dans NetScaler Console
total_nsvpx_device	Le nombre total d'instances VPX gérées dans NetScaler Console
total_cpx_device	Le nombre total d'instances CPX gérées dans NetScaler Console
total_nsap_device	Le nombre total d'instances de partition d'administration dans NetScaler Console
total_nssdx_device	Le nombre total d'instances SDX gérées dans NetScaler Console
total_waf_devices	Le nombre total d'instances NetScaler pour lesquelles les violations WAF sont activées
total_gw_devices	Le nombre total d'instances NetScaler pour lesquelles le VPN SSL est activé
total_icaproxy_devices	Le nombre total d'instances NetScaler pour lesquelles HDX Insight est activé dans NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
total_bot_devices	Le nombre total d'instances NetScaler pour lesquelles les violations de bot sont activées
total_pooled_devices	Le nombre total d'instances NetScaler (gérées et non gérées) avec des licences en pool
total_lb_devices	Le nombre total d'instances NetScaler configurées avec des serveurs virtuels d'équilibrage de charge
total_lb_devices_http	Le nombre total d'instances NetScaler configurées avec des serveurs virtuels HTTP d'équilibrage de charge
total_lb_devices_ssl	Le nombre total d'instances NetScaler configurées avec des serveurs virtuels SSL d'équilibrage de charge
total_cs_devices	Le nombre total d'instances NetScaler configurées avec des serveurs virtuels de commutation de contenu
total_gslb_devices	Le nombre total d'instances NetScaler configurées avec des serveurs virtuels d'équilibrage de charge de serveur global
total_aaa_devices	Le nombre total d'instances NetScaler configurées avec des serveurs virtuels AAA
device_id	L'ID unique de l'instance VPX
Numéro de version	La version de build de l'instance VPX
état	L'état actuel (actif ou inactif) de l'instance VPX
plateforme_appareil	La plateforme sur laquelle l'instance VPX est hébergée
st	L'heure actuelle de l'extraction des données
instances_de_pool_autorisées	Le nombre total d'instances de pool autorisées

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
instances_de_pool_utilisées	Le nombre total d'instances de pool utilisées
instances_de_pool_fips_autorisées	Le nombre total d'instances de pool FIPS autorisées
instances_de_pool_fips_utilisées	Le nombre total d'instances FIPS du pool utilisées
pool_entvcpu_entitled	Le nombre total de vCPU Enterprise du pool alloués
pool_entvcpu_used	Le nombre total de vCPU Enterprise du pool utilisés
pool_entbw_entitled	La bande passante Enterprise totale du pool allouée [MBps]
pool_entbw_used	La bande passante Enterprise totale du pool utilisée [MBps]
pool_pltbw_entitled	La bande passante Platinum totale du pool allouée [MBps]
pool_pltbw_used	La bande passante Platinum totale du pool utilisée [MBps]
pool_pltvcpu_entitled	Le nombre total de vCPU Platinum du pool alloués
pool_pltvcpu_used	Le nombre total de vCPU Platinum du pool utilisés
pool_stdbw_entitled	La bande passante Standard totale du pool allouée
pool_stdbw_used	La bande passante Standard totale du pool utilisée
pool_stdvcpu_entitled	Le nombre total de vCPU Standard du pool alloués

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
pool_stdvcpu_used	Le nombre total de vCPU Standard du pool utilisés
pool_cpxvcpu_entitled	Le nombre total de vCPU CPX du pool alloués
pool_cpxvcpu_used	Le nombre total de vCPU CPX du pool utilisés
pool_perc_instances_used	Le % d'instances utilisées
pool_perc_vcpu_used	Le % de vCPU utilisées
pool_perc_bw_used	Le % de bande passante utilisée
total_entitled_vservers	Le nombre total de serveurs virtuels autorisés
total_used_vservers	Le nombre total de serveurs virtuels utilisés
total_discovered_vservers	Le nombre total de serveurs virtuels découverts
perc_used_vservers	Le % de serveurs virtuels utilisés/autorisés
perc_discovered_vservers	Le % de serveurs virtuels découverts/autorisés
is_local_license	Vérifie si la licence est hébergée dans NetScaler Console
license_edition	Le type de licence (Platinum/Standard/ Enterprise)
is_pooled_license	Vérifie si la licence est une licence groupée
model_id	L'ID de modèle de l'instance
plt_license_allocation	L'allocation de licence Platinum
ent_license_allocation	L'allocation de licence Enterprise
std_license_allocation	L'allocation de licence Standard
license_end_date	Nombre total de jours avant l'expiration de la licence

