Guide de déploiement sécurisé NetScaler®

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

Contents

Bonnes pratiques pour la sécurité de NetScaler MPX™, VPX et SDX 5
Ressources d'informations supplémentaires 5
Directives de déploiement 6
Meilleures pratiques de sécurité physique 6
Déployer l'appliance NetScaler dans un emplacement sécurisé 6
Sécuriser l'accès au panneau avant et au port console de NetScaler 6
Protection de l'alimentation électrique 6
Protection des clés cryptographiques 6
Meilleures pratiques de sécurité NetScaler 7
Effectuer les mises à jour logicielles de NetScaler 7
Sécuriser le système d'exploitation des serveurs hébergeant NetScaler VPX 7
Réinitialiser la gestion hors bande (LOM) de NetScaler 7
Maintenance et suppression des données persistantes 8
Directives de configuration 8
Sécurité réseau 9
Considérations clés en matière de sécurité réseau 9
Autres considérations relatives à la sécurité réseau 10
Sécurisation du trafic de transit sur NetScaler® 19
Administration et gestion 27
Comptes système et utilisateur 28
Journalisation et surveillance 37
Configurer le protocole NTP (Network Time Protocol) 37
Configurer SNMP 37
Configurer la journalisation vers un hôte de journal externe NetScaler 38
Configurer l'exportation des messages sur un canal sécurisé 40
Configuration LOM 40

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

Applications et services 41
Configurer NetScaler® pour supprimer ou transmettre l'en-tête de mise à niveau 41
Configurer NetScaler pour qu'il supprime les requêtes HTTP non valides 41
Configurer la protection contre les attaques par déni de service HTTP 42
Configurer NetScaler pour se défendre contre les attaques d'usurpation TCP 43
Configurer la conformité RFC 5961 44
Configurer NetScaler pour accepter des en-têtes HTTP spécifiques 44
Configurer la taille des en-têtes HTTP 44
Normaliser les URL dans NetScaler 45
Génération ISN TCP améliorée 46
Configurer la notification de fermeture 46
Sécuriser l'interface graphique de gestion, l'API NITRO et la communication RPC 47
Recommandations de sécurité DNSSEC 47
Utiliser RSA 1024 bits ou plus pour les clés privées KSK/ZSK 47
Activer l'alarme SNMP pour l'expiration des clés DNSSEC 47
Renouveler les clés privées KSK/ZSK avant l'expiration du certificat x.509 47
Sécuriser le serveur ADNS DNSSEC 48
Configuration héritée 49
Configurer NetScaler® pour désactiver la redirection de chiffrement 49
Configurer les paramètres de renégociation SSL sur NetScaler 50
Configurer la vérification de certificat de conformité NDcPP 50
Recommandations cryptographiques NetScaler® 51
Gestion des certificats et clés TLS 51
Configuration des suites de chiffrement TLS pour les déploiements FIPS et NDcPP 51
Recommandations NetScaler -FIPS 53
Configuration de NetScaler SDX dans un déploiement basé sur FIPS 53
Stocker le mot de passe HSM dans un emplacement sécurisé 54
Autres fonctionnalités 54

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

Recommandations de sécurité pour NetScaler® Web App Firewall 55

Déployer NetScaler en mode deux bras 55

Utiliser une politique de 'refus par défaut' 55

NetScaler Web App Firewall – Création de plusieurs niveaux de sécurité 56

Recommandations de sécurité pour NetScaler® Gateway 58

Utiliser une politique de 'refus par défaut' 58

Utiliser la communication TLS1.2 entre les serveurs 59

Utiliser les applications intranet 59

Recommandations de sécurité pour l'authentification, l'autorisation et l'audit 59

Bonnes pratiques pour la sécurité de NetScaler® Console 63

Ne pas exposer l'adresse IP de NetScaler Console et l'adresse IP de l'agent NetScaler à Internet 63

Mot de passe fort pour l'utilisateur système 64

Modifier le certificat par défaut 64

Désactiver l'authentification locale 65

fix 66

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

Bonnes pratiques pour la sécurité de NetScaler MPX™, VPX et SDX

NetScaler MPX est un contrôleur de livraison d'applications qui accélère les sites Web, fournit une gestion du trafic L4-L7, offre un pare-feu d'applications Web NetScaler intégré et décharge les serveurs. L'instance NetScaler VPX est une appliance virtuelle qui possède toutes les fonctionnalités de NetScaler MPX, s'exécute sur des serveurs standard et offre une disponibilité accrue pour les applications Web, y compris Citrix Virtual Apps and Desktops. NetScaler SDX offre une virtualisation avancée pour toute la flexibilité de VPX avec les performances de MPX. En utilisant MPX, VPX et SDX, une organisation peut déployer la solution de flexibilité ou de véritable multi-location qui optimise votre infrastructure de livraison d'applications Web en séparant les services réseau partagés à volume élevé des services intensifs en processeur et spécifiques aux applications. NetScaler assure également une intégration transparente avec Citrix OpenCloud Access qui peut étendre le centre de données avec la puissance du Cloud.

Pour maintenir la sécurité tout au long du cycle de vie du déploiement, nous vous recommandons de prendre en compte les éléments suivants pour :

- Sécurité physique
- Sécurité des appliances
- Sécurité réseau
- Administration et gestion

Différents déploiements peuvent nécessiter des considérations de sécurité différentes. Ce document fournit des conseils généraux en matière de sécurité pour vous aider à choisir un déploiement sécurisé approprié en fonction de vos exigences de sécurité spécifiques.

Ressources d'informations supplémentaires

Consultez les ressources suivantes pour d'autres informations de sécurité concernant NetScaler® et NetScaler Gateway :

- Portail de sécurité
- Documentation produit

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

Pour obtenir de l'aide supplémentaire concernant la configuration de votre NetScaler, vous pouvez soumettre une demande de support à l'adresse suivante : `<https://www.citrix.com/support.html>`

Directives de déploiement

Lors du déploiement d'un NetScaler, tenez compte des meilleures pratiques suivantes en matière de sécurité physique et de l'appliance :

Meilleures pratiques de sécurité physique

Déployer l'appliance NetScaler dans un emplacement sécurisé

Les appliances NetScaler doivent être déployées dans un emplacement sécurisé avec des contrôles d'accès physique suffisants pour protéger NetScaler contre tout accès non autorisé. Au minimum, l'accès à la salle des serveurs doit être contrôlé par une serrure, un lecteur de carte électronique ou d'autres méthodes physiques similaires.

D'autres mesures peuvent inclure l'utilisation d'un système de surveillance électronique, par exemple la vidéosurveillance (CCTV), pour surveiller en permanence l'activité de la pièce. En cas d'intrusion non autorisée, la sortie de ce système doit alerter le personnel de sécurité. S'il y a une vidéosurveillance, les enregistrements sont disponibles à des fins d'audit.

Sécuriser l'accès au panneau avant et au port console de NetScaler

Le serveur d'hébergement NetScaler ou VPX doit être déployé dans une baie ou une cage qui peut être verrouillée avec une clé appropriée, ou d'autres méthodes physiques. Le verrouillage empêche l'accès aux ports physiques du NetScaler ou, dans un déploiement VPX, à la console de l'hôte de virtualisation.

Protection de l'alimentation électrique

NetScaler (ou le serveur d'hébergement) doit être protégé par une alimentation sans interruption appropriée. En cas de panne de courant, l'alimentation sans interruption assure le fonctionnement continu de NetScaler, ou permet un arrêt contrôlé d'un NetScaler physique ou virtuel. L'utilisation d'une alimentation sans interruption contribue également à la protection contre les surtensions.

Protection des clés cryptographiques

Si une protection supplémentaire est requise pour les clés cryptographiques de votre déploiement, envisagez l'utilisation d'un NetScaler conforme à la norme FIPS 140-2 Niveau 2. La plateforme

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

FIPS utilise un module de sécurité matérielle pour protéger les clés cryptographiques critiques de NetScaler contre tout accès non autorisé.

Meilleures pratiques de sécurité NetScaler

Effectuer les mises à jour logicielles de NetScaler

Nous recommandons qu'avant le déploiement, les clients s'assurent que leur NetScaler a été mis à jour avec les dernières versions du firmware. Lorsque la mise à jour est effectuée à distance, nous recommandons aux clients d'utiliser un protocole sécurisé, tel que SFTP ou HTTPS, pour mettre à niveau NetScaler.

Il est également conseillé aux clients de consulter les bulletins de sécurité relatifs à leurs produits NetScaler. Pour plus d'informations sur les bulletins de sécurité nouveaux et mis à jour, consultez la page Web des bulletins de sécurité NetScaler `<https://support.citrix.com/knowledge-center/search#/>` et envisagez de vous inscrire aux alertes pour les bulletins nouveaux et mis à jour `<https://support.citrix.com/user/alerts>`.

Sécuriser le système d'exploitation des serveurs hébergeant NetScaler VPX

NetScaler VPX peut s'exécuter soit en tant qu'appliance virtuelle sur un serveur de virtualisation standard, soit en tant qu'appliance virtuelle sur NetScaler SDX.

En plus d'appliquer les procédures de sécurité physique normales, vous devez protéger l'accès à l'hôte de virtualisation avec un contrôle d'accès basé sur les rôles et une gestion robuste des mots de passe. De plus, le serveur doit être mis à jour avec les derniers correctifs de sécurité pour le système d'exploitation dès qu'ils sont disponibles, et déployer un logiciel antivirus à jour sur le serveur, si cela s'applique au type de virtualisation. Les clients utilisant la plateforme NetScaler SDX pour héberger NetScaler VPX doivent s'assurer qu'ils utilisent la dernière version du firmware pour leur NetScaler SDX.

Réinitialiser la gestion hors bande (LOM) de NetScaler

Nous vous recommandons, avant de configurer le LOM pour une utilisation en déploiement de production, d'effectuer une réinitialisation d'usine du LOM pour restaurer les paramètres par défaut.

1. À l'invite de commande NetScaler, exécutez la commande suivante :

```
>ipmitool raw 0x30 0x41 0x1
```

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

REMARQUE :

L'exécution de cette commande réinitialise le LOM aux paramètres d'usine par défaut et supprime tous les certificats SSL. Pour obtenir des instructions sur la reconfiguration du port LOM, consultez Port de gestion hors bande de l'appliance NetScaler MPX.

2. Dans l'interface graphique du LOM, accédez à **Configuration > Certification SSL**, puis ajoutez un certificat et une clé privée.

   De plus, nous recommandons que la configuration utilisateur suivante soit effectuée à l'aide de l'interface graphique du LOM :

   - Accédez à **Configuration** > **Utilisateurs** > **Modifier l'utilisateur**, et modifiez le mot de passe du compte superutilisateur `nsroot`.
   - Accédez à **Configuration** > **Utilisateurs** > **Modifier l'utilisateur**, et créez des stratégies pour les utilisateurs, ou liez des stratégies existantes à ceux-ci.
   - Accédez à **Configuration** > **Contrôle d'accès IP** > **Ajouter**, et configurez le contrôle d'accès IP pour autoriser l'accès à la plage d'adresses IP connue.
   - Accédez à **Configuration** > **Utilisateurs** > **Modifier l'utilisateur**, et créez un compte superutilisateur alternatif et liez des stratégies à ce compte.

   Pour plus de détails sur la configuration LOM, consultez Configuration LOM.

Maintenance et suppression des données persistantes

Si un NetScaler est redéployé vers un autre environnement, mis hors service ou renvoyé dans le cadre d'un RMA, assurez-vous que les données persistantes sont correctement supprimées du NetScaler.

Pour plus d'informations sur ce processus, consultez Effacement de vos données avant d'envoyer l'appliance ADC à Citrix.

Directives de configuration

Lors de la configuration d'un NetScaler, tenez compte des directives de configuration suivantes :

- Sécurité réseau
- Sécurisation du trafic de transit sur NetScaler

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

Sécurité réseau

Lors du déploiement de NetScaler dans un environnement de production, nous recommandons d'apporter les modifications de configuration clés suivantes :

- N'exposez pas l'interface d'administration NetScaler (NSIP) à Internet.
- Le certificat SSL par défaut de NetScaler doit être remplacé.
- HTTPS (HTTP sur TLS) doit être utilisé lors de l'accès à l'interface graphique et l'interface HTTP par défaut doit être désactivée.

La section suivante fournit plus d'informations sur ces considérations clés, en plus des modifications supplémentaires recommandées.

Considérations clés en matière de sécurité réseau

N'exposez pas l'adresse IP NSIP et l'adresse IP du service de gestion à Internet :

Nous recommandons que l'adresse IP de gestion NetScaler (NSIP) et l'adresse IP du service de gestion de SDX ne soient pas exposées à l'Internet public et soient déployées derrière un pare-feu d'inspection de paquets (SPI) avec état approprié.

Remplacez le certificat TLS par défaut de NetScaler :

Lors de la configuration initiale de NetScaler, les certificats TLS par défaut sont créés. Ces certificats ne sont pas destinés à être utilisés dans des déploiements de production et doivent être remplacés.

Nous recommandons aux clients de configurer NetScaler pour utiliser des certificats provenant soit d'une autorité de certification (CA) réputée, soit des certificats appropriés de votre autorité de certification d'entreprise.

