# NetScaler Console 14.1

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

# Contents

リリースノート 67

NetScaler Console on-prem を Citrix Cloud に移行する 70

NetScalerエージェントを構成する 71

Citrix Cloudからクライアントおよびシークレットcsvファイルを取得する 71

NetScaler Consoleサービスライセンスを検証する 71

スクリプトを使用した移行 72

NetScaler Consoleオンプレミスへのロールバック 76

前提条件 76

ロールバックスクリプトを使用する 76

よくある質問 78

NetScaler Consoleサービス 78

NetScaler agentは、オンプレミスのNetScaler agentと同様にオプションですか? 78

NetScaler Consoleサービスを使用する理由? 78

オンプレミスのNetScaler ConsoleがHAペアの場合、移行後にどうなりますか? 78

何らかの理由でエージェントがダウンした場合、どうなりますか? 78

インスタンスのバックアップも移行されますか? 78

履歴データも移行されますか? 79

オンプレミスライセンスも移行されますか? 79

オンプレミスのNetScaler Consoleから移行されないものは何ですか? 79

オンプレミスのNetScaler ConsoleはCitrix Directorと統合されています。この統合はどうなりますか? 79

移行後のインスタンスのライセンス取得とアナリティクス有効化について? 79

移行ツール 80

マイグレーションスクリプト実行後のエラーメッセージ表示とその原因? 80

NetScalerインスタンスのバージョンが、プールライセンスの制限よりも低い場合、ライセンスサーバーを変更するために「Y」オプションを選択するとどうなりますか? 80

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

マイグレーションスクリプトがNetScalerインスタンスに関する構成に失敗した場合、どうなりますか? 80

NetScalerインスタンスの一部がNetScaler Consoleサービスへの移行に失敗した場合の対応と、マイグレーションスクリプトの再実行による解決策? 80

マイグレーションステータスを確認するためのログファイルについて? 80

マイグレーションスクリプトの実行中にセッションが終了した場合、どうなりますか? 81

NetScaler ConsoleサービスがオンプレミスのNetScaler Consoleよりも少ないライセンスしか持たず、移行スクリプトが開始された場合、どうなりますか? 81

オンプレミスのNetScaler ConsoleがNetScaler ConsoleサービスExpressアカウントに移行された場合、どうなります? 81

Citrix Cloudの招待ユーザー（Citrix Cloudアカウントを作成した管理者ユーザー以外）がNetScaler Consoleオンプレミス設定の移行を試みた場合、どうなります? 81