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMÈTRES	DESCRIPTION
plateforme	Le type d'appareil
instance_id	L'identifiant unique de l'instance
instance_mode	Vérifie si l'instance est autonome ou une paire HA
instance_state	L'état de l'instance (Actif/Inactif)
flex_vpx_inst_entitled	Le nombre total d'instances VPX autorisées
flex_vpx_inst_allocated	Le nombre total d'instances VPX allouées
flex_sdx_inst_entitled	Le nombre total d'instances SDX autorisées
flex_sdx_inst_allocated	Le nombre total d'instances SDX allouées
flex_mpx_inst_entitled	Le nombre total d'instances MPX autorisées
flex_mpx_inst_allocated	Le nombre total d'instances MPX allouées
flex_plt_bw_entitled	La bande passante Platinum autorisée
flex_plt_bw_allocated	La bande passante Platinum allouée
flex_ent_bw_entitled	La bande passante Enterprise autorisée
flex_ent_bw_allocated	La bande passante Enterprise allouée
flex_std_bw_entitled	La bande passante standard autorisée
flex_std_bw_allocated	La bande passante standard allouée
flex_vpx_fips_inst_entitled	Le nombre total d'instances FIPS autorisées
flex_vpx_fips_inst_allocated	Le nombre total d'instances FIPS allouées
type de licence ns	Le type de licence (Flexed ou Fixed)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Données de télémétrie requises pour le programme de télémétrie NetScaler®

Les données collectées dans le cadre du programme de télémétrie NetScaler sont répertoriées dans le document Gouvernance des données de télémétrie.

REMARQUE :

Certains paramètres sont collectés via un script qui est poussé de NetScaler Console vers les instances NetScaler.

Les informations collectées via la télémétrie, telles que les adresses e-mail, les noms d'utilisateur et les adresses IP, sont pseudonymisées de manière sécurisée en hachant les informations à la source à l'aide d'algorithmes de hachage unidirectionnels. Par conséquent, Citrix ne peut pas accéder à ces valeurs ni les lire. Ces données de télémétrie sont utilisées uniquement à des fins de correspondance logique des actifs.

Licences

NetScaler Console nécessite une licence NetScaler vérifiée pour gérer et surveiller les instances NetScaler, lorsque les instances sont découvertes via le protocole `https`.

NetScaler Console prend en charge les éditions de licence suivantes. Contactez votre représentant commercial ou partenaire NetScaler pour acheter une licence NetScaler Console.

Édition Express – Vous pouvez gérer et surveiller n'importe quel nombre d'instances avec la licence Édition Express. Par défaut, la licence Édition Express est appliquée.

Édition Advanced - Elle permet de gérer les applications découvertes et d'afficher les analyses pour les serveurs virtuels achetés ainsi que pour les serveurs virtuels gratuits.

Points à noter :

- Pour la version **13.1-9.x ou antérieure**, vous pouvez gérer jusqu'à 30 applications découvertes ou serveurs virtuels et afficher les analyses. Au-delà des 30 applications découvertes ou des 30 serveurs virtuels, vous devez acheter et appliquer une licence Advanced. Par exemple, si vous achetez 100 licences de serveurs virtuels, vous avez le droit d'utiliser jusqu'à 130 licences de serveurs virtuels.
- Pour la version **13.1-12.x ou ultérieure**, vous pouvez gérer jusqu'à deux applications découvertes ou serveurs virtuels et afficher les analyses. Au-delà des deux applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

découvertes ou des deux serveurs virtuels, vous devez acheter et appliquer une licence Advanced. Par exemple, si vous achetez 100 licences de serveurs virtuels, vous avez le droit d'utiliser jusqu'à 102 licences de serveurs virtuels.