Lorsqu'il est lié à un serveur virtuel public, un certificat TLS valide provenant d'une autorité de certification réputée simplifie l'expérience utilisateur pour les applications web accessibles via Internet ; les navigateurs web des utilisateurs ne nécessitent aucune interaction utilisateur lors de l'établissement d'une communication sécurisée avec le serveur web. Pour remplacer le certificat NetScaler par défaut par un certificat CA approuvé, consultez l'article CTX122521 du Centre de connaissances : « Comment remplacer le certificat par défaut d'une appliance NetScaler par un certificat CA approuvé qui correspond au nom d'hôte de l'appliance. »

Alternativement, il est possible de créer et d'utiliser des certificats TLS personnalisés et des clés privées. Bien que cette action puisse fournir un niveau équivalent de sécurité de la couche de transport, elle nécessite que les certificats TLS soient distribués aux utilisateurs et qu'une

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

interaction utilisateur soit requise lors de l'établissement des connexions au serveur web. Pour plus d'informations sur la création de certificats personnalisés, consultez l'article CTX121617 du Centre de connaissances : Comment créer et installer des certificats auto-signés sur une appliance NetScaler.

Plus d'informations sur la gestion et la configuration des certificats TLS sont disponibles dans la section « Recommandations TLS de NetScaler » de ce guide.

Désactiver l'accès HTTP à l'interface d'administration :

Pour protéger le trafic vers l'interface administrative et l'interface graphique de NetScaler, NetScaler doit être configuré pour utiliser HTTPS. Effectuez les étapes suivantes :

- Créez une paire de clés RSA privée et publique de 2048 bits ou plus et utilisez ces clés pour HTTPS et SSH afin d'accéder à l'adresse IP de NetScaler, en remplaçant la paire de clés RSA privée et publique de 512 bits fournie en usine.
- Configurez NetScaler pour qu'il utilise uniquement des suites de chiffrement fortes et modifiez l'ensemble de suites de chiffrement 'DEFAULT' en suites de chiffrement fortes sur NetScaler. Nous vous recommandons d'utiliser la liste des suites de chiffrement TLS approuvées dans la section 3.3 de la publication spéciale NIST 800-52 (révision 1). Ce document peut être trouvé sur le site Web du NIST à l'adresse suivante : `<https://www.nist.gov/publications/guidelines-selection-configuration-and-use-transport-layer-security-tls-implementations?pub_id=915295>`
- Configurez NetScaler pour utiliser l'authentification par clé publique SSH afin d'accéder à l'interface d'administration. N'utilisez pas les clés par défaut de NetScaler. Créez et utilisez votre propre paire de clés RSA privée et publique de 2048 bits. Pour plus d'informations, consultez l'article CTX109011 du Knowledge Center : Comment sécuriser l'accès SSH à l'appliance NetScaler avec l'authentification par clé publique et la documentation produit NetScaler : Authentification basée sur les clés SSH pour les utilisateurs du système local
- Une fois que NetScaler a été configuré pour utiliser ces nouveaux certificats, l'accès HTTP à l'interface de gestion GUI peut être désactivé avec la commande suivante :

```
set ns ip <NSIP> -gui SECUREONLY
```

Autres considérations relatives à la sécurité réseau

Limiter l'accès shell VPX des administrateurs VPX qui ne sont pas autorisés à gérer le SDX :

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

Dans les situations où il est souhaitable qu'une personne différente administre un VPX par rapport au service de gestion, l'administrateur du service de gestion doit créer un utilisateur administrateur VPX qui a un accès shell limité sur le VPX et ne fournir le compte d'utilisateur administrateur restreint qu'à l'administrateur VPX.

Certaines opérations peuvent nécessiter un accès shell (comme l'administration des certificats SSL). Cependant, seules les personnes autorisées à administrer le SVM doivent se voir accorder l'accès au shell de l'instance VPX. Les commandes de niveau RBAC, énumérées plus loin dans cette section, peuvent être attribuées à ces comptes. Ces recommandations sont applicables à tous les workflows de gestion SVM-IP/VPX-NSIP (L2/L3) et doivent être suivies à des fins d'audit d'accès sécurisé.

Les étapes suivantes peuvent être utilisées pour supprimer l'accès shell d'un administrateur VPX.

Sécurisation d'une instance VPX existante :

1. Connectez-vous à l'interface de ligne de commande VPX en tant que `nsroot` ou superutilisateur.

   Nous vous recommandons de ne pas utiliser le compte `nsroot` et de créer plutôt un compte superutilisateur. Lorsque vous utilisez le compte `nsroot`, assurez-vous que les mots de passe sont forts et contiennent des caractères spéciaux. Pour plus de détails sur les mots de passe forts, consultez Administration et gestion.

   - Créez un utilisateur et une politique RBAC dans une instance VPX sur NetScaler SDX.
   - Lier cet utilisateur à la politique.

```
> add system user userabc

Enter password:

Confirm password:

Done

> bind system user userabc superuser 2

Done

> add system cmdpolicy shell deny (shell)

Done
```

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

```
> bind system user userabc shell 1

Done
```

REMARQUE :

Dans cet exemple, le système `cmdpolicy` (ex : nom `cmdpolicy` : shell) est créé pour refuser l'accès au shell. Cette politique est liée à l'utilisateur `userabc` avec une priorité élevée. Le superutilisateur par défaut `cmdpolicy` est également lié à l'utilisateur système avec une priorité inférieure. Avec cette configuration, le nouvel utilisateur système dispose des politiques RBAC de superutilisateur, mais l'accès au shell est refusé.

2. Connectez-vous en tant que nouvel utilisateur système et effectuez les actions suivantes :

   - Vérifiez que l'utilisateur actuel a appliqué les politiques RBAC.
   - Exécutez toutes les commandes que l'utilisateur est autorisé à exécuter. (par exemple, `show system cmdpolicy`)
   - Exécutez la commande `shell` pour vérifier que l'accès au shell est restreint.

   connexion en tant que : `userabc`

   Message de bannière de pré-authentification du serveur :

```
|
#########################################################################
######

> ##

| #

>  #

| #        WARNING: Access to this system is for authorized users only

>  #

| #         Disconnect IMMEDIATELY if you are not an authorized user!
```

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

```
>  #

| #

>  #

|
##############################################################################
######

> ##

|

End of banner message from server

Keyboard-interactive authentication prompts from server:

| Password:

End of keyboard-interactive prompts from server

Last login: Thu May 13 04:11:15 2021 from 10.10.1.1

Done
```

```
> whoami

    UserName:  userabc        LoggedIn:  "Thu May 13 04:18:50 2021"

Done
```

3. Dans la console de ce VPX, connectez-vous en tant que cet utilisateur et assurez-vous que l'accès au shell n'est pas autorisé pour cet utilisateur :

```
> shell

ERROR: Not authorized to execute this command [shell]
```

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

4. Connectez-vous en tant qu'utilisateur administrateur régulier (`nsroot`) et assurez-vous que l'accès au shell est autorisé :

```
> shell

Copyright (c) 1992-2013 The FreeBSD Project.

Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
1994

The Regents of the University of California. All rights reserved.



root@Zela-40G-10#
```

Sécurisation d'une nouvelle instance VPX :

1. Lorsqu'une nouvelle instance VPX est créée à partir de l'interface graphique du service de gestion, créez un utilisateur INSTANCE ADMIN et décochez la case **Accès Shell/SFTP/SCP**. Lors de la désactivation de l'accès au shell, `svm_access_policy` (action DENY) est explicitement lié à l'utilisateur administrateur d'instance spécifié.
2. Fournissez ces informations d'utilisateur à l'administrateur VPX. L'administrateur SDX doit conserver ce mot de passe administrateur `nsroot` et ne doit pas le partager avec l'administrateur VPX.

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

REMARQUES

.

- Pour modifier le mot de passe `nsroot`, connectez-vous au service de gestion, sélectionnez l'instance et modifiez le mot de passe. Ne modifiez jamais le mot de passe `nsroot` à partir de l'interface de ligne de commande VPX.
- Pour plus de détails sur les utilisateurs RBAC, consultez Utilisateur, groupes d'utilisateurs et stratégies de commande.
- Pour modifier le mot de passe de NetScaler à partir de SVM, consultez Modifier une instance NetScaler.
- Pour provisionner NetScaler avec l'administration d'instance, consultez Ajouter une instance NetScaler.

Désactiver le transfert de port SSH :

Le transfert de port SSH n'est pas requis par NetScaler. Si vous ne souhaitez pas utiliser cette fonctionnalité, nous vous recommandons de la désactiver en suivant les étapes suivantes :

1. Modifiez le fichier `/etc/sshd_config` en ajoutant la ligne suivante :

   AllowTcpForwarding no
2. Enregistrez le fichier et copiez-le dans le répertoire `/nsconfig` pour vous assurer que les modifications sont persistantes au cas où vous redémarrez pendant les tests.
3. Redémarrez le processus `sshd` en utilisant la commande suivante :

   ```
   kill -HUP `cat /var/run/sshd.pid`
   ```

Configurer NetScaler avec la haute disponibilité :

Dans les déploiements où un fonctionnement continu est requis, NetScaler peut être déployé dans une configuration de haute disponibilité. Une telle configuration assure un fonctionnement continu si l'un des NetScaler cesse de fonctionner ou nécessite une mise à niveau hors ligne.

Pour plus d'informations sur la configuration d'une configuration de haute disponibilité, consultez Configuration de la haute disponibilité.

Configurer une communication sécurisée entre les appliances homologues :

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

Si vous avez configuré votre NetScaler dans une configuration de haute disponibilité, de cluster ou de GSLB, sécurisez la communication entre les appliances NetScaler.

Pour sécuriser la communication, nous vous recommandons de modifier le compte utilisateur interne ou le mot de passe du nœud RPC, et d'activer les options **Secure** et **-validateCert**. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. L'option `-validateCert` permet la validation du certificat de serveur pour la communication RPC, telle que la synchronisation de configuration ou la propagation de configuration entre les nœuds.

```
set ns rpcNode <IP> -secure ON -validateCert YES
```

L'option `-validateCert` est valide uniquement si le paramètre `-secure` est défini sur `ON`.

Pour valider le certificat de serveur, le fichier CA `/nsconfig/ssl/certs/ca.pem` doit être configuré. Par conséquent, configurez le fichier CA `/nsconfig/ssl/certs/ca.pem` avec le certificat CA homologue, qui est utilisé pour signer le certificat de serveur pour le service `nsrpcs-127.0.0.1-3008`. Pour plus d'informations, consultez Modifier un mot de passe de nœud RPC.

Les fonctionnalités NetScaler peuvent également utiliser une authentification basée sur des clés SSH pour la communication interne lorsque le compte utilisateur interne est désactivé. Dans de tels cas, le nom de la clé doit être défini comme « ns_comm_key ». Pour plus d'informations, consultez Accéder à une appliance NetScaler à l'aide de clés SSH et sans mot de passe.

Modifier les mots de passe par défaut :

Pour une sécurité renforcée, nous vous recommandons de modifier les mots de passe de l'administrateur et du compte utilisateur interne ou du nœud RPC pour les déploiements sur site et dans le cloud. Il est conseillé de changer fréquemment les mots de passe.

- Mot de passe administrateur : consultez Modifier le mot de passe administrateur.
- Compte utilisateur interne ou mot de passe du nœud RPC : consultez Modifier un mot de passe de nœud RPC.

REMARQUE

Nous vous recommandons également de désactiver le compte utilisateur interne et d'utiliser plutôt l'authentification par clé.

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

Configurer les domaines de sécurité réseau et les VLAN :

Nous vous recommandons de séparer le trafic réseau vers l'interface de gestion NetScaler, physiquement ou logiquement, du trafic réseau normal. La meilleure pratique recommandée est d'avoir trois VLAN :

- VLAN Internet externe
- VLAN de gestion
- VLAN de serveur interne

Nous recommandons de configurer le réseau pour que le port LOM fasse partie du VLAN de gestion.

Lors du déploiement de NetScaler en mode deux bras, dédiez un port spécifique à un réseau spécifique. Si le marquage VLAN et la liaison de deux réseaux à un seul port sont nécessaires, vous devez vous assurer que les deux réseaux ont des niveaux de sécurité identiques ou similaires.

Si les deux réseaux ont des niveaux de sécurité différents, le marquage VLAN ne doit pas être utilisé. Au lieu de cela, envisagez de dédier un port pour chaque réseau spécifique et d'utiliser des VLAN indépendants répartis sur les ports de NetScaler.

Envisagez d'utiliser NetScaler Web App Firewall : Un NetScaler sous licence Premium Edition fournit un NetScaler Web App Firewall intégré qui utilise un modèle de sécurité positif et apprend automatiquement le comportement approprié des applications pour la protection contre les menaces telles que l'injection de commandes, l'injection SQL et le Cross Site Scripting.

Lorsque vous utilisez NetScaler Web App Firewall, les utilisateurs peuvent ajouter une sécurité supplémentaire à l'application web sans modifications de code et avec un minimum de changements de configuration. Pour plus d'informations, consultez Introduction à NetScaler Web Application Firewall.

Restreindre l'accès des applications non-administratives : Exécutez la commande suivante pour restreindre la capacité des applications non-administratives à accéder à NetScaler.

```
set ns ip <NSIP> -restrictAccess enabled
```

Déploiement de cluster sécurisé :

Pour sécuriser les déploiements de cluster, nous vous recommandons d'activer la fonction de pulsations sécurisées (secure heartbeats) qui offre une protection contre les attaques réseau.

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

REMARQUE :

La fonction de pulsations sécurisées (secure heartbeats) est disponible à partir de la version 14.1 build 12.x de NetScaler.