ロールバックスクリプト 81

NetScaler ConsoleオンプレミスHAペアでロールバックスクリプトが使用された場合、どうなりますか? 81

ロールバックスクリプトの使用後、ディザスタリカバリノードはどうなりますか? 81

トラブルシューティング 82

NetScaler Consoleサービスに追加された手動プロファイル 82

NetScaler Consoleサービスに追加されたNetScalerデバイス 82

NetScaler ConsoleサービスへのStyleBookカスタムテンプレートのインポート 82

NetScaler Consoleサービスに追加された構成ジョブ 83

NetScaler Consoleサービスに追加されたIPブロック 83

ネットワークダッシュボードレポートの追加ステータス 83

すべてのハウツー記事 84

インスタンス管理 84

構成管理 85

証明書管理 87

StyleBooks 87

アナリティクス 88

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

イベント管理 89

認証 89

NetScaler Consoleシステム 90

ネットワーク機能 92

概要 93

機能とソリューション 93

アプリケーション分析と管理 93

ネットワーク 94

オーケストレーション 95

アーキテクチャ 95

NetScaler Consoleがインスタンスを検出する方法 96

ポーリングの概要 98

NetScaler Consoleが管理対象インスタンスとエンティティをポーリングする方法 99

インスタンスをポーリングするさまざまな方法 103

インスタンスのグローバルポーリング 104

インスタンスの手動ポーリング 104

エンティティの手動ポーリング 105

NetScaler® テレメトリプログラム 106

テレメトリ収集モード 111

自動テレメトリ収集モード 111

手動テレメトリ収集モード 112

テレメトリ収集とアップロードの問題をトラブルシューティングするための診断 113

リリース14.1ビルド56.x以降の診断動作 113

仕組み 114

コレクターレベル (コンソール) の診断 114

デバイスレベル (NetScaler) 診断 115

リリース14.1ビルド56.x以前の診断動作 121

テレメトリアップロードの通知 122


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

データガバナンス 124
IoC情報の利用条件 127
NetScaler Consoleライセンス 128
ライセンス 128
高可用性 132
NetScaler Consoleの高可用性ノード間でライセンスはどのように同期されますか? 133
オーケストレーション 133
仮想サーバーライセンスのアップグレード 133
検証 134
仮想サーバーの管理 134
仮想サーバーの自動ライセンス付与を無効にする 135
ライセンス付与するサードパーティ製仮想サーバーを選択する 135
仮想サーバーライセンスを手動で適用する 135
ポリシーベースの仮想サーバーライセンスを構成する 136
ライセンスされた仮想サーバーを表示する 136
アドレス指定不可能な仮想サーバーの自動ライセンスサポートを構成する 137
ライセンス 137
高可用性 139
システム要件 140
NetScaler Console の要件 140
NetScaler Consoleオンプレミスエージェントの要件 141
NetScaler Consoleの機能に必要なNetScalerの最小バージョン 141
NetScaler Consoleアナリティクスの要件 142
NetScaler Console機能に必要なCitrix Virtual Apps and Desktopsの最小バージョン 142
HDX™ Insightでサポートされているシンクライアント 143
HDX Insightに必要なNetScalerインスタンスライセンス 143
サポートされているハイパーバイザー 144
サポートされているオペレーティングシステムとWorkspaceのバージョン 144

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

対応ブラウザ 144
対応ポート 145
NetScaler Console サーバーのポート 146
エージェント用ポート 148
NetScalerインスタンス用ポート 149
NetScaler 組み込みエージェント用のポート 150
外部サーバー用ポート 151
制限事項 152
はじめに 153
ステップ 1 - システム要件の確認 153
ステップ 2 - NetScaler Console の展開 154
ステップ3 - NetScaler Consoleへのインスタンスの追加 154
ステップ4 - 仮想サーバーでの分析の有効化 155
ステップ5 - NetScaler ConsoleでNTPサーバーを構成する 155
ステップ6 - NetScaler Consoleの最適なパフォーマンスのためのシステム設定を構成する 155
次のステップ 156
強化されたグラフィカルユーザーインターフェイス 157
ホバーで表示するメニュー 157
合理化されたメニュー階層 157
更新されたサブメニューラベル 158
**インフラストラクチャ > 構成** 158
**NetScalerライセンス > プールライセンス** 158
**ゲートウェイ > HDX Insight** 159
**設定** 159
折りたたみ可能なメニュー 160
展開されたメニュー 160
折りたたまれたメニュー 160
サイドバーの切り替え 160