Après la mise à niveau vers les versions 13.1-12.x jusqu'à 14.1-17.x :

- Tous les serveurs virtuels gratuits par défaut de l'édition Express restent fonctionnels pendant 30 jours. Vous pouvez sélectionner les deux serveurs virtuels et appliquer les deux licences par défaut dans un délai de 30 jours. Si aucune action de l'utilisateur n'est effectuée 30 jours après la mise à niveau, NetScaler Console applique aléatoirement la licence à deux serveurs virtuels et retire la licence des serveurs virtuels restants. Vous devez acheter et appliquer de nouvelles licences Advanced pour activer ces serveurs virtuels.
- Après la mise à niveau, voici les changements de comportement de NetScaler Console :
  - NetScaler Console accorde 30 jours supplémentaires pour effectuer l'action requise.
  - Pendant la période de 30 jours, l'allocation de nouveaux serveurs virtuels pour les 30 serveurs virtuels gratuits de l'édition Express est bloquée.
    - Par exemple, si le nombre de licences de serveurs virtuels disponibles avant votre mise à niveau vers la version 12.x était de 30 et que seuls 20 serveurs virtuels sous licence étaient utilisés, vous n'êtes autorisé à utiliser que les 20 serveurs virtuels et n'êtes pas autorisé à licencier les 10 serveurs virtuels restants pendant la période de 30 jours.
  - Cependant, pendant la période de 30 jours, en tant qu'administrateur, vous pouvez toujours appliquer des licences NetScaler Console Advanced et allouer de nouveaux serveurs virtuels.

Le tableau suivant fournit les détails de la licence :

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION ADVANCE	LICENCE NETSCALER
Applications	Tableau de bord des applications	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Les informations relatives au pare-feu d'applications Web NetScaler sur le tableau de bord des applications

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION ADVANCE	LICENCE NETSCALER
				nécessitent une licence Premium (ou) Advanced avec App Firewall.
	Web Insight	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	NA
	Graphe de services	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	NA
	Configuration > StyleBooks	Illimité	Illimité	NA
Sécurité	Tableau de bord de sécurité	Jusqu'à deux serveurs virtuels.	Droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Les informations relatives au pare-feu d'applications Web NetScaler sur le tableau de bord de sécurité nécessitent une licence Premium (ou)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION ADVANCE	LICENCE NETSCALER
				Advanced avec App Firewall.
	Violations de sécurité	Jusqu'à deux serveurs virtuels.	Donne droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Premium (ou) Advanced avec licence App Firewall
	Utilisateurs et points de terminaison	Jusqu'à deux serveurs virtuels.	Donne droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	N/A
Passerelle	HDX Insight	Jusqu'à deux serveurs virtuels.	Donne droit à toutes les licences de serveurs virtuels achetées et à deux serveurs virtuels supplémentaires.	Advanced (rapports < 1 heure) Premium (rapports = Illimité)
	Gateway Insight	Jusqu'à deux serveurs virtuels.	Donne droit à toutes les licences de serveurs virtuels	Advanced (rapports < 1 heure) Premium

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION ADVANCE	LICENCE NETSCALER
			achetées et à deux serveurs virtuels supplémentaires.	(rapports = Illimité)
Infrastructure	Analyse d'infrastructure	Illimité	Illimité	NA
	Instances	Illimité	Illimité	NA
	Tableau de bord SSL	Illimité	Illimité	NA
	Événements	Illimité	Illimité	NA
	Fonctions réseau	Illimité	Illimité	NA
	Rapports réseau	Illimité	Illimité	NA
	Licences mutualisées	Illimité	Illimité	NA
	Configuration > Tâches de configuration, Modèles de configuration et Conseils de configuration	Illimité	Illimité	NA
	Tâches de mise à niveau	Illimité	Illimité	NA
	Orchestration	Illimité	Illimité	NA
Paramètres	RBAC et authentification	Illimité	Illimité	NA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FONCTIONNALITÉS	OPTIONS	ÉDITION EXPRESS	ÉDITION ADVANCE	LICENCE NETSCALER
	externe (niveau d'instance)			
	RBAC et authentification externe	Illimité	Illimité	NA

*Pour l'intégration de Citrix Director avec la prise en charge de NetScaler Console – Citrix Director doit disposer d'une licence Premium.

Des licences pour davantage de serveurs virtuels sont disponibles par packs de 10 serveurs virtuels. Vous pouvez obtenir une licence valide et l'ajouter sur les serveurs NetScaler Console via l'interface graphique de NetScaler Console.

Haute disponibilité

Le serveur NetScaler Console peut contenir des licences VIP, CICO et de capacité groupée. Lorsque les licences sont émises pour un serveur NetScaler Console, elles sont liées à l'ID d'hôte du serveur. L'attribution de licences à un autre serveur NetScaler Console est restreinte.