Pour activer la fonction de pulsations sécurisées, connectez-vous à l'adresse IP du cluster et exécutez la commande suivante :

```
set cluster instance <clId> secureHeartbeats ENABLED
```

Pour plus d'informations sur la fonction de pulsations sécurisées, consultez Configurer les pulsations sécurisées.

Pour sécuriser la communication, nous vous recommandons de modifier le compte utilisateur interne ou le mot de passe du nœud RPC, et d'activer les options **Secure** et **-validateCert**.

```
set rpcnode <ip> -secure on -validateCert YES
```

Remarque : D'autres configurations peuvent être nécessaires. Pour plus d'informations, consultez les rubriques **Clustering** dans la Documentation du produit.

Lorsqu'il est déployé dans un cluster L3, les paquets entre les nœuds NetScaler sont échangés via un tunnel GRE non chiffré qui utilise les adresses NSIP des nœuds source et destination pour le routage. Lorsque l'échange a lieu sur Internet, en l'absence de tunnel IPsec, les NSIP sont exposées sur Internet, ce qui n'est pas recommandé car cela ne respecte pas les meilleures pratiques de sécurité pour NetScaler.

Nous recommandons aux clients d'établir leur propre solution IPsec pour utiliser le cluster via la fonctionnalité L3.

Si la fonctionnalité de transfert IP n'est pas utilisée, utilisez la commande suivante pour désactiver le mode L3 :

```
disable ns mode L3
```

Utiliser un MEP sécurisé pour l'équilibrage de charge global des serveurs (GSLB) : Pour chiffrer le MEP entre NetScaler pour GSLB, exécutez la commande suivante depuis le NSCLI :

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

```
set rpcNode <GSLB Site IP> -secure yes
```

Sécuriser le cookie de persistance de l'équilibrage de charge :

Nous recommandons de chiffrer le cookie de persistance de l'équilibrage de charge en plus du canal SSL/TLS. Pour plus d'informations, consultez Persistance des cookies HTTP.

Paramètre Helloverifyrequest pour atténuer l'attaque par amplification DDoS DTLS :

À partir des versions NetScaler 12.1 build 62.x et 13.0 build 79.x, le paramètre `helloverifyrequest` est activé par défaut. L'activation du paramètre `helloverifyrequest` sur le profil DTLS permet d'atténuer le risque qu'un attaquant ou des bots ne saturent le débit réseau, ce qui pourrait entraîner un épuisement de la bande passante sortante. Autrement dit, cela aide à atténuer l'attaque par amplification DDoS DTLS.

Pour afficher l'état du paramètre `helloverifyrequest`, à l'invite de commande CLI, tapez :

```
show dtlsProfile
```

Sécurisation du trafic de transit sur NetScaler®

Les paramètres du mode infrastructure peuvent être utilisés pour sécuriser le trafic de transit sur NetScaler. Ces paramètres du mode infrastructure offrent un niveau de sécurité de base sans interrompre aucune application. La liste suivante récapitule les paramètres du mode infrastructure disponibles.

- Protection de l'état de session
- Protection contre la fixation de session (activer HTTP Only)
- HSTS (activer HTTP Strict Transport Security (HSTS))
- Authentification forte
- SSL de bout en bout préféré
- Proxy HTTPS / Refuser tout autre trafic

Protection de l'état de session :

Recommandation : Activé NetScaler : Activé par défaut pour la plupart des entités

Le paramètre **Protection de l'état de session** est activé par défaut et ne nécessite aucune configuration spécifique. Lorsque NetScaler est configuré pour proxifier une connexion. Par

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

exemple, lorsque le flux sélectionne un serveur virtuel configuré ou un service de type TCP ou supérieur, NetScaler crée une session avec état. NetScaler continue de maintenir l'état de ces connexions et seuls les paquets qui entrent dans cette machine d'état sont traités. Les autres paquets sont soit abandonnés, soit réinitialisés.

Les entités de type service suivantes atteignent ce comportement avec état sur NetScaler.

- ADNS_TCP
- DIAMETER, DNS_TCP
- FTP-c
- GRE-c
- HTTP
- MYSQL, MSSQL
- NNTP
- ORACLE
- PUSH, PPTP
- RTSP, RDP
- SIP_SSL, SIP_TCP
- SMPP
- SSL, SSL_BRIDGE, SSL_DIAMETER, SSL_PUSH
- SSL_TCP, SYSLOG_TCP
- TCP
- ADNS_TCP
- RNAT (rnat_tcpproxy est activé)

Protection contre la fixation de session (en activant l'indicateur HttpOnly ou en ajoutant une politique de réécriture) :

Recommandation : Pour activer HttpOnly pour les cookies définis par NetScaler ou le serveur principalNetScaler : Activé par défaut pour les cookies insérés par NetScaler, possible via la réécriture pour les cookies définis par le serveur principal.

HttpOnly : Lorsque vous marquez un cookie avec l'attribut HttpOnly, cela indique au navigateur que ce cookie ne doit être accessible que par le serveur. Toute tentative d'accès au cookie à partir du script client est strictement interdite. Les cookies HttpOnly, s'ils sont correctement implémentés,

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

rendent beaucoup plus difficiles à réaliser de vastes catégories d'attaques courantes de script intersite.

Voici un exemple de cookie avec l'attribut HttpOnly défini :

```
Set-Cookie: ASP.NET_SessionId=ig2fac55; path=/; HttpOnly
```

Les cookies insérés par NetScaler pour la persistance d'insertion de cookies, par défaut, définissent l'attribut HttpOnly pour indiquer que le cookie n'est pas scriptable et ne doit pas être révélé à l'application cliente. Par conséquent, un script côté client ne peut pas accéder au cookie, et le client n'est pas vulnérable aux scripts intersites.

Pour activer le paramètre d'attribut HttpOnly à l'aide de l'interface de ligne de commande :

À l'invite de commande, tapez :

```
set lb parameter -HttpOnlyCookieFlag (ENABLED)
```

Utilisation de la politique de réécriture pour insérer Secure et HttpOnly pour les cookies :

La politique de réécriture insère Secure et HTTP uniquement pour les cookies envoyés par le serveur principal.

Remarque : Les cookies Secure et HttpOnly peuvent être combinés pour les VIP SSL. Pour les VIP non-SSL, on peut insérer l'attribut HttpOnly.

Avec NetScaler, on peut inclure les attributs HTTP only et Secure pour les cookies définis par le serveur.

- HttpOnly - Cette option sur un cookie oblige les navigateurs web à renvoyer le cookie en utilisant uniquement le protocole HTTP (ou HTTPS) ; les méthodes non-HTTP telles que les références JavaScript document.cookie ne peuvent pas accéder au cookie. Cette option aide à prévenir le vol de cookies dû aux scripts intersites.
- Secure - Cette option sur un cookie oblige les navigateurs web à ne renvoyer la valeur du cookie que lorsque la transmission est chiffrée par SSL. Cette option peut être utilisée pour prévenir le vol de cookies par écoute clandestine de la connexion.

Créer une politique de réécriture à l'aide de l'interface de ligne de commande

1. Activez la fonctionnalité de réécriture, si elle n'est pas déjà activée.

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

```
enable feature REWRITE
```

2. Créez une action de réécriture (cet exemple est configuré pour définir les attributs Secure et HttpOnly. Si l'un d'eux est manquant, modifiez-le si nécessaire pour d'autres combinaisons).

```
add rewrite action <action name> replace_all http.RES.full_Header
"\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;
HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)"
-bypassSafetyCheck YES
```

Exemple :

```
add rewrite action act_cookie_Secure replace_all http.RES.full_Header
"\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;
HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)"



or



add rewrite action act_cookie_Secure replace_all http.RES.full_Header
"\"path=/; Secure; HttpOnly\"" -search "regex(re!(path=/\\; Secure;
HttpOnly)|(path=/\\; Secure)|(path=/\\; HttpOnly)|(path=/)!)"
-bypassSafetyCheck YES
```

REMARQUE :

À partir de la version 13.1 de NetScaler, le paramètre `bypassSafetyCheck` n'est pas applicable. Cependant, pour les versions antérieures à 13.1, ce paramètre est pris en charge.

3. Créez une stratégie de réécriture pour déclencher l'action.

```
add rewrite policy <policy name> "http.RES.HEADER(\"Set-
Cookie\").EXISTS" <action name>
```

Exemple :

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

```
add rewrite policy rw_force_secure_cookie "http.RES.HEADER(\"Set-
Cookie\").EXISTS" act_cookie_Secure
```

4. Lie la stratégie de réécriture au serveur virtuel à sécuriser (si l'option Sécurisé est utilisée, un serveur virtuel SSL doit être utilisé).

   ```
   bind lb vserver <vserver name> - <policy name> -priority <priority
   number> -gotoPriorityExpression NEXT -type RESPONSE
   ```

   Exemple :

   ```
   bind lb vserver mySSLVServer -policyName rw_force_secure_cookie
   -priority 100 -gotoPriorityExpression NEXT -type RESPONSE
   ```

   Pour plus d'informations, consultez `<https://support.citrix.com/article/CTX138055>`.

HSTS (activer la sécurité de transport stricte HTTP (HSTS)) :

Pour activer HSTS à l'aide de la ligne de commande NetScaler :

À l'invite de commande, tapez :

```
set ssl vserver <vServerName> -HSTS ( ENABLED ) maxage <positive_integer>
-IncludeSubdomains ( YES | NO)
```

OU

```
set ssl profile <name> -HSTS ( ENABLED ) -maxage <positive_integer>
-IncludeSubdomains ( YES | NO )
```

Pour plus d'informations, consultez les rubriques suivantes.

- Configurer la prise en charge de la sécurité de transport stricte HTTP (HSTS).
- `<https://support.citrix.com/article/CTX205221>`

Authentification forte :

L'authentification forte (ou authentification multifacteur – MFA) doit être activée pour tous les accès aux données sensibles, aux applications et à l'administration.

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

Pour plus de détails sur la configuration de l'authentification multifacteur pour les applications sensibles, consultez (/fr-fr/citrix-adc/current-release/aaa-tm/authentication-methods/multi-factor-nfactor-authentication.html) .

SSL de bout en bout préféré :

Il est recommandé d'avoir le SSL à la fois sur le front-end et le back-end. Les anciennes versions de protocole non sécurisées, telles que SSLv3, TLS 1.0 et TLS 1.1, peuvent être désactivées sur les entités SSL. Seuls TLS 1.2 et TLS 1.3 peuvent être activés. Cela peut être fait au niveau de l'entité SSL ou au niveau du profil, et toutes les entités SSL héritent des paramètres SSL du profil.

Désactiver les versions de protocole non sécurisées et activer les versions sécurisées sur les entités SSL à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ssl vserver <vServerName> -ssl2 DISABLED   -ssl3  DISABLED   -tls1
DISABLED   -tls11   DISABLED    -tls12   ENABLED    -tls13   ENABLED



set ssl service <vServiceName> -ssl2 DISABLED   -ssl3  DISABLED   -tls1
DISABLED   -tls11   DISABLED    -tls12   ENABLED    -tls13   ENABLED
```

Si le profil SSL est activé, utilisez la commande suivante :

```
set ssl profile <frontend profile> -ssl3  DISABLED   -tls1   DISABLED  -
tls11  DISABLED   -tls12   ENABLED    -tls13   ENABLED



set ssl profile <backend profile> -ssl3  DISABLED   -tls1   DISABLED  -
tls11  DISABLED   -tls12   ENABLED    -tls13   ENABLED
```

**Remarque :

> Nous recommandons d'activer TLS 1.3 à l'aide du profil plutôt que de l'activer sur les entités de serveur virtuel. Pour plus d'informations, consultez Prise en charge du protocole TLS 1.3.

Suites de chiffrement recommandées par NetScaler :

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

Les chiffrements suivants pris en charge par NetScaler n'incluent aucun composant figurant sur la liste de « rejet obligatoire ». Ces chiffrements sont organisés par échange de clés (RSA, DHE et ECDHE), les plus performants étant placés en haut et les plus sécurisés en bas :

Suites de chiffrement d'échange de clés RSA recommandées :

- TLS1-AES-128-CBC-SHA
- TLS1-AES-256-CBC-SHA
- TLS1.2-AES-128-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES256-GCM-SHA384

Suites de chiffrement d'échange de clés DHE recommandées :

- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES128-GCM-SHA256
- TLS1.2-DHE-RSA-AES256-GCM-SHA384

Suites de chiffrement d'échange de clés ECDHE recommandées :

- TLS1-ECDHE-RSA-AES128-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384

Suites de chiffrement recommandées par ordre de préférence :

La liste suivante d'algorithmes de chiffrement inclut les échanges de clés RSA, DHE et ECDHE. Elle offre le meilleur compromis entre sécurité, performances et compatibilité.

1. TLS1.2-AES128-GCM-SHA256

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

2. TLS1.2-AES-128-SHA256
3. TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
4. TLS1.2-ECDHE-RSA-AES-128-SHA256
5. TLS1-ECDHE-RSA-AES128-SHA
6. TLS1.2-DHE-RSA-AES128-GCM-SHA256
7. TLS1.2-DHE-RSA-AES-128-SHA256
8. TLS1-DHE-RSA-AES-128-CBC-SHA
9. TLS1-AES-128-CBC-SHA

Profil SSL sécurisé et algorithmes de chiffrement sécurisés :

Nous vous recommandons de lier le profil frontal sécurisé (ns_default_ssl_profile_secure_frontend) à votre serveur virtuel SSL. Un alias de chiffrement sécurisé est ajouté et lié au profil frontal sécurisé. Pour lister les chiffrements qui font partie de cet alias, à l'invite de commande, tapez :