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

サイドバーを表示 160

サイドバーを非表示 160

ホーム画面に設定 160

お気に入りの項目をピン留め 161

サービスに移行 161

展開 162

NetScaler Consoleのインストール要件 163

NetScaler Consoleの一般要件 163

プールまたはフレックスライセンス専用の軽量 NetScaler® Console 164

Citrix Hypervisor 上で動作する NetScaler Console 165

前提条件 165

XenCenter® システム要件 165

NetScaler® Application Delivery Management のインストール 166

検証 167

Microsoft Hyper-V 上の NetScaler コンソール 167

前提条件 167

Microsoft Hyper-V のシステム要件 167

NetScaler® Application Delivery Managementのインストール 168

検証 170

VMware ESXi 上の NetScaler コンソール 170

前提条件 170

NetScaler Consoleをインストールするには 170

検証 173

VMware ESXi 上でのNetScaler® エージェントの展開を自動化 173

NetScaler エージェントを構成する 174

NetScaler エージェントを登録し、デフォルトパスワードを変更する 174

前提条件 174

NetScaler エージェントを構成および登録する方法 175


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

ステップ1：.OVFファイルをダウンロードして編集する 175
ステップ2：VMware ESXiにNetScaler Console仮想アプライアンスをインストールする 179
ステップ 3: 確認 180
Kubernetesクラスター上のNetScaler Console 181
前提条件 181
Kubernetesクラスター 181
NFS共有 181
NetScalerアプライアンス 182
KubernetesクラスターへのNetScaler Consoleのインストール 182
Linux KVMサーバー上のNetScaler コンソール 184
前提条件 184
ハードウェア要件 184
ソフトウェア要件 185
NetScaler Consoleセットアップファイルのダウンロード 185
Linux-KVM への NetScaler Application Delivery Management のインストール 186
ネットスケーラー アプリケーション デリバリー マネジメント を構成する 188
Nutanixハイパーバイザー (Acropolis) でのNetScaler Console 190
ハードウェア要件 190
NetScaler Consoleセットアップファイルをダウンロードする 191
NutanixハイパーバイザーでNetScaler Consoleを構成する 191
ネットワーク構成 192
Red Hat OpenShift Virtualization 上の NetScaler コンソール 193
ハードウェア要件 194
前提条件 194
プラットフォーム要件 194
展開アーキテクチャ 194
Red Hat OpenShift Virtualization への NetScaler Console のインストール 195
ステップ 1 - 環境を準備する 195

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

ステップ2 - NetScaler Consoleセットアップファイルをダウンロードする 195
ステップ3 - イメージをRHOCPVブータブルボリュームにアップロードする 195
ステップ 4 - 仮想マシンを作成する 196
ステップ 5. 仮想マシンを起動する 196
ステップ 6. NetScaler Console にアクセスする 196
Azure クラウド上の NetScaler コンソール 197
前提条件 197
NetScaler Consoleの設定 197
Azure Cloud上のネットスケーラー コンソール HAペア 198
前提条件 199
NetScaler Console HAペアの構成 199
Amazon Web Services (AWS) 上の NetScaler コンソール 202
前提条件 202
NetScaler Consoleの構成 202
高可用性展開を構成する 203
展開シナリオ 204
高可用性アーキテクチャのコンポーネント 205
監視ツール 205
プライマリノード 206
セカンダリノード 206
物理ストリーミングレプリケーション 206
ハートビートメッセージ 206
フローティングIPアドレス 206
注意すべき重要な点 207
前提条件 208
NetScaler Console を高可用性モードでセットアップするには 209
最初のサーバー (プライマリノード) を登録する 209
2番目のサーバー（セカンダリノード）を登録する 210

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

プライマリノードGUIから高可用性セットアップを展開する 211
高可用性を無効にする 212
高可用性を再展開する 212
高可用性フェイルオーバーシナリオ 213
データベース同期ログメッセージを表示する 213
スプリットブレインシナリオ 213
ライセンス 214
異なるレイヤー3サブネット間での高可用性 (HA over L3) の構成 214
高レベルアーキテクチャ 215
展開と構成 216
NetScaler ConsoleでHAを構成する 217
NetScalerを外部ロードバランサーとして構成する 217
NetScalerロードバランシング構成スクリプトの例 218
利点 224
高可用性のためのディザスターリカバリを構成する 224
基本認証を有効にする 225
基本認証を構成する 225
ディザスタリカバリワークフロー 225
ディザスター発生前の初期設定 226
前提条件 226
初めてのディザスタリカバリ設定 227
NetScaler Console を高可用性モードで展開する 227
DR コンソールを使用して NetScaler Console ディザスタリカバリノードを展開および登録する 228
NetScaler Console GUIを使用して災害復旧ノードを展開する 229
災害後のワークフロー 230
ディザスタリカバリ後 231
設定を元のプライマリサイトに戻す 232