Si vous configurez une paire haute disponibilité NetScaler Console en tant que serveur de licences, les serveurs principal et secondaire doivent disposer des mêmes fichiers de licence. Par conséquent, dans un déploiement haute disponibilité NetScaler Console, NetScaler Console prend en charge l'attribution des mêmes fichiers de licence aux deux serveurs.

REMARQUE

- Si vous avez installé NetScaler Console version 12.1-49.x ou antérieure, vous disposez de 30 jours pour maintenir la licence sur le nœud secondaire. Après 30 jours, vous devez contacter Citrix pour réhéberger la licence d'origine.
- Dans la version 12.1-50.x et ultérieure, la licence NetScaler Console est automatiquement synchronisée avec le nœud secondaire.
- Les licences groupées sont automatiquement synchronisées avec le nœud secondaire dans la version 12.1-50.x et ultérieure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Comment les licences sont-elles synchronisées entre les nœuds haute disponibilité de NetScaler Console ?

Chaque fois qu'un basculement se produit, le serveur secondaire assume le rôle de serveur principal. L'ID d'hôte réel du serveur principal est configuré comme l'ID d'hôte virtuel du nouveau serveur principal. Les fichiers de licence reconnaissent le nouveau serveur principal à l'aide de l'ID d'hôte virtuel.

- **ID d'hôte réel** - Cet ID est généré à partir d'une adresse MAC du serveur NetScaler Console. Chaque déploiement autonome de NetScaler Console possède un ID d'hôte unique.
- **ID d'hôte virtuel** - Cet ID est généré automatiquement lors du déploiement HA. L'ID d'hôte réel d'un serveur principal NetScaler Console est utilisé comme ID d'hôte virtuel du serveur secondaire. Cet ID est stocké dans la base de données NetScaler Console dans un format chiffré et toute modification de cet ID est restreinte. L'ID d'hôte virtuel est préféré à l'ID d'hôte réel.

Supposons que le nœud 1 est le serveur principal et le nœud 2 est le serveur secondaire. L'ID d'hôte virtuel du nœud 1 est synchronisé avec le nœud 2.

1. Les fichiers de licence disponibles sur le nœud 1 sont synchronisés avec le nœud 2.
2. Tous les nouveaux fichiers de licence sur le nœud 1 sont synchronisés périodiquement avec le nœud 2.
3. NetScaler Console garantit que le serveur de licences s'exécute uniquement sur le nœud 1 afin d'éviter le doublement de la capacité de licence.
4. Les instances NetScaler extraient les licences du nœud 1 à l'aide de l'adresse IP flottante.

Les licences sont verrouillées aux instances NetScaler. Pour extraire les licences de NetScaler Console HA, les instances nécessitent l'adresse IP spécifique de NetScalerNetScaler. Lorsque vous appliquez des licences sur un serveur principal qui sera en charge de la gestion des licences, cela s'applique à toutes les futures licences sur cette instance. Vous ne pouvez supprimer les licences que du serveur sur lequel vous les avez installées.

Orchestration

Le module d'orchestration est indépendant de la gestion des licences et est toujours disponible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mettre à niveau les licences de serveur virtuel

Vous pouvez mettre à niveau la gestion des licences sur NetScaler Console pour surveiller et gérer davantage de serveurs virtuels hébergés sur NetScaler.

Pour mettre à niveau vos licences NetScaler :

1. Connectez-vous à NetScaler Console à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Infrastructure > Licences en pool**.
3. Accédez à **Fichiers de licence**, puis sélectionnez l'une des options suivantes :

   - **Télécharger les fichiers de licence à partir d'un ordinateur local**. Si une licence est déjà présente sur votre ordinateur local, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez utiliser pour allouer vos licences. Cliquez sur **Terminer**.
   - **Utiliser le code d'activation de licence**. Citrix envoie par e-mail le code d'accès à la licence que vous avez achetée. Saisissez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir les licences**.

   REMARQUE

   Si vous sélectionnez cette option, NetScaler Console doit être connecté à Internet, ou un serveur proxy doit être disponible.

   

4. Vous pouvez ajouter d'autres licences à tout moment depuis la page Paramètres de licence.

   

Vérification

Vous pouvez vérifier les licences installées sur NetScaler Console en accédant à **Paramètres > Configuration des licences et des analyses**.