```
show cipher SECURE



    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1

           Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
Mac=AEAD   HexCode=0xc030

    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2

           Description: TLS 1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
Mac=AEAD   HexCode=0xc02f

    3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
 Priority : 3

           Description: TLS 1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
Mac=AEAD   HexCode=0xc02c

    4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
 Priority : 4

           Description: TLS 1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
```

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

```
Mac=AEAD   HexCode=0xc02b

Done
```

Pour plus d'informations sur le profil frontal sécurisé, consultez Profil frontal sécurisé.

Les protocoles inférieurs à TLS 1.2 sont désactivés sur les services internes SSL. Si le profil par défaut (amélioré) est activé, alors le profil ns_default_ssl_profile_internal_frontend_service est lié aux services internes SSL et les protocoles SSLv3, TLS 1.0, TLS 1.1 et TLS 1.3 sont désactivés dans le profil.

Proxy HTTPS / refuser tout autre trafic :

Dans la mesure du possible, utilisez des VIP SSL pour un meilleur chiffrement des données, en utilisant des versions SSL sécurisées (TLS 1.2 ou TLS 1.3) et des chiffrements sécurisés. Le TPS SSL et le débit SSL doivent être pris en compte lors de l'activation du SSL pour les VIP et les services SSL back-end.

Administration et gestion

Cette section fournit des exemples de modifications de configuration spécifiques qui peuvent être appliquées pour renforcer la sécurité de NetScaler et NetScaler SDX. Des conseils supplémentaires sur les meilleures pratiques de configuration de NetScaler sont disponibles dans l'article Paramètres recommandés et meilleures pratiques pour une implémentation générique d'une appliance NetScaler.

Consultez les rubriques suivantes pour plus d'informations.

- Comptes système et utilisateur
- Journalisation et surveillance
- Configuration LOM
- Applications et services
- Recommandations de sécurité DNSSEC
- Configuration héritée
- Configurer la vérification du certificat de conformité NDCPP

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

Comptes système et utilisateur

Modifier le mot de passe du compte superutilisateur : Vous ne pouvez pas supprimer le superutilisateur administrateur intégré (`nsroot`). Par conséquent, modifiez le mot de passe par défaut de ce compte pour un mot de passe sécurisé. Pour modifier le mot de passe par défaut de l'utilisateur admin, procédez comme suit :

1. Connectez-vous en tant que superutilisateur et ouvrez l'utilitaire de configuration.
2. Dans le volet de navigation, développez le nœud Systèmes.
3. Sélectionnez le nœud Utilisateurs.
4. Sur la page Utilisateurs système, sélectionnez l'utilisateur `nsroot`.
5. Sélectionnez Modifier le mot de passe.
6. Saisissez le mot de passe requis dans les champs Mot de passe et Confirmer le mot de passe.
7. Cliquez sur OK.

Créer un compte superutilisateur alternatif : Pour créer un compte superutilisateur, exécutez les commandes suivantes :

```
add system user <newuser> <password>



bind system user <newuser> superuser 0
```

Utilisez ce compte superutilisateur au lieu du compte superutilisateur par défaut `nsroot`.

Pour les déploiements NetScaler SDX, un administrateur doit modifier les informations d'identification par défaut de NetScaler SDX et de sa console de gestion GUI après la configuration initiale. Pour modifier le mot de passe de l'utilisateur par défaut, procédez comme suit :

1. Connectez-vous en tant que superutilisateur et ouvrez l'utilitaire de configuration.
2. Dans le volet de navigation, développez le nœud Systèmes.
3. Sélectionnez le nœud Utilisateurs.
4. Sur la page Utilisateurs système, sélectionnez l'utilisateur par défaut.
5. Sélectionnez Modifier.
6. Saisissez le mot de passe requis dans les champs Mot de passe et Confirmer le mot de passe.
7. Cliquez sur OK.

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

Mot de passe fort pour l'utilisateur système :

Nous recommandons d'utiliser un mot de passe fort pour les comptes d'utilisateurs système créés dans NetScaler. Voici des exemples d'exigences de complexité de mot de passe :

- Le mot de passe doit avoir une longueur minimale de huit caractères.
- Le mot de passe ne doit pas contenir de mots du dictionnaire ou une combinaison de mots du dictionnaire.
- Le mot de passe doit inclure au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Des mots de passe forts peuvent être imposés en définissant deux paramètres, l'un pour la longueur minimale des mots de passe et l'autre pour appliquer la complexité du mot de passe :

```
set system parameter -minpasswordlen <positive_integer> -

-strongpassword ( ENABLED | DISABLED )
```

Dans les déploiements où plusieurs administrateurs sont requis, envisagez d'utiliser une méthode d'authentification externe pour authentifier les utilisateurs, par exemple RADIUS, TACACS+ ou LDAP(S). Pour plus d'informations, consultez Authentification des utilisateurs externes.

Verrouiller le compte d'utilisateur système pour l'accès à la gestion : NetScaler vous permet de verrouiller un utilisateur système pendant 24 heures et de lui refuser l'accès. NetScaler prend en charge la configuration pour les utilisateurs système et les utilisateurs externes. À l'invite de commandes, tapez :

`set aaa parameter –persistentLoginAttempts DISABLED`

Maintenant, pour verrouiller un compte utilisateur, à l'invite de commandes, tapez :

`lock aaa user test`

Pour plus d'informations sur la configuration de cette fonctionnalité à l'aide de l'interface graphique, consultez Gestion des comptes utilisateur et des mots de passe.

Déverrouiller un compte utilisateur système verrouillé pour l'accès à la gestion : Les utilisateurs système et les utilisateurs externes peuvent être verrouillés pendant 24 heures à l'aide de la commande utilisateur de verrouillage d'authentification, d'autorisation et d'audit. Le NetScaler vous permet de déverrouiller l'utilisateur système verrouillé. À l'invite de commandes, tapez :

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

`unlock aaa user test` Pour plus d'informations sur la configuration de cette fonctionnalité à l'aide de l'interface graphique, consultez Gestion des comptes utilisateur et des mots de passe.

Désactiver l'accès à la gestion pour le compte utilisateur système : Lorsque l'authentification externe est configurée sur NetScaler et qu'en tant qu'administrateur, vous préférez refuser l'accès aux utilisateurs système pour se connecter à l'accès de gestion, vous devez désactiver l'option localAuth dans le paramètre système.

REMARQUE :

Le serveur externe doit être configuré.

À l'invite de commandes, tapez ce qui suit :

```
set system parameter localAuth <ENABLED|DISABLED>
```

Exemple :

`set system parameter localAuth DISABLED` Pour plus d'informations sur la configuration de cette fonctionnalité à l'aide de l'interface graphique, consultez Gestion des comptes utilisateur et des mots de passe.

Forcer le changement de mot de passe pour les utilisateurs administratifs : Pour l'authentification sécurisée `nsroot`, NetScaler invite l'utilisateur à changer le mot de passe par défaut pour un nouveau si l'option `forcePasswordChange` est activée dans le paramètre système. Vous pouvez modifier votre mot de passe `nsroot` à partir de la CLI ou de l'interface graphique, lors de votre première connexion avec les informations d'identification par défaut. À l'invite de commandes, tapez :

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

Pour un exemple de configuration de cette fonctionnalité, consultez Gestion des comptes utilisateur et des mots de passe.

Accéder au NetScaler à l'aide de clés SSH et sans mot de passe : Dans les déploiements où il est nécessaire d'administrer de nombreux appliances NetScaler, envisagez d'utiliser des clés SSH et aucun mot de passe. Pour plus d'informations sur la configuration de cette fonctionnalité, consultez Accéder à une appliance NetScaler à l'aide de clés SSH et sans mot de passe.

Créer la clé principale du système pour la protection des données : De Citrix ADC 12.1 à Citrix 13.0–71.44, il est nécessaire de créer une clé principale du système pour protéger certains

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

paramètres de sécurité, tels que les mots de passe des comptes de service requis pour l'authentification LDAP et les comptes utilisateur d'authentification, d'autorisation et d'audit stockés localement.

REMARQUE :

À partir de Citrix 13.0 build 76.31 et versions ultérieures, une clé principale système aléatoire est créée par défaut automatiquement lors du processus de mise à niveau. Assurez-vous de mettre à jour la KEK fréquemment conformément à la politique de mot de passe de l'organisation.

Pour créer la clé principale du système :

1. À l'aide de l'interface de ligne de commande (CLI), connectez-vous en tant qu'administrateur système.
2. Entrez la commande suivante :

```
create kek <passphrase>
```

Remarque :

- Une fois la commande `create kek` exécutée, la KEK est utilisée pour la plupart des chiffrements de mots de passe (les mots de passe des utilisateurs locaux ne sont pas chiffrés avec la KEK).
- Vous ne devez pas supprimer le fichier KEK. Si vous avez un accès shell et que vous supprimez les fichiers de fragments de clé par erreur, cela pourrait entraîner une perte de configuration, un échec de synchronisation, un échec de connexion. Notez ce qui suit.
  - Utilisez toujours un fichier de configuration plus ancien correspondant à la version installée lors de la rétrogradation ; sinon, la connexion, la configuration source, la synchronisation, le basculement pourraient échouer.
  - Si l'un des fichiers de fragments de clé est perdu ou corrompu, le chiffrement/déchiffrement des données sensibles échoue, ce qui pourrait à son tour entraîner une perte de configuration, un échec de synchronisation, un échec de connexion.
- La phrase secrète doit comporter au moins 8 caractères.

Mettre à jour la clé de chiffrement de clé sur un NetScaler déployé :

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

NetScaler prend en charge la mise à jour de la KEK sur un ADC déployé. Utilisez la commande suivante pour mettre à jour la KEK.

```
update kek -level <basic | extended>
```

La commande de mise à jour de la KEK est prise en charge uniquement sur l'interface NSIP. La commande prend en charge les deux options suivantes.

- **Basique** : Sauvegarde les anciennes clés, crée des clés et répond. Si l'une des mises à jour de fichiers échoue, le système signale une erreur et revient à l'état d'origine.
- **Étendu** : Sauvegarde les anciennes clés et crée de nouvelles clés. Met à jour les fichiers de configuration tels que ns.conf et ns.conf.0 sous les partitions par défaut et non par défaut. Pendant la mise à jour, bloque toutes les modifications de configuration. Une fois la mise à jour terminée, NetScaler répond. Si l'une de ces mises à jour de fichiers échoue, le système signale une erreur et revient à l'état d'origine.

Auparavant, NetScaler ne prenait en charge que la KEK par nœud par défaut. Il n'y avait aucune option pour mettre à jour la KEK.

En tant que bonne pratique de sécurité, la KEK doit être modifiée fréquemment conformément à la politique de mot de passe de l'organisation.

Utiliser les listes de contrôle d'accès :

Par défaut, tous les protocoles et ports, y compris l'interface graphique et SSH, sont accessibles sur NetScaler. Les listes de contrôle d'accès (ACL) peuvent vous aider à gérer NetScaler en toute sécurité en n'autorisant que les utilisateurs explicitement spécifiés à accéder aux ports et aux protocoles.

Recommandations pour contrôler l'accès à NetScaler :

- Envisagez d'utiliser NetScaler Gateway pour limiter l'accès à NetScaler à l'interface graphique uniquement. Pour les administrateurs qui ont besoin de méthodes d'accès en plus de l'interface graphique, le NetScaler Gateway doit être configuré avec une ACL 'DENY' par défaut pour les ports 80, 443 et 3010, mais avec un 'ALLOW' explicite pour les adresses IP fiables afin d'accéder à ces ports.

Cette politique peut être étendue pour être utilisée avec la plage d'adresses IP fiables à l'aide de la commande NSCLI suivante :

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

```
add acl local_access allow -srcip 192.168.0.1-192.168.0.3 -destip
192.168.0.1-192.168.0.3



apply acls
```

- Si vous utilisez SNMP, autorisez explicitement le trafic SNMP avec une ACL. Voici un ensemble d'exemples de commandes :

```
add acl snmp1-ssh ALLOW -srcip 10.0.0.1-10.0.0.20 -destip
192.168.0.2-192.168.0.3 -destport 161 -protocol udp



add acl snmp2-ssh ALLOW -srcip 172.16.0.1-172.16.0.20 -destip
192.168.0.2-192.168.0.3 –destport 161 -protocol udp



apply acls
```

Dans l'exemple précédent, la commande donne accès à toutes les requêtes SNMP aux deux sous-réseaux définis, même si les requêtes sont destinées à la communauté définie de manière appropriée.

Vous pouvez activer les fonctions de gestion sur les adresses NSIP et SNIP. Si elles sont activées, accordez l'accès aux adresses NSIP, SNIP, avec des ACL pour protéger l'accès aux fonctions de gestion. L'administrateur peut également configurer NetScaler de manière à ce qu'il ne soit pas accessible avec la commande ping.

- Open Shortest Path First (OSPF) et IPSEC ne sont pas des protocoles basés sur TCP ou UDP. Par conséquent, si vous avez besoin que NetScaler prenne en charge ces protocoles, autorisez explicitement le trafic utilisant ces protocoles à l'aide d'une ACL. Exécutez la commande suivante pour définir une ACL afin de spécifier OSPF et IPSEC par numéros de protocole :

```
add acl allow_ospf allow -protocolnumber 89
```

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