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

スタンドアロンノードのディザスタリカバリを構成する 232
ディザスタリカバリのワークフロー 233
前提条件 233
初回ディザスターリカバリ設定 235
災害後のワークフロー 237
災害復旧後 238
元のプライマリサイトに設定を戻す 239
マルチサイト展開のためのオンプレミスエージェントの構成 240
アーキテクチャ 242
基本認証を有効にする 242
基本認証を構成する 242
はじめに 243
データセンターにエージェントをインストールします 243
ポート 244
エージェントを登録する 245
エージェントをサイトにアタッチする 246
エージェントのアクション 246
NetScalerインスタンスの追加 247
既存のインスタンスをエージェントにアタッチする 247
イベントを検証するためにインスタンスのGUIにアクセスする 248
NetScalerエージェントのフェイルオーバー 248
エージェントの到達不能しきい値と通知を構成する 249
NetScaler® Console エージェントと NetScaler Console 間のセキュアな通信 250
KubernetesクラスターにNetScaler®エージェントをマイクロサービスとしてインストールする 251
はじめに 251
KubernetesクラスターにNetScalerエージェントをインストールする 252
NetScaler Console オンプレミス展開用の NetScaler Console エージェント OpenShift オペレーターをインストールする 252

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

前提条件 253
エージェントオペレーターをインストールする 254
エージェントインスタンスを削除する 255
エージェントオペレーターをアンインストールする 255
エージェントのアップグレード 256
アップグレードワークフロー 256
NetScaler Consoleシングルサーバー展開を高可用性展開に移行する 257
NetScaler Insight CenterからNetScaler Consoleへの移行 258
前提条件 258
ハードウェア要件 259
インストール手順 259
NetScaler Console と Citrix Director を統合する 260
前提条件 261
HDX Insight から NetScaler Console への移行のハードウェア要件 261
最小要件 261
ソフトウェア要件 261
制限事項 262
NetScaler Console に追加ディスクを接続する 262
スタンドアロン NetScaler Console に追加ディスクを接続する 263
ディスクパーティションツールを起動する 263
新しい追加ディスクにパーティションを作成する 265
既存の追加ディスク内のパーティションのサイズを変更する 266
追加ディスクのパーティションを削除する 267
仮想マシンを再起動する 268
ディスクデータのバックアップファイルを作成する 268
追加コマンド 269
高可用性で展開されたNetScaler Consoleに追加ディスクをアタッチする 271
NetScaler Console を介した NetScaler MPX™ ディスク暗号化 273

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

前提条件 274
HSM（Thales CipherTrust Manager）サーバーにインスタンスのシリアル番号を追加する 275
NetScaler Consoleによるインスタンスディスク暗号化 276
暗号化後の検証 277
暗号化後にNetScaler MPXインスタンスを復元する 278
NetScaler MPX™ HAペアの暗号化後の動作 278
暗号化後のNetScaler MPX™クラスターの動作 279
NetScaler Console クラウドコネクト 281
前提条件 281
Cloud Connect を構成する 285
ワークフロー 1 – 新規ユーザー (Citrix Cloud アカウントなし、NetScaler Console サービステナントなし) 285
ワークフロー2 – Citrix Cloudアカウントは存在するが、NetScaler Consoleサービステナントは存在しない 285
ワークフロー3 - Citrix CloudアカウントとNetScaler Consoleサービステナントが存在する場合 286
Cloud Connect のプロキシ構成サポート 286
Cloud Connect のステータスと更新動作 287
Cloud Connect のステータス 287
Cloud Connect ステータスの更新 288
Cloud Connect の診断 288
エラー処理とメッセージング 289
Cloud Connect ステータスの通知 289
通知頻度 290
通知チャネル 290
通知の管理 290
Cloud Connect を介して収集されるデータ 291
Cloud Connect 接続の問題のトラブルシューティング 291