Gérer les serveurs virtuels

Vous pouvez sélectionner les serveurs virtuels ou les serveurs virtuels tiers que vous souhaitez gérer et surveiller via NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POINTS À NOTER

- Par défaut, NetScaler Console attribue automatiquement des licences aux serveurs virtuels de manière aléatoire après chaque cycle d'interrogation des serveurs virtuels.
- Si le nombre total de serveurs virtuels découverts dans votre NetScaler Console est inférieur au nombre de licences de serveurs virtuels installées, NetScaler Console, par défaut, attribue des licences à tous les serveurs virtuels.

Pour sélectionner manuellement les serveurs virtuels ou pour limiter l'attribution de licences à un nombre restreint de serveurs virtuels, vous devez d'abord désactiver l'attribution automatique de licences aux serveurs virtuels, puis sélectionner les serveurs virtuels que vous souhaitez gérer.

Désactiver l'attribution automatique de licences aux serveurs virtuels

1. Accédez à **Paramètres > Configuration des licences et des analyses**.

   Le tableau de bord affiche les licences de serveurs virtuels disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de la licence.
2. Dans **Allocation de licences de serveurs virtuels**, désactivez **Serveurs virtuels sous licence automatique** et **Sélection automatique des serveurs virtuels non adressables**.

   

Sélectionner des serveurs virtuels tiers pour l'attribution de licences

1. Accédez à **Paramètres > Configuration des licences et des analyses**.

   Le tableau de bord affiche les licences de serveurs virtuels disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de la licence.
2. Dans **Résumé des serveurs virtuels tiers**, désactivez **Sélection automatique des serveurs virtuels tiers**.

   

Appliquer manuellement les licences de serveurs virtuels

Vous pouvez appliquer manuellement des licences à un serveur virtuel individuel.

1. Dans **Allocation de licences de serveur virtuel**, sélectionnez **Configurer les licences**.

   La page **Tous les serveurs virtuels** s'affiche.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Filtrez les serveurs virtuels sans licence à l'aide de la propriété : `Licensed: No`.
3. Sélectionnez le serveur virtuel que vous souhaitez licencier.
4. Cliquez sur **Licence**.

Configurer la licence de serveur virtuel basée sur une stratégie

Vous pouvez configurer une stratégie pour appliquer des licences aux serveurs virtuels. Cette stratégie contrôle le nombre de serveurs virtuels que vous souhaitez licencier automatiquement. Elle applique également des licences uniquement aux serveurs virtuels des instances sélectionnées.

Cliquez sur **Modifier les stratégies** et vous pouvez spécifier les éléments suivants :

- Définissez séparément une limite de serveurs virtuels sur les instances CPX pour appliquer des licences. NetScaler Console applique une licence aux serveurs virtuels sur les instances CPX jusqu'à une limite spécifiée.

  IMPORTANT

  Cette limite s'applique aux instances CPX, à l'exception des types de déploiement sidecar.

  Pour afficher les instances CPX des types de déploiement sidecar, filtrez les serveurs virtuels à l'aide de la propriété : `License Type: Freely Managed`.
- Définissez une limite de serveurs virtuels sur les instances NetScaler sélectionnées (MPX/VPX/BLX) pour appliquer des licences. NetScaler Console applique des licences aux serveurs virtuels sur les instances NetScaler jusqu'à une limite spécifiée.
- Sélectionnez les instances NetScaler prioritaires pour appliquer les licences de serveur virtuel. Par conséquent, NetScaler Console ne peut appliquer de licence qu'aux serveurs virtuels des instances sélectionnées.

Afficher les serveurs virtuels sous licence

Une fois les licences appliquées aux serveurs virtuels, vous pouvez afficher les serveurs virtuels sous licence ou les serveurs virtuels tiers.

1. Accédez à **Paramètres > Configuration des licences et de l'analyse**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur le type de serveur virtuel dans la section **Total sous licence** du **Résumé des licences des serveurs virtuels**.

Configurer la prise en charge automatique des licences pour les serveurs virtuels non adressables

NetScaler Console, par défaut, n'applique pas automatiquement les licences aux serveurs virtuels non adressables. Pour attribuer des licences aux serveurs virtuels non adressables, vous devez désactiver l'option de licence automatique et sélectionner manuellement les serveurs virtuels non adressables. Cela augmente vos efforts pour sélectionner manuellement les serveurs non adressables initialement lorsque vous appliquez les licences. Vous devez également sélectionner manuellement les nouveaux serveurs virtuels non adressables chaque fois qu'ils sont ajoutés à votre réseau.