```
add acl allow_ipsec allow -protocolnumber 50
```

- Si un service Web XML-API est utilisé, effectuez les tâches suivantes pour sécuriser l'interface API :
- Accordez l'autorisation à l'hôte d'accéder à l'interface à l'aide d'une ACL. Par exemple, exécutez les commandes suivantes pour permettre aux hôtes de la plage d'adresses IP 10.0.0.1-20 et 172.16.0.1-20 d'accéder à l'interface XML-API :

```
add acl xml-api1 ALLOW -srcip 10.0.0.1-10.0.0.20 -destip
192.168.0.2-192.168.0.3 -destport 80 -protocol tcp



add acl xml-api2 ALLOW -srcip 172.16.0.1-172.16.0.20 -destip
192.168.0.2-192.168.0.3 -destport 80 -protocol tcp



apply acls
```

- Pour appliquer des ACL aux ports internes, utilisez la commande suivante :

```
set l3param -implicitACLAllow DISABLED
```

REMARQUE :

La valeur par défaut de la commande *implicitACLAllow* est **ACTIVÉE**.

- Pour supprimer les ACL des ports internes, utilisez la commande suivante :

```
set l3param -implicitACLAllow ENABLED
```

- Vous pouvez renforcer la sécurité en utilisant un certificat côté client. Pour plus d'informations sur les certificats côté client et l'authentification client, consultez Authentification client ou l'article du Knowledge Center CTX214874 : Comment créer et utiliser des certificats clients sur une appliance NetScaler avec le firmware 10.1 et versions ultérieures.

Utiliser le contrôle d'accès basé sur les rôles pour les utilisateurs administratifs :

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

NetScaler inclut quatre stratégies de commande ou rôles tels qu'opérateur, lecture seule, réseau et superutilisateur. Vous pouvez également définir des stratégies de commande, créer différents comptes d'administration pour différents rôles et attribuer aux comptes les stratégies de commande nécessaires au rôle. Voici un ensemble d'exemples de commandes pour restreindre l'accès en lecture seule à l'utilisateur en lecture seule :

```
add system user readonlyuser



bind system user readonlyuser read-only 0
```

Pour plus d'informations sur la configuration des utilisateurs, des groupes d'utilisateurs ou des stratégies de commande, consultez Utilisateurs, groupes d'utilisateurs et stratégies de commande.

Configurer le délai d'expiration de session système :

Un intervalle de délai d'expiration de session est fourni pour limiter la durée pendant laquelle une session (GUI, CLI ou API) reste active lorsqu'elle n'est pas utilisée. Pour NetScaler, le délai d'expiration de session système peut être configuré aux niveaux suivants :

- Délai d'expiration au niveau de l'utilisateur. Applicable à l'utilisateur spécifique.

GUI : Accédez à **Système** > **Administration des utilisateurs** > **Utilisateurs**, sélectionnez un utilisateur et modifiez le paramètre de délai d'expiration de l'utilisateur. CLI : À l'invite de commandes, entrez la commande suivante :

```
set system user <name> -timeout <secs>
```

- Délai d'expiration au niveau du groupe d'utilisateurs. Applicable à tous les utilisateurs du groupe.

GUI : Accédez à **Système** > **Administration des utilisateurs** > **Groupes**, sélectionnez un groupe et modifiez le paramètre de délai d'expiration du groupe. CLI : À l'invite de commandes, entrez la commande suivante :

```
set system group <groupName> -timeout <secs>
```

- Délai d'expiration système global. Applicable à tous les utilisateurs et aux utilisateurs des groupes pour lesquels aucun délai d'expiration n'est configuré.

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

GUI : Accédez à **Système** > **Paramètres**, cliquez sur **Définir les paramètres système globaux** et définissez le paramètre ANY Client Idle Time-out (secs). CLI : À l'invite de commandes, entrez la commande suivante :

```
set system parameter -timeout <secs>
```

La valeur de délai d'expiration spécifiée pour un utilisateur a la priorité la plus élevée. Si aucun délai d'expiration n'est configuré pour l'utilisateur, celui configuré pour un groupe de membres est pris en compte. Si aucun délai d'expiration n'est spécifié pour un groupe (ou si l'utilisateur n'appartient pas à un groupe), celui configuré globalement est pris en compte. Si aucun délai d'expiration n'est configuré à quelque niveau que ce soit, la valeur par défaut de 900 secondes est définie comme délai d'expiration de session système.

Vous pouvez également restreindre la valeur du délai d'expiration afin que la valeur du délai d'expiration de session ne puisse pas être configurée au-delà de la valeur de délai d'expiration configurée par l'administrateur. Vous pouvez restreindre la valeur du délai d'expiration entre 5 minutes et 1 jour. Pour restreindre la valeur du délai d'expiration :

- GUI : Accédez à **Système** > **Paramètres**, cliquez sur **Définir les paramètres système globaux**, et sélectionnez le champ Délai d'expiration restreint.
- CLI : À l'invite de commandes, entrez la commande suivante :

```
set system parameter -restrictedtimeout <ENABLED/DISABLED>
```

Une fois que l'utilisateur a activé le paramètre restrictedTimeout, et si la valeur du délai d'expiration est déjà configurée à une valeur supérieure à 1 jour ou inférieure à 5 minutes, l'utilisateur est informé de modifier la valeur du délai d'expiration. Si l'utilisateur ne modifie pas la valeur du délai d'expiration, par défaut, la valeur du délai d'expiration sera reconfigurée à 900 secondes (15 minutes) lors du prochain redémarrage.

Vous pouvez également spécifier des durées de délai d'expiration pour chacune des interfaces auxquelles vous accédez. Cependant, la valeur de délai d'expiration spécifiée pour une interface spécifique est restreinte à la valeur de délai d'expiration configurée pour l'utilisateur qui accède à l'interface. Par exemple, considérons qu'un utilisateur `publicadmin` a une valeur de délai d'expiration de 20 minutes. Maintenant, lors de l'accès à une interface, l'utilisateur doit spécifier une valeur de délai d'expiration qui est de 20 minutes maximum.

Pour configurer la durée du délai d'expiration pour chaque interface :

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

- CLI : Spécifiez la valeur du délai d'expiration à l'invite de commandes en utilisant la commande suivante :

```
set cli mode -timeout <secs>
```

- API : Spécifiez la valeur du délai d'expiration dans la charge utile de connexion.

Journalisation et surveillance

Configurer le protocole NTP (Network Time Protocol)

Nous recommandons que le protocole NTP (Network Time Protocol) soit activé sur NetScaler et configuré pour utiliser un serveur de temps réseau fiable. L'activation du NTP garantit que les heures enregistrées pour les entrées de journal et les événements système sont précises et synchronisées avec les autres ressources réseau.

Lors de la configuration du NTP, le fichier ntp.conf doit être modifié pour empêcher le serveur NTP de divulguer les informations contenues dans les paquets sensibles.

Vous pouvez exécuter les commandes suivantes pour configurer le NTP sur NetScaler :

```
add ntp server <IP_address> 10



enable ntp sync
```

Modifiez le fichier ntp.conf pour chaque serveur NTP fiable que vous ajoutez. Il doit y avoir une entrée de restriction correspondante pour chaque entrée de serveur. Vous pouvez localiser le fichier ntp.conf en exécutant la commande `find . –name ntp.conf` à partir de l'invite de commande NetScaler.

Configurer SNMP

NetScaler prend en charge la version 3 du protocole SNMP. SNMPv3 intègre des capacités d'administration et de sécurité telles que l'authentification, le contrôle d'accès et les vérifications d'intégrité des données. Pour plus d'informations, consultez Configuration de NetScaler pour les requêtes SNMPv3.

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

REMARQUE :

Nous vous recommandons d'utiliser SNMPv3 au lieu de SNMPv1 et SNMPv2.

Si vous ne configurez pas au moins un gestionnaire SNMP, NetScaler accepte et répond aux requêtes SNMP de toutes les adresses IP du réseau. Exécutez la commande suivante pour ajouter un gestionnaire SNMP et restreindre ce comportement :

```
add snmp manager <IP_address>
```

Dans les déploiements où SNMP n'est pas requis, la fonctionnalité doit être désactivée avec la commande suivante :

```
set ns ip <IP_Address> -snmp disabled
```

Configurer la journalisation vers un hôte de journal externe NetScaler

Le serveur d'audit NetScaler enregistre toutes les informations d'état et de statut collectées par différents modules du noyau et des démons de niveau utilisateur. Le serveur d'audit permet à un administrateur de consulter l'historique des événements par ordre chronologique. Le serveur d'audit est similaire au serveur SYSLOG qui collecte les journaux de NetScaler. Le serveur d'audit utilise les informations d'identification de l'administrateur pour récupérer les journaux d'une ou plusieurs appliances.

- Configuration du serveur d'audit local

Exécutez la commande suivante pour configurer la journalisation vers le serveur d'audit local dans NetScaler : `> set audit nslogparams –serverip <hostname> -serverport <port>`

- Configuration du serveur d'audit distant

Pour configurer la journalisation vers le serveur d'audit sur un ordinateur distant, installez le serveur d'audit sur cet ordinateur. Voici des exemples d'options de serveur d'audit :

```
./audserver -help

usage : audserver -[cmds] [cmd arguments]

cmds cmd arguments: -f <filename> -d debug
```

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

```
-help - detail help

-start - cmd arguements,[starts audit server]

-stop - stop audit server

-verify - cmd arguments [verifies config file]

-addns - cmd arguments [add a netscaler to conf file]

-version - prints the version info
```

Ces options permettent de journaliser uniquement les messages d'audit générés par le fichier ns.log de NetScaler. Pour journaliser tous les messages syslog, procédez comme suit :

1. Supprimez les spécifications de fichier journal du fichier /nsconfig/syslog.conf pour les installations locales.
2. Remplacez les spécifications du fichier journal par le nom d'hôte du journal ou l'adresse IP de l'hôte syslog distant, comme dans les entrées suivantes :

   local0.* @10.100.3.53

   local1.* @10.100.3.53
3. Configurez le serveur syslog pour qu'il accepte les entrées de journal des installations de journalisation précédentes. Pour plus d'informations, consultez la documentation du serveur syslog.
4. Pour la plupart des serveurs basés sur UNIX utilisant le logiciel syslog standard, vous devez ajouter une entrée de configuration d'installation locale pour les fichiers messages et nsvpn.log au fichier de configuration syslog.conf. Les valeurs d'installation doivent correspondre aux valeurs configurées sur NetScaler.
5. Le serveur syslog distant sur tout ordinateur basé sur UNIX n'écoute pas les journaux distants par défaut. Par conséquent, exécutez la commande suivante pour démarrer le serveur syslog distant :

```
syslogd -m 0 –r
```

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

REMARQUE :

Consultez les options équivalentes de la variante syslog déployée dans le serveur d'audit.

Configurer l'exportation des messages sur un canal sécurisé

Vous pouvez exporter syslog en toute sécurité via SSL (Secure Sockets Layer), garantissant que les données de journal sensibles traversent le réseau de manière chiffrée et authentifiée. En tirant parti de SSL, vous pouvez protéger les transmissions syslog contre l'écoute clandestine, la falsification et l'accès non autorisé. Pour plus d'informations, consultez Exporter syslog en toute sécurité via SSL.

Configuration LOM

Nous recommandons de prendre les mesures suivantes pour sécuriser l'interface LOM :

- N'exposez pas le port LOM à Internet.
- Déployez le LOM derrière un pare-feu SPI.
- Déployez le LOM sur un segment de réseau qui est séparé soit logiquement (VLAN séparé) soit physiquement (LAN séparé) du trafic réseau non fiable.
- Définissez des valeurs différentes pour le nom d'utilisateur, le mot de passe, le certificat SSL et la clé SSL pour le LOM et les ports de gestion NetScaler.
- Assurez-vous que les appareils utilisés pour accéder à l'interface de gestion LOM sont exclusivement dédiés à des fins de gestion de réseau et placés sur un segment de réseau de gestion qui se trouve dans le même LAN physique ou VLAN que les ports d'autres appareils de gestion.
- Pour identifier et isoler facilement les adresses IP LOM, réservez des adresses IP spéciales (sous-réseaux privés) pour les interfaces de gestion LOM et les serveurs de gestion. N'utilisez pas de sous-réseaux IP réservés avec les interfaces LAN du NetScaler géré. Les adresses IP dynamiques attribuées par DHCP ne sont pas recommandées, car elles rendent difficile la mise en œuvre de listes de contrôle d'accès de pare-feu basées sur une adresse MAC en dehors du segment LAN.
- Définissez le mot de passe pour un minimum de 8 caractères, avec une combinaison de caractères alphanumériques et spéciaux. Changez le mot de passe fréquemment.

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

Applications et services

Configurer NetScaler® pour supprimer ou transmettre l'en-tête de mise à niveau

Un nouveau paramètre `passProtocolUpgrade` est ajouté au profil HTTP pour prévenir les attaques sur les serveurs back-end. Selon l'état de ce paramètre, l'en-tête de mise à niveau est transmis dans la requête envoyée au back-end ou supprimé avant l'envoi de la requête.

- Si le paramètre `passProtocolUpgrade` est activé, l'en-tête de mise à niveau est transmis au back-end. Le serveur accepte la requête de mise à niveau et la notifie dans sa réponse.
- Si ce paramètre est désactivé, l'en-tête de mise à niveau est supprimé et la requête restante est envoyée au back-end.

Le paramètre `passProtocolUpgrade` est ajouté aux profils suivants.

- nshttp_default_profile - activé par défaut
- nshttp_default_strict_validation - désactivé par défaut
- nshttp_default_internal_apps - désactivé par défaut
- nshttp_default_http_quic_profile - activé par défaut

Nous vous recommandons de désactiver le paramètre `passProtocolUpgrade`.

Définir le paramètre `passProtocolUpgrade` à l'aide de l'interface de ligne de commande (CLI) :

À l'invite de commandes, tapez ce qui suit :