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

その他のオプション 291
ビルド固有の機能動作 292
よくある質問 293
設定 295
NetScaler Consoleにインスタンスを追加する 296
NetScalerプロファイルの作成方法 296
NetScalerインスタンスをNetScaler Consoleに追加する 298
NetScaler ConsoleにNetScaler CPXインスタンスを追加する 300
NetScaler ConsoleでスタンドアロンのNetScaler BLXインスタンスを追加する 301
NetScaler Consoleで高可用性NetScaler BLXインスタンスを追加する 302
NetScaler ConsoleからインスタンスGUIにアクセスする 303
クラウドに展開されたNetScaler VPXインスタンスをNetScaler Consoleに追加する 303
分析の設定 304
仮想サーバーのライセンス管理とアナリティクス有効化 305
仮想サーバーでのライセンス管理 306
アナリティクスをグローバルに設定する 309
前提条件 310
アナリティクスを有効にする 310
仮想サーバーでアナリティクスを構成する 311
既存の仮想サーバーでアナリティクスを構成する 311
グローバルアナリティクスを構成する 314
アナリティクスを移行する 317
管理対象のNetScalerインスタンスにネットプロファイルを割り当てる 318
前提条件 318
NTPサーバーを構成する 319
システム設定を構成する 320
システムアラームを構成する 320
システム通知を構成する 321

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

システムバックアップ設定の構成 321
インスタンスバックアップ設定の構成 321
基本認証を有効にする 322
基本認証を構成する 322
NetScaler Console機能を有効または無効にする 322
NetScaler Console を ServiceNow インスタンスと統合する 323
前提条件 324
NetScaler Console を ServiceNow と統合する方法? 324
ステップ1 - Citrix CloudでITSMアダプターサービスを購読する 324
ステップ2 - ServiceNowインスタンスでエンドポイントアクセスを作成する 324
ステップ3 - ServiceNowインスタンスを追加する 325
ステップ4 - NetScaler ConsoleでのServiceNowチケットの自動生成をテストする 325
NetScaler ConsoleでServiceNow通知を設定する 325
レポートのエクスポートまたはエクスポートのスケジュール 326
レポートのエクスポート 327
エクスポートレポートをスケジュールする 327
スケジュールされたエクスポートレポートの表示と編集 328
アップグレード 329
アップグレードする前に 329
14.1-xx.xx以降へのアップグレード前に注意すべき重要な点 330
単一のNetScaler Consoleサーバーを14.1-xx.xxにアップグレードする 331
高可用性ペアを14.1リリースにアップグレードする 332
NetScaler Consoleディザスタリカバリ展開のアップグレード 332
NetScaler Console災害復旧ノードをアップグレードする 332
マルチサイト展開用のオンプレミスエージェントをアップグレードする 333
オンプレミスエージェントのアップグレード 333
NetScaler Consoleサーバーにディスクを追加する 333
認証 335

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

外部認証サーバー 335
NetScaler Consoleでユーザーを認証する 336
LDAP認証サーバーを追加 337
RADIUS認証サーバーを追加 339
TACACS認証サーバーを追加する 340
NetScaler Console のユーザー 341
NetScaler Console のユーザーグループ 341
認証サーバーグループを抽出する 342
外部認証サーバーとフォールバックオプションを有効にする 343
フォールバックおよびカスケード外部サーバーを設定する 344
LDAP、RADIUS、TACACS を使用した二要素認証 (2FA) のサポート 344
二要素認証を構成する 345
2要素認証を使用したNetScaler® Consoleへのユーザーアクセス 346
アクセスコントロール 347
ロールベースのアクセス制御 347
制限事項 348
アクセス ポリシーを構成する 349
ユーザーにStyleBookの権限を付与する 351
グループを構成する 352
ユーザーグループを作成する 352
承認スコープに基づいてユーザーアクセスがどのように変化するか 361
NetScaler Consoleを12.0からそれ以降のリリースにアップグレードする際のRBACのマッピング 361
ロールの構成 362
ユーザーを構成する 363
実行可能なタスクと推奨事項 365
タスク 366
推奨事項 369