NetScaler Console propose une option sous **Allocation de licences de serveurs virtuels**. Si vous activez l'option **Sélectionner automatiquement les serveurs virtuels non adressables**, les licences sont appliquées automatiquement aux serveurs virtuels non adressables.

REMARQUE

- NetScaler Console, par défaut, ne sélectionne toujours pas automatiquement les serveurs virtuels non adressables pour l'octroi de licences.
- L'analyse des applications (tableau de bord des applications) est la seule analyse actuellement prise en charge sur les serveurs virtuels non adressables sous licence.

Sauvegarder et restaurer une configuration NetScaler Console dans une paire HA

Vous pouvez sauvegarder la configuration actuelle d'une NetScaler Console. Dans un déploiement HA de NetScaler Console, vous pouvez sauvegarder et restaurer la configuration NetScaler Console à partir de l'un ou l'autre des serveurs. Si vous utilisez une adresse IP de serveur virtuel d'équilibrage de charge pour effectuer la sauvegarde, le fichier de sauvegarde peut être stocké sur l'un ou l'autre des serveurs et doit être vérifié manuellement.

Si vous restaurez alors qu'un seul nœud est actif, ou si un basculement se produit pendant la restauration, le processus de restauration échoue.

Pour sauvegarder une configuration NetScaler Console :

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Accédez à **Système** \> **Paramètres avancés** \> **Fichiers de sauvegarde**, puis cliquez sur **Sauvegarder**.
2. Pour chiffrer le fichier de sauvegarde, cochez la case **Protéger le fichier par mot de passe**.

Pour restaurer une configuration NetScaler Console à partir d'un fichier de sauvegarde :

1. Accédez à **Système** \> **Paramètres avancés** \> **Fichiers de sauvegarde**.
2. Sélectionnez le fichier de sauvegarde que vous souhaitez restaurer, puis cliquez sur **Restaurer**.

Pour configurer les paramètres de sauvegarde du système :

1. Accédez à **Système** \> **Administration système**. Sous **Paramètres de sauvegarde**, cliquez sur **Paramètres de sauvegarde du système**.
2. Sur la page **Configurer les paramètres de sauvegarde du système**, spécifiez les éléments suivants :
   - Nombre de sauvegardes à conserver. Vous ne pouvez conserver que jusqu'à 10 sauvegardes.
   - Chiffrer le fichier de sauvegarde.
   - Activer le transfert externe. Vous pouvez transférer une copie de votre fichier de sauvegarde vers un autre système à titre de précaution. Lorsque vous souhaitez restaurer la configuration, vous devez d'abord télécharger le fichier sur le serveur NetScaler Console, puis effectuer l'opération de restauration. Spécifiez le serveur, le nom d'utilisateur et le mot de passe, le port, le protocole de transfert à utiliser et le chemin du répertoire. Pour en savoir plus sur le transfert externe, consultez Transférer un fichier de sauvegarde NetScaler Console vers un système externe.
3. Cliquez sur **OK**.



Configurer les paramètres de notification système

Vous pouvez envoyer des notifications à des groupes d'utilisateurs sélectionnés pour diverses fonctions liées au système. Ces fonctions système sont organisées en catégories d'événements telles que SystemReboot, StatusPoll et SystemState. Vous pouvez configurer NetScaler Console pour vous envoyer des notifications par e-mail ou par SMS. Vous devez configurer un serveur de messagerie ou un serveur de passerelle de service de messages courts (SMS), ou les deux, pour envoyer des notifications par e-mail et par SMS aux utilisateurs. Cela garantit que vous êtes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

informé de toute activité au niveau du système, telle que la connexion d'un utilisateur ou le redémarrage du système.

Par exemple, vous pouvez souhaiter envoyer une notification par e-mail à deux utilisateurs lorsqu'une personne tente de se connecter à NetScaler Console à l'aide de la CLI et que la tentative de connexion échoue. Vous devez configurer la notification système en sélectionnant la catégorie UserLogin et en créant un serveur de notification par e-mail ou en choisissant une liste de distribution d'e-mails existante pour envoyer la notification.