```
set ns httpProfile <name> [-passProtocolUpgrade ( ENABLED | DISABLED )]
```

Définir le paramètre `passProtocolUpgrade` à l'aide de l'interface graphique (GUI) :

1. Accédez à **Système -> Profils -> Profils HTTP**.
2. Créez ou modifiez un profil HTTP.
3. Cochez la case **Pass Protocol Upgrade**.

Configurer NetScaler pour qu'il supprime les requêtes HTTP non valides

Nous recommandons de configurer NetScaler avec une vérification et une application strictes des requêtes HTTP afin d'empêcher les requêtes HTTP non valides de passer par les serveurs virtuels. Pour ce faire, liez un profil HTTP intégré, *nshttp_default_strict_validation*, à un ou plusieurs serveurs virtuels à l'aide de la commande suivante sur la CLI :

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

```
show ns httpProfile (Shows the available http profile (default+user
configured profiles))



set lb vserver <vserver name> -httpProfileName
nshttp_default_strict_validation
```

Nous recommandons aux clients utilisant cette option de tester les modifications dans un environnement de pré-production avant de les déployer en production.

La protection contre les attaques de désynchronisation HTTP est activée par défaut sur le profil de validation HTTP strict (nshttp_default_strict_validation). Utilisez le profil strict pour toutes les entités côté client.

Pour plus d'informations sur les attaques par dissimulation de requêtes HTTP et leur atténuation, consultez l'article de support NetScaler - Guide de référence sur la dissimulation de requêtes HTTP.

Configurer la protection contre les attaques par déni de service HTTP

Le firmware NetScaler prend en charge des contre-mesures limitées contre les attaques par déni de service HTTP, y compris les attaques de type 'slow-read'. Vous pouvez configurer ces fonctionnalités en utilisant l'utilitaire `nsapimgr` à partir de l'invite de commande NetScaler :

- small_window_threshold (par défaut=1)
- small_window_idle_timeout (par défaut=7 s)
- small_window_cleanthresh (par défaut=100)
- small_window_protection (par défaut=Activé)

Les paramètres par défaut sont adéquats pour prévenir les attaques par déni de service HTTP, y compris les attaques de type 'slow-read', cependant, un certain ajustement des paramètres pourrait être nécessaire pour d'autres attaques.

Pour se protéger contre de telles attaques, ajustez la propriété `small_window_threshold` à la hausse en utilisant la commande `nsapimgr` suivante à partir de l'invite de commande NetScaler :

`$ nsapimgr –ys small_window_threshold=<desired value>`

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

REMARQUE :

La valeur souhaitée `small_window_threshold` peut être définie en fonction du modèle de trafic entrant dans le déploiement. La plage acceptable est de 0 à 2\^32.

Vous pouvez vérifier la protection contre les attaques par déni de service HTTP en surveillant les compteurs suivants avec la commande `nsconmsg –d stats` à partir de l'invite de commande NetScaler :

- nstcp_cur_zero_win_pcbs : Ce compteur suit le nombre de PCB qui ont actuellement une faible valeur de fenêtre.
- nstcp_err_conndrop_at_pass : Ce compteur est incrémenté lorsque NetScaler détecte que, lors du passage de paquets d'un côté à l'autre, la valeur nscfg_small_window_idletimeout a été dépassée.
- nstcp_err_conndrop_at_retx : Ce compteur est incrémenté lorsque le temps écoulé pendant la retransmission dépasse la valeur nscfg_small_window_idletimeout.
- nstcp_cur_pcbs_probed_withKA : Ce compteur suit le nombre de PCB dans la file d'attente de surtension qui sont sondés avec une sonde KA.

Nous recommandons aux clients utilisant cette option de tester les modifications dans un environnement de pré-production avant de les déployer en production.

Configurer NetScaler pour se défendre contre les attaques d'usurpation TCP

Les commandes suivantes peuvent être utilisées pour aider à protéger les serveurs back-end contre les attaques d'usurpation TCP :

```
set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -spoofSynDrop
ENABLED



Done



set lb vserver lbvserver1 -tcpProfileName profile1
```

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

```
Done
```

Nous recommandons aux clients utilisant cette option de tester les modifications dans un environnement de pré-production avant de les déployer en production.

Configurer la conformité RFC 5961

À partir de la version 14.1-4.x de NetScaler, l'option `-rfc5961Compliance` est disponible dans le profil TCP. Cette option inclut la protection contre l'usurpation et couvre à la fois - `rstWindowAttenuate` et `-spoofSynDrop`. Activez `-rfc5961Compliance` pour bénéficier de toutes ces protections sans configurer chaque option séparément.

Pour plus d'informations, consultez Configurations TCP d'exemple.

Configurer NetScaler pour accepter des en-têtes HTTP spécifiques

Il est possible de configurer le NetScaler pour qu'il n'accepte que des en-têtes HTTP spécifiques. Ceci peut être réalisé en ajoutant une action de réécriture pour empêcher le trafic réseau avec des en-têtes HTTP spécifiques et définis d'être transmis au serveur back-end.

L'action de réécriture globale suivante envoie uniquement le trafic réseau avec des en-têtes tels que Host, Accept et test au serveur :

```
add rewrite action act1 replace_all q/
HTTP.REQ.FULL_HEADER.after_str("\r\n")/     q{TARGET.REGEX_SELECT(re/
(iu)^(Host|Accept|test):.*\r\n/) ALT ""} -pattern q{re/(U).+:.+r\n/}



add rewrite policy pol1 HTTP.REQ.IS_VALID act1



bind rewrite global pol1 100
```

Configurer la taille des en-têtes HTTP

Nous vous recommandons de maintenir une valeur adaptée à vos besoins métier pour les paramètres de taille d'en-tête HTTP `maxHeaderLen` et `maxHeaderFieldLen`. La valeur par défaut est définie à 24820, ce qui assure la compatibilité avec les applications qui nécessitent de grands en-têtes HTTP.

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

```
set httpprofile http-prof -maxHeaderLen <header-length> -maxHeaderFieldLen
<header-field-length>
```

Le paramètre `maxHeaderLen` contrôle la taille totale de l'en-tête et `maxHeaderFieldLen` contrôle la taille des champs d'en-tête individuels. Ces paramètres sont disponibles pour renforcer la sécurité en limitant la surface d'attaque pour les exploits basés sur les en-têtes, tels que les débordements de tampon ou les attaques par injection d'en-tête. Définissez la taille de l'en-tête sur le profil HTTP configuré sur le serveur virtuel et le groupe de services ou le service lié au serveur virtuel.

Bien qu'il soit possible de configurer ces paramètres à une valeur inférieure, cela pourrait entraîner la suppression de requêtes légitimes si l'application utilise des en-têtes dépassant les limites configurées. Par conséquent, les administrateurs doivent évaluer attentivement les exigences de leur application avant de réduire ces valeurs.

Normaliser les URL dans NetScaler

La normalisation d'URL standardise les formats d'URL incohérents en une structure unique et prévisible, garantissant que les règles de sécurité, les moteurs de recherche et les robots d'exploration Web traitent les différentes représentations de la même ressource Web comme identiques. NetScaler y remédie grâce aux paramètres de profil HTTP natifs, aidant à empêcher les attaquants d'exploiter les URL non normalisées pour contourner les filtres de sécurité.

La normalisation d'URL est disponible dans les versions NetScaler suivantes :

- 14.1-73.37 et versions ultérieures
- 14.1-73.37 FIPS et versions ultérieures
- 13.1-64.23 et versions ultérieures
- 13.1 37.279 FIPS et versions ultérieures

Utilisez la commande suivante pour activer le paramètre de normalisation d'URL :

`set ns httpProfile <profilename> -normalizeURL ENABLED`

Utilisez la commande suivante pour activer la normalisation d'URL RFC 3986 pour les requêtes envoyées au serveur d'origine :

`set ns httpProfile <profilename> -normalizeURLtoOrigin ENABLED`

Pour plus d'informations, consultez Normaliser les URL dans NetScaler.

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

Génération ISN TCP améliorée

La génération ISN améliorée augmente le caractère aléatoire des numéros de séquence initiaux lors de l'établissement de la connexion TCP sur NetScaler (côté serveur uniquement), réduisant ainsi la prévisibilité que les attaquants pourraient exploiter. Ce paramètre est désactivé par défaut mais peut être activé à l'aide de l'interface de ligne de commande.

La génération ISN TCP améliorée est disponible dans les versions NetScaler suivantes :

- 14.1-73.37 et versions ultérieures
- 14.1-73.37 FIPS et versions ultérieures
- 13.1-64.23 et versions ultérieures
- 13.1 37.279 FIPS et versions ultérieures

Utilisez la commande suivante pour activer le paramètre de génération ISN améliorée :

```
set ns tcpparam -enhancedISNgeneration ENABLED
```

Pour plus d'informations, consultez Génération ISN améliorée.

Configurer la notification de fermeture

Une notification de fermeture est un message sécurisé qui indique la fin de la transmission de données SSL. Conformément à la RFC 5246 : Le client et le serveur doivent partager la connaissance que la connexion se termine pour éviter l'attaque par troncation. Chaque partie peut initier l'échange de messages de fermeture en envoyant une alerte close_notify. Toute donnée reçue après une alerte de fermeture est ignorée, à moins qu'une autre alerte fatale n'ait été transmise. Chaque partie est tenue d'envoyer une alerte close_notify avant de fermer le côté écriture de la connexion. Pour vous assurer que les événements d'audit sont capturés pour les événements de terminaison TLS, connectez-vous à l'interface de ligne de commande (CLI) en tant que superutilisateur ou administrateur système et exécutez les commandes suivantes :

```
set ssl parameter -sendCloseNotify y



save ns config
```

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

Sécuriser l'interface graphique de gestion, l'API NITRO et la communication RPC

Pour sécuriser l'interface graphique de gestion, l'API NITRO et la communication RPC sur NetScaler et NetScaler Gateway, vous devez définir `-maxclient` dans NetScaler pour le service HTTP/HTTPS interne.

```
set service nshttpd-gui-127.0.0.1-80 -maxclient $max_client{}


set service nshttpd-vpn-127.0.0.1-81 -maxclient $max_client{}


set service nshttps-127.0.0.1-443 -maxclient $max_client{}
```

Pour plus d'informations sur la définition de la valeur `-maxclient` et les versions de NetScaler qui prennent en charge ce paramètre, consultez Configurer le service GUI HTTP interne à l'aide de l'interface graphique NetScaler, de l'interface de ligne de commande NetScaler ou des API NITRO NetScaler.

Recommandations de sécurité DNSSEC

Nous recommandons d'appliquer les recommandations suivantes aux clients utilisant DNSSEC :

Utiliser RSA 1024 bits ou plus pour les clés privées KSK/ZSK

Le NIST recommande aux administrateurs DNS de conserver des ZSK RSA/SHA-1 ou RSA/SHA-256 de 1024 bits jusqu'au 01 October 2015.

Activer l'alarme SNMP pour l'expiration des clés DNSSEC

Par défaut, l'alarme SNMP pour l'expiration des clés DNSSEC est activée sur NetScaler. La notification d'expiration de clé est envoyée via un trap SNMP appelé dnskeyExpiry. Trois variables MIB, `dnskeyName`, et `dnskeyUnitsOfExpiry`, sont envoyées avec le trap SNMP `dnskeyExpiry`. Pour plus d'informations, consultez le Guide de référence des OID SNMP NetScaler.

Renouveler les clés privées KSK/ZSK avant l'expiration du certificat x.509

Sur NetScaler, vous pouvez utiliser les méthodes de pré-publication et de double signature pour effectuer un renouvellement de la clé de signature de zone (Zone Signing Key) et de la clé de

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

signature de clé (Key Signing Key). Pour plus d'informations, consultez la rubrique **Système de noms de domaine > Configuration de DNSSEC** dans la documentation NetScaler.

Sécuriser le serveur ADNS DNSSEC

Si NetScaler est configuré en mode proxy DNSSEC, il met en cache les réponses du serveur ADNS principal et transmet les réponses mises en cache aux clients DNS.

Lorsque NetScaler est autoritaire pour une zone donnée, tous les enregistrements de ressources de la zone sont configurés sur NetScaler. Pour signer la zone autoritaire, vous devez créer les clés (la clé de signature de zone et la clé de signature de clé) pour la zone, ajouter les clés à NetScaler, puis signer la zone.

Pour configurer NetScaler en tant que serveur autoritaire, procédez comme suit :

1. Ajouter un service ADNS.

   Par exemple :

   ```
   add service s1 <ip address> adns 53`
   ```

2. Créer des clés DNS.

   Par exemple, pour agir en tant que serveur faisant autorité pour le domaine `com` :

   ```
   create dns key -zoneName com -keytype ksK -algorithm rsASHA512 -keysize
   3000 -fileNamePrefix com.ksk.rsasha1.3000



   create dns key -zoneName com -keytype zsk -algorithm rsASHA512 -keysize
   3000 -fileNamePrefix com.zsk.rsasha1.3000
   ```

   REMARQUE :

   Vous devez créer les clés DNS une seule fois et elles sont enregistrées dans /nsconfig/dns.

3. Ajoutez les clés DNS.

   Par exemple,

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

```
add dns key com.zsk.3000 /nsconfig/dns/com.zsk.rsasha1.3000.key /
nsconfig/dns/com.zsk.rsasha1.3000.private

add dns key com.ksk.3000 /nsconfig/dns/com.ksk.rsasha1.3000.key /
nsconfig/dns/com.ksk.rsasha1.3000.private
```

4. Ajoutez les enregistrements NS et SOA pour la zone `com`, puis signez la zone.

```
add dns soaRec com -originServer n1.com -contact citrix

add dns nsrec com n1.com

add dns zone com -proxyMode no

add dns addRec n1.com 1.1.1.1



sign dns zone com
```

Remarque : En outre, vous devez également activer le paramètre d'extension DNSEC dans les paramètres globaux DNS.

Pour plus d'informations sur la configuration du NetScaler en tant que serveur de noms de domaine faisant autorité, consultez la rubrique **Système de noms de domaine > Configuration du NetScaler en tant que serveur ADNS** dans la Documentation du produit.

Configuration héritée

Configurer NetScaler® pour désactiver la redirection de chiffrement

Avec la redirection de chiffrement, vous pouvez configurer un serveur virtuel SSL pour fournir des messages d'erreur précis et significatifs lorsqu'une négociation SSL échoue. Lorsqu'une négociation SSL échoue, NetScaler redirige l'utilisateur vers une URL précédemment configurée. Si aucune URL n'est configurée, NetScaler affiche une page d'erreur générée en interne.

À l'invite de commandes, exécutez les commandes suivantes pour configurer la redirection de chiffrement et vérifier la configuration :

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

```
set ssl vserver <vServerName> -cipherRedirect DISABLED

show ssl vserver <vServerName>
```

Lorsque vous liez le profil SSL par défaut à un serveur virtuel dans NetScaler, les paramètres SSL de ce serveur virtuel sont hérités du profil lié. Par conséquent, vous ne pouvez pas modifier directement les paramètres SSL sur le serveur virtuel car le profil SSL contrôle ces paramètres.

```
set ssl profile <ssl Profile name> -cipherredirect DISABLED
```

Pour plus d'informations, consultez Redirection de chiffrement.

Configurer les paramètres de renégociation SSL sur NetScaler

Nous vous recommandons de désactiver la renégociation SSL :

```
set ssl parameter -denySSLReneg ALL
```

Si le profil est activé, nous vous recommandons également de définir ce paramètre sur les profils front-end et back-end.

```
set ssl profile <frontend ssl profile name> -denySSLReneg ALL



set ssl profile <backend ssl profile name> -denySSLReneg ALL
```

Pour plus d'informations, consultez Comment configurer et utiliser le paramètre -denySSLReneg.

Configurer la vérification de certificat de conformité NDcPP

La vérification de certificat de conformité NDcPP s'applique lorsque NetScaler agit en tant que client (connexion back-end). Lors de la vérification du certificat, ignorez le nom commun si un SAN est présent dans le certificat SSL.

À l'invite de commandes, tapez les commandes suivantes pour configurer l'attribut « ndcppComplianceCertCheck » dans le paramètre SSL :

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

```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB
<positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
<positive_integer>] [-sendCloseNotify (YES | NO)] [-encryptTriggerPktCount
<positive_integer>] [-denySSLReneg <denySSLReneg>] [-insertionEncoding
(Unicode|UTF-8)] [-ocspCacheSize <positive_integer>][- pushFlag
<positive_integer>] [- dropReqWithNoHostHeader (YES | NO)] [-
pushEncTriggerTimeout <positive_integer>] [-ndcppComplianceCertCheck ( YES
| NO)] [-heterogeneousSSLHW (ENABLED | DISABLED )]
```

Exemple :

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks no
-ssltriggerTimeout 100 -sendClosenotify no -encryptTriggerPktCount 45
-denySSLReneg NONSECURE -insertionEncoding unicode -ocspCacheSize 10
-pushFlag 3 -dropReqWithNoHostHeader YES  -pushEncTriggerTimeout 100 ms
-ndcppComplianceCertCheck YES
```

Recommandations cryptographiques NetScaler®

Cette section détaille certaines étapes clés à suivre pour garantir que le matériel cryptographique est correctement sécurisé sur le NetScaler. Elle fournit également des informations sur la façon de configurer NetScaler pour utiliser ce matériel afin de protéger NetScaler, les serveurs back-end et les utilisateurs finaux.

Gestion des certificats et clés TLS

Configuration des suites de chiffrement TLS pour les déploiements FIPS et NDcPP

Les suites de chiffrement TLS suivantes sont prises en charge pour les déploiements FIPS et NDcPP.

- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384

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

- TLS1.2-AES128-GCM-SHA256
- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- TLS1.2-AES-256-SHA256
- TLS1.2-AES-128-SHA256
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1.2-ECDHE-ECDSA-AES256-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
- TLS1.3-AES256-GCM-SHA384
- TLS1.3-AES128-GCM-SHA256

  Pour la liste des chiffrements pris en charge sur MPX 14000 FIPS, consultez `<https://docs.netscaler.com/fr-fr/citrix-adc/downloads/cipher-support-on-netscaler-mpx-sdx-14000-fips.pdf>`.

Pour vous assurer que seules les suites de chiffrement approuvées sont configurées sur NetScaler, suivez les étapes de configuration suivantes à partir de l'interface de ligne de commande :

1. Délier tous les chiffrements du serveur virtuel

   ```
   unbind ssl vs v1 –cipherName FIPS
   ```

2. Liez uniquement TLS1-AES-256-CBC-SHA, puis TLS1-AES-128-CBC-SHA avec la commande :

   ```
   bind ssl vs v1 –cipherName <cipher>



   bind ssl vs v1 -cipherName TLS1-AES-256-CBC-SHA
   ```

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

Installation des certificats et des paires de clés à l'aide d'une autorité de certification approuvée :

Pour obtenir un certificat d'une autorité de certification (CA) publique ou d'entreprise, vous devez d'abord générer une clé privée et une demande de signature de certificat (CSR). Effectuez les étapes suivantes :

1. Authentifiez-vous à l'interface de ligne de commande (CLI) de NetScaler en tant que sysadmin ou superutilisateur.
2. Créez une clé privée RSA.

```
create fipsKey m1 -keytype RSA -modulus 2048 -exponent F4
```

3. Créez la demande de signature de certificat (CSR) :

```
create certreq csr_1 -fipsKeyName m1 -countryName IN -stateName BA
-organizationName citrix
```

4. Soumettez la CSR à l'autorité de certification.

Pour la plupart des autorités de certification (CA) commerciales et d'entreprise, la CSR est envoyée par e-mail. Cependant, la méthode de soumission peut varier selon les environnements de CA d'entreprise. La CA renvoie un certificat valide par e-mail, mais cette action peut également varier d'une CA d'entreprise à l'autre. Après avoir reçu le certificat de la CA, copiez-le en toute sécurité dans le répertoire /nsconfig/ssl.

Connectez-vous en tant que superutilisateur ou sysadmin et exécutez la commande suivante depuis l'interface de ligne de commande (CLI) : `> add ssl certKey ck_1 -cert cert1_1 -fipsKey m1`

Recommandations NetScaler -FIPS

Configuration de NetScaler SDX dans un déploiement basé sur FIPS

Si vous êtes un client FIPS existant et que vous utilisez NetScaler SDX pour une véritable multi-location, utilisez le NetScaler MPX certifié FIPS pour terminer TLS et transférer le trafic vers le NetScaler SDX. Alternativement, il est possible d'utiliser un HSM externe Thales. Modifier les mots de passe de la carte cryptographique FIPS Lorsque vous utilisez une version certifiée FIPS de NetScaler avec un module de sécurité matérielle (HSM), modifiez l'officier de sécurité (SO) par défaut et définissez un nouveau mot de passe utilisateur comme suit. Si vous ne connaissez pas le

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

mot de passe SO par défaut d'un NetScaler compatible FIPS, contactez le support NetScaler.
Remarque : Seul un superutilisateur ou un sysadmin peut effectuer cette tâche.

```
set ssl fips -initHSM Level-2 <soPassword> <oldSoPassword> <user-Password>
[-hsmLabel <string>]



save configuration



initHSM
```

Niveau d'initialisation FIPS. NetScaler prend actuellement en charge le niveau 2 (FIPS 140-2). Cet argument est obligatoire. Valeurs possibles : Niveau-2

hsmLabel

Étiquette pour identifier le module de sécurité matérielle (HSM).

Longueur maximale : 31

Remarque : Toutes les données de la carte FIPS sont effacées avec la commande précédente.

Stocker le mot de passe HSM dans un emplacement sécurisé

Le mot de passe du HSM doit être stocké dans un emplacement sécurisé, conformément aux procédures d'exploitation de votre entreprise.

Remarque : Le HSM est verrouillé après trois tentatives de connexion infructueuses. Lorsqu'il est verrouillé, il devient inopérant et vous ne pouvez pas modifier sa configuration.

Autres fonctionnalités

Cette section fournit des exemples de modifications de configuration pouvant être appliquées à la fois au NetScaler Web App Firewall et au NetScaler Gateway pour améliorer la sécurité des appliances déployées et des informations sur la création de plusieurs niveaux de sécurité. Cette section contient également des informations sur les détails de configuration lors de l'utilisation de NetScaler ou de NetScaler Gateway en tant que SAML SP ou SAML IdP, ou les deux.

Consultez les rubriques suivantes pour plus d'informations.

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

- Recommandations de sécurité de NetScaler Web App Firewall
- Recommandations de sécurité de NetScaler Gateway

Recommandations de sécurité pour NetScaler® Web App Firewall

- Pour les vérifications de conformité RFC, il est recommandé de conserver 'APPFW_RFC_BLOCK' comme `rfcprofile` par défaut pour le profil WAF.
- Le WAF prend en charge l'insertion de la valeur d'attribut de cookie `Samesite` et le cookie peut être restreint au contexte du même site ou inter-sites en sélectionnant les valeurs 'Strict' ou 'Lax'.

Déployer NetScaler en mode deux bras

Avec une installation en mode deux bras, NetScaler est physiquement situé entre les utilisateurs et les serveurs web que NetScaler protège. Les connexions doivent passer par NetScaler. Cette disposition minimise les chances de trouver un chemin de contournement de NetScaler.

Utiliser une politique de 'refus par défaut'

Nous recommandons aux administrateurs de configurer NetScaler Web App Firewall avec une politique de refus de tout au niveau global pour bloquer toutes les requêtes qui ne correspondent pas à une politique NetScaler Web App Firewall. Voici un exemple d'ensemble de commandes pour configurer une politique de 'refus de tout' au niveau global :

```
add appfw profile default_deny_profile -defaults advanced



add appfw policy default_deny_policy true default_deny_profile



bind appfw global default_deny_policy <PRIORITY>
```

REMARQUE :

Le paramètre **PRIORITY** doit garantir que la politique par défaut est évaluée en dernier (uniquement si la requête ne correspond à aucune autre politique configurée).

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

Le logiciel NetScaler inclut des profils par défaut, tels que appfw_block, qui, une fois configurés, bloquent les requêtes qui ne correspondent pas aux politiques NetScaler Web App Firewall. Exécutez la commande suivante pour définir le profil par défaut :

```
set appfw settings -defaultProfile appfw_block
```

NetScaler Web App Firewall – Création de plusieurs niveaux de sécurité

Les directives suivantes vous aident à créer plusieurs niveaux de sécurité en fonction de votre environnement et des applications prises en charge.

Configurez une valeur différente pour le paramètre **sessionCookieName** dans chaque niveau.

```
set appfw settings -sessionCookieName "citrix_ns_id_1"
```

Premier niveau de sécurité

Pour construire le premier niveau de sécurité, effectuez les opérations suivantes :

- Activez le dépassement de tampon, l'injection SQL et le script intersite.
- Une URL de démarrage est nécessaire lorsque l'application est spécifique quant aux URL qui doivent être accédées et qu'elle doit se protéger contre la navigation forcée.
- Activez les vérifications du format des champs si votre application attend des entrées dans un champ de formulaire.

La vérification de script intersite peut générer des faux positifs, car de nombreuses entreprises disposent d'une large base installée de contenu web amélioré par JavaScript qui viole la règle de la même origine. Si vous activez la vérification de script intersite HTML sur un tel site, vous devez générer les exceptions appropriées afin que la vérification ne bloque pas les activités légitimes.

Déployez le premier niveau, recherchez les faux positifs, déployez les exceptions, puis passez au niveau suivant. Une implémentation par étapes aide à gérer le déploiement d'AppFw.

Deuxième niveau de sécurité

Pour construire le deuxième niveau de sécurité, procédez comme suit :

Activez les signatures sur le profil en plus du dépassement de tampon, de l'injection SQL et du script intersite. Il y a plus de 1300 signatures. Essayez d'activer uniquement les signatures applicables à la protection de votre application, plutôt que d'activer toutes les règles de signature.

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

Déployez le deuxième niveau, recherchez les faux positifs, déployez les exceptions, puis passez au niveau suivant. Une implémentation par étapes aide à gérer le déploiement du NetScaler Web App Firewall.

Troisième niveau de sécurité

Pour construire le troisième niveau de sécurité, procédez comme suit :

- Selon les besoins de l'application, activez les vérifications de sécurité avancées du profil telles que le marquage CSRF, la cohérence des cookies, la cohérence des champs de formulaire sur les parties des applications qui en ont besoin.
- Les vérifications de sécurité avancées nécessitent plus de traitement et peuvent affecter les performances. À moins que votre application n'ait besoin d'une sécurité avancée, vous pouvez commencer par un profil de base et renforcer la sécurité selon les besoins de votre application.