Pour configurer les paramètres de notification système sur NetScaler Console :

1. Accédez à **Système** \> **Notifications**. Sous **Paramètres**, cliquez sur **Modifier les paramètres de notification**.
2. Sur la page **Configurer les paramètres de notification système**, sous **Catégorie**, sélectionnez une catégorie telle que **UserLogin**.

   
3. Sélectionnez **Envoyer un e-mail**, puis sélectionnez une distribution d'e-mails dans la liste déroulante ou cliquez sur l'icône « **+** » pour créer une nouvelle liste de distribution d'e-mails, comme illustré dans la figure suivante. Si vous souhaitez envoyer des notifications textuelles, sélectionnez **Envoyer un SMS (message texte)** et créez une liste de distribution SMS en cliquant sur l'icône « **+** » et en spécifiant les détails du serveur SMS.

   

   Une fois les notifications définies pour certaines catégories d'événements, chaque fois qu'un événement appartenant à cette catégorie se produit, une notification est envoyée aux destinataires par e-mail ou par SMS. Dans cet exemple, vous pouvez voir les notifications par e-mail lorsqu'un utilisateur ne parvient pas à se connecter à NetScaler Console à l'aide de la CLI.

   

Les notifications système sont envoyées pour les événements suivants :

CATÉGORIE	CAUSE
BackupFailure	La sauvegarde du système échoue
DataStorageExceeded	Le stockage de la base de données dépasse la limite spécifiée dans la licence
DeviceBackupFailure	La sauvegarde de l'instance échoue

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIE	CAUSE
`HAMonitoring`	Le basculement HA du système se produit, aucun battement de cœur n'est reçu d'un nœud pair, et la synchronisation de la base de données échoue
HealthMontoring	L'utilisation du CPU, de la RAM ou du disque dépasse la valeur seuil
LicensePool	Le pool de licences dépasse la valeur seuil
Licenses	La licence échoue lors de son application
PasswordRecovery	La récupération du mot de passe échoue ou réussit
PerfCounterThresholdHigh	La valeur du compteur de performance dépasse la limite
PerfCounterThresholdNormal	La valeur du compteur de performance est normale
PolicyFailed	L'une des stratégies système échoue
RemoteDeviceBackupFailure	La sauvegarde de l'instance distante échoue
RemoteSystemBackupFailure	La sauvegarde du système distant échoue
RemoteSystemBackupNormal	La sauvegarde du système distant réussit
SSLCertThreshold	Le seuil d'un certificat est dépassé
StatusPoll	Tout changement d'état d'une instance
SubSystemState	Tout changement d'état du sous-système
SystemReboot	Le système est redémarré
SystemState	Tout changement d'état du système
TrapConfigFailure	Échec lors de l'ajout d'un piège SNMP sur une instance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CATÉGORIE	CAUSE
UserLogin	L'authentification de l'utilisateur échoue

Configurer les sites pour les géocartes

Un site NetScaler Console est un regroupement logique des instances NetScaler dans un emplacement géographique spécifique. Vous pouvez avoir plusieurs instances NetScaler au sein d'un site qui peuvent être surveillées et gérées par le serveur NetScaler Console. Vous pouvez utiliser le serveur NetScaler Console pour gérer des données telles que syslog, AppFlow et SNMP, ainsi que d'autres données provenant des instances gérées.

Pour créer un site :

1. Accédez à **Infrastructure > Instances > Sites**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un site**, spécifiez les informations suivantes :
   a. **Type de site** : Sélectionnez **Centre de données**.

      REMARQUE

      Le site peut fonctionner comme le centre de données principal ou comme une succursale. Choisissez en conséquence.

   b. **Type** : Sélectionnez AWS comme fournisseur de cloud dans la liste.

      REMARQUE

      Cochez la case **Utiliser un VPC existant comme site** en conséquence.

   c. **Nom du site** : Saisissez le nom du site.
   d. **Ville** : Saisissez la ville.
   e. **Code postal** : Saisissez le code postal.
   f. **Région** : Saisissez la région.
   g. **Pays** : Saisissez le pays
   h. **Latitude** : Saisissez la latitude de l'emplacement.
   i. **Longitude** : Saisissez la longitude de l'emplacement.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur **Créer**.



Pour plus d'informations sur l'ajout d'instances NetScaler à NetScaler Console, consultez Ajout d'une instance à NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.

© 1997–2026 Citrix Systems, Inc. All rights reserved.