Les vérifications de sécurité désactivées dans le profil de base du NetScaler Web App Firewall opèrent toutes sur des objets dans la réponse HTTP. Par conséquent, ces vérifications de sécurité sont plus gourmandes en ressources. Lorsque le NetScaler Web App Firewall effectue des protections côté réponse, il doit se souvenir des informations envoyées à chaque client individuel. Par exemple, si un formulaire est protégé par le NetScaler Web App Firewall, les informations des champs de formulaire envoyées dans la réponse sont conservées en mémoire. Lorsque le client soumet le formulaire dans la requête suivante, il est vérifié pour détecter les incohérences avant que les informations ne soient envoyées au serveur Web. Ce concept est appelé Sessionization. Les vérifications de sécurité telles que l'encapsulation d'URL dans l'URL de démarrage, la cohérence des cookies, la cohérence des champs de formulaire et le marquage de formulaire CSRF impliquent toutes la Sessionization. La quantité de ressources CPU et mémoire utilisées par ces vérifications de sécurité augmente linéairement avec le nombre de requêtes envoyées via le NetScaler Web App Firewall. Par exemple :

- Activez la vérification de cohérence des champs de formulaire : Cette vérification est nécessaire pour vérifier que les formulaires web n'ont pas été modifiés de manière inappropriée par le client. Une application qui sert et héberge des informations critiques dans des formulaires a besoin de cette vérification.
- Vérification de l'étiquetage des formulaires CSRF : Cette vérification est destinée aux formulaires. La vérification d'étiquetage des formulaires (CSRF) de falsification de requêtes intersites attribue à chaque formulaire web envoyé par un site web protégé aux utilisateurs un FormID unique et imprévisible, puis examine les formulaires web renvoyés par les utilisateurs pour s'assurer que le FormID fourni est correct. Cette vérification protège contre les attaques de falsification de requêtes intersites. Cette vérification doit être activée si l'application contient

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

des formulaires web. Cette vérification nécessite une capacité de traitement CPU relativement faible par rapport à d'autres vérifications de sécurité qui analysent les formulaires web en profondeur. Elle est donc capable de gérer des attaques à volume élevé sans dégrader sérieusement les performances du site web protégé ou du NetScaler Web App Firewall lui-même.

Étapes du flux de travail du NetScaler Web App Firewall

Effectuez les étapes suivantes dans le flux de travail du NetScaler Web App Firewall :

1. Configurez le profil de sécurité.
2. Appliquez les signatures pour toutes les menaces connues - le modèle négatif.
3. Configurez des stratégies de trafic capables de détecter le flux de trafic correct où ce profil de sécurité doit être activé.

Vous êtes prêt à ce que le trafic de production transite par le système. Le premier niveau de flux est terminé. Ensuite, configurez l'infrastructure d'apprentissage. Souvent, les clients souhaitent effectuer l'apprentissage sur le trafic de production, de sorte que l'application des signatures évite tout risque. Effectuez les étapes suivantes :

1. Configurez l'infrastructure d'apprentissage.
2. Déployez les règles apprises pour la protection.
3. Validez les données d'apprentissage ainsi que les signatures appliquées avant la mise en production.

Recommandations de sécurité pour NetScaler® Gateway

Utiliser une politique de 'refus par défaut'

Nous recommandons aux administrateurs de configurer le NetScaler Gateway avec une politique de 'tout refuser' au niveau global, en plus de l'utilisation de politiques d'autorisation pour activer sélectivement l'accès aux ressources par groupe.

Par défaut, le paramètre defaultAuthorizationAction est défini sur DENY. Vérifiez ce paramètre et accordez un accès explicite à chaque utilisateur. Vous pouvez utiliser la commande `show vpn parameter` sur la CLI pour vérifier le paramètre. Pour définir le paramètre afin de refuser toutes les ressources au niveau global, exécutez la commande suivante depuis la CLI :

```
set vpn parameter -defaultAuthorizationAction DENY
```

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

Utiliser la communication TLS1.2 entre les serveurs

Nous recommandons l'utilisation de TLS1.2 ou TLS 1.3 pour les liens entre NetScaler Gateway et d'autres services, tels que les serveurs LDAP et Web Interface. L'utilisation de versions plus anciennes de ce protocole, TLS 1.1, TLS 1.0, et SSLv3 et antérieures n'est pas recommandée.

Utiliser les applications intranet

Utilisez la fonctionnalité `Intranet Applications` pour définir quels réseaux sont interceptés par le plug-in NetScaler Gateway et envoyés à la passerelle. Voici un exemple d'ensemble de commandes pour définir l'interception :

```
add vpn intranetApplication intra1 ANY 10.217.0.0 -netmask 255.255.0.0
-destPort 1-65535 -interception TRANSPARENT



bind vpn vserver v1 –intranetapp intra1
```

Recommandations de sécurité pour l'authentification, l'autorisation et l'audit

Si une appliance NetScaler ou NetScaler Gateway est configurée en tant que SAML SP ou SAML IdP ou les deux, consultez l'article `<https://support.citrix.com/article/CTX316577>` pour les détails de configuration recommandés.

Pour plus de détails sur l'authentification SAML, consultez Authentification SAML.

SAML Rejeter l'assertion non signée

Lors de la configuration de NetScaler en tant que fournisseur de services SAML (SP), assurez-vous que le paramètre **Rejeter les assertions non signées** dans l'action SAML est défini sur **ON** ou **Strict**.

- **ON** (par défaut) : Rejette les assertions sans signature.
- **STRICT** : Garantit que la réponse SAML et l'assertion sont toutes deux signées.

Recommandation : Utilisez **STRICT**.

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

REMARQUE :

- Si votre fournisseur d'identité SAML prend en charge la signature de l'assertion SAML et de la réponse SAML, alors optez pour le mode **STRICT**.
- Utilisez **ON** comme paramètre minimal acceptable.

Utilisez la commande suivante pour vérifier la valeur **Rejeter l'assertion non signée** dans l'action SAML :

```
show samlaction <SAML Action Name> | grep 'Reject unsigned assertion'
```

Rejeter l'assertion non signée : ON

Exemple de configuration :

```
set samlAction <SAML Action Name> -samlRejectUnsignedAssertion <STRICT | ON>
```

Activer le chiffrement des informations de connexion de NetScaler Gateway pour l'authentification nFactor

Une appliance NetScaler Gateway avec authentification nFactor peut chiffrer les champs de requête de connexion soumis par un client (navigateur ou applications SSO) pendant le processus d'authentification. Les champs de requête de connexion chiffrés offrent une couche de sécurité supplémentaire pour protéger les données sensibles de l'utilisateur contre la divulgation.

Pour activer le chiffrement de la connexion à l'aide de l'interface de ligne de commande, exécutez la commande suivante.

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

Pour activer le chiffrement de la connexion à l'aide de l'interface graphique

1. Accédez à **Sécurité > AAA – Trafic d'application**.
2. Cliquez sur **Modifier les paramètres AAA d'authentification** sous la section Paramètres d'authentification.
3. Sur la page **Configurer le paramètre AAA**, dans **Chiffrement de connexion**, cliquez sur **Activé**.

Pour plus de détails sur le chiffrement de connexion, consultez Chiffrement des informations de connexion de NetScaler Gateway pour l'authentification nFactor.

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

Protéger le serveur virtuel VPN d'authentification, d'autorisation et d'audit et NetScaler Gateway

Nous recommandons les mesures d'atténuation suivantes pour protéger le serveur virtuel VPN d'authentification, d'autorisation et d'audit et NetScaler Gateway :

1. Assurez-vous que l'authentification multifacteur est activée pour NetScaler Gateway et que le facteur de vérification de l'authentification multifacteur est avant le facteur LDAP. Pour plus d'informations, consultez Configurer l'authentification multifacteur.
2. Créez une stratégie de répondeur pour autoriser les requêtes uniquement pour le FQDN souhaité, car certaines attaques semblent être déclenchées pour l'adresse IP de NetScaler Gateway et non pour le FQDN.

   ```
   add responder policy IP_Block "HTTP.REQ.HOSTNAME.EQ(\"<enter gateway
   FQDN here>\").NOT" DROP



   bind vpn vserver <vserver name> -policy IP_Block -priority 100 -type
   REQUEST
   ```

3. Activez la réputation IP. L'activation de la réputation IP permet de rejeter les requêtes provenant d'adresses IP malveillantes connues et de réduire l'impact des attaques. Exécutez les commandes suivantes pour activer la réputation IP :

   ```
   enable feature reputation



   add responder policy policy_brute_block_ip
   "CLIENT.IP.SRC.IPREP_IS_MALICIOUS" DROP



   bind vpn vserver <Gateway_vserver_name> -policy policy_brute_block_ip
   -priority 50 -gotoPriorityExpression END -type AAA_REQUEST
   ```

   Pour plus d'informations sur la configuration de la réputation IP, consultez Réputation IP.
4. Activez reCAPTCHA sur NetScaler. Pour plus d'informations sur la configuration de reCAPTCHA, consultez Configuration de reCAPTCHA pour l'authentification nFactor.

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

Configurer la valeur DNS fractionnée comme REMOTE

Nous vous recommandons de configurer la résolution DNS comme `REMOTE`.

Vous pouvez configurer la résolution DNS en utilisant l'une des méthodes suivantes :

1. `set vpn parameter splitDns REMOTE`
2. `set vpn sessionAction <action-name> splitDns REMOTE`

La configuration de `splitDns` à `sessionAction` est facultative. Si `splitDns` n'est pas fourni à `sessionAction`, la passerelle prend la valeur `splitDns` de la configuration `vpn parameter`.

Si `splitDns` est configuré à `sessionAction`, alors la configuration `sessionAction` prend le pas sur la configuration `vpn parameter`.

Par défaut, la CLI définit `vpn parameter splitDns` sur `BOTH`. Nous vous recommandons de configurer cette valeur comme `REMOTE`.

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

Bonnes pratiques pour la sécurité de NetScaler® Console

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 XenServer, VMware ESXi et Linux KVM. NetScaler Console répond au 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 circulant via les instances NetScaler sur 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.

Pour maintenir la sécurité tout au long du cycle de vie du déploiement, nous recommandons les considérations suivantes :

Ne pas exposer l'adresse IP de NetScaler Console et l'adresse IP de l'agent NetScaler à Internet

Nous recommandons que l'adresse IP de NetScaler Console et l'adresse IP de l'agent NetScaler ne soient pas exposées à l'Internet public et soient déployées derrière un pare-feu d'inspection de paquets (SPI) avec état approprié.

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

Mot de passe fort pour l'utilisateur système

Nous recommandons d'utiliser un mot de passe fort pour les comptes d'utilisateurs système créés dans NetScaler Console. Voici des exemples d'exigences de complexité de mot de passe :

- Le mot de passe doit avoir une longueur minimale de huit caractères.
- Le mot de passe ne doit pas contenir de mots du dictionnaire ou une combinaison de mots du dictionnaire.
- Le mot de passe doit inclure au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Pour définir une longueur de mot de passe minimale à l'aide de NetScaler Console :

1. Accédez à **Paramètres > Utilisateurs et rôles**.
2. Dans la page **Administration des utilisateurs**, cliquez sur **Paramètres** à droite.
3. Sélectionnez **Activer la complexité du mot de passe**.
4. Dans la page **Stratégie de mot de passe**, spécifiez la longueur minimale du mot de passe à 8.
5. Cliquez sur **OK**.

Modifier le certificat par défaut

Lors de la configuration initiale de NetScaler Console, les certificats TLS par défaut sont créés. Ces certificats ne sont pas destinés à être utilisés dans des déploiements de production et doivent être remplacés.

Nous vous recommandons de configurer NetScaler Console pour utiliser des certificats provenant d'une autorité de certification (CA) réputée ou des certificats appropriés de l'autorité de certification de votre entreprise. Pour plus d'informations, consultez Installer des certificats SSL.

Pour installer un certificat SSL sur NetScaler Console :

1. Accédez à **Paramètres > Administration**.
2. Sous **Paramètres SSL**, cliquez sur **Installer le certificat SSL**.
3. Dans la page **Installer le certificat SSL sur la console**, sélectionnez les fichiers de certificat et de clé et, éventuellement, spécifiez un mot de passe si la clé privée est chiffrée.
4. Cliquez sur **OK**.

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

Désactiver l'authentification locale

Lorsque l'authentification externe est configurée sur NetScaler Console et qu'en tant qu'administrateur, vous préférez refuser l'accès aux utilisateurs système locaux pour se connecter à l'accès de gestion, vous devez désactiver l'authentification locale. Pour plus d'informations, consultez Activer l'authentification externe.

REMARQUE :

Le serveur externe doit être configuré.

Pour désactiver l'authentification locale :

1. Accédez à **Paramètres > Authentification**.
2. Sur la page **Authentification**, cliquez sur **Paramètres**.
3. Sur la page **Paramètres d'authentification**, dans **Type de serveur**, sélectionnez EXTERNE.
4. Cliquez sur **Insérer**, et sur la page **Serveurs externes**, sélectionnez un ou plusieurs serveurs d'authentification à cascader.
5. Décochez **Activer l'authentification locale de secours** pour désactiver l'authentification locale.
6. Cliquez sur **OK**.

© 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.