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

ガイド付きワークフローを使用して推奨事項を完了する方法? 372
通知を構成する 372
よくある質問 372
インスタンスの主要なメトリックの詳細を表示する統合ダッシュボード 374
アプリケーション 374
NetScalerインフラストラクチャ 375
アプリケーションセキュリティ 375
ゲートウェイ 376
ダッシュボードをカスタマイズ 376
エージェントの詳細を表示 376
フィルターの作成と適用 377
フィルターの編集 378
インスタンスの主要なメトリックの詳細を表示するためのカスタムダッシュボードを作成する 378
ダッシュボードのその他のオプション 379
他のユーザーとダッシュボードを共有する 380
アプリケーション 381
前提条件 381
アプリケーションの概要 381
ディスクリートアプリケーション 382
カスタムアプリケーション 382
注意点 382
マイクロサービスアプリケーション 382
アプリケーション管理とアプリケーションダッシュボード 382
アプリケーションの管理 383
アプリケーションダッシュボード 383
以前のダッシュボードと比較した新しいダッシュボードの動作の更新点 383
アプリケーションの管理 384
アプリケーションの詳細を表示 384

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

アプリケーションを追加 385
StyleBookを使用してアプリケーションを作成する 387
アプリケーションの編集または削除 388
アプリダッシュボードとセキュリティダッシュボードのレポートをエクスポートする 388
アプリケーションの表示 389
アプリケーションを構成し、複数のカスタムアプリケーションに関連付ける 390
アプリケーションダッシュボードの概要 391
検索バーを使用して結果を検索およびフィルタリングする 394
アプリケーションにタグを作成して適用する 394
アプリケーションの詳細 395
App Score コンポーネントを選択し、しきい値を設定する 398
マイクロサービスアプリケーションのアプリケーション詳細 400
インテリジェントアプリ分析 403
インテリジェントアプリ分析の構成 403
アプリケーション分析のパフォーマンス指標 405
レスポンスタイム 406
アクティブサービス 406
平均CPU使用率 407
メモリ使用量 407
サービスフラップ 407
不安定なサーバー 408
セッションビルドアップ 409
低セッション再利用 410
サージキューの蓄積 410
異常に大きいHTTPパケット 411
不適切なパーシステンスタイプ 412
TCP再構成キュー制限ヒット 412
SSLリアルタイムトラフィック 413

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

アプリダッシュボードのトラブルシューティング 414
トラブルシューティングのシナリオ 414
アプリケーションはライセンスされています 414
メトリックコレクターが有効になっています 415
NetScaler®インスタンスの以前のビルド 415
NetScalerインスタンスの後のビルド 416
アプリケーションの使用状況と異常 419
ピーク時と閑散時の使用状況分析 420
アプリケーションのスケール制限を評価する 420
アプリケーションのメンテナンスウィンドウ上位5つを特定する 420
アプリケーション使用状況分析 422
メトリックの詳細をグラフィカル形式で表示 427
Web Insightの問題をトラブルシューティングする 430
A+ SSL評価分析 431
A+ SSLレーティングにアップグレード 432
SSLレーティングをロールバック 433
アプリケーショントラフィックに対するSSL評価の影響を判断する 433
Web Insight ダッシュボード 434
統合キャッシュリクエスト 436
Web Insight の問題のトラブルシューティング 436
アプリケーションの遅延の根本原因を表示する 437
アプリケーションのドリルダウン 437
応答時間 438
サービスグラフ 440
すべてのNetScalerインスタンスにわたるアプリケーションのサービスグラフ 440
Kubernetesアプリケーションのサービスグラフ 441
3層Webアプリケーションのサービスグラフ 442
Kubernetesアプリ向けサービスグラフ 443

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

サービスグラフのセットアップ 444
ソフトウェア要件 444
始める前に 445
シングルティアまたは統合イングレストポロジ 445
デュアルティアまたはService Mesh Liteトポロジ 445
サービスメッシュトポロジ 446
サービスグラフで詳細を表示 447
サービスグラフダッシュボード 448
表形式ビューを使用して主要メトリックの傾向を表示する 450
クライアントメトリックを表示する 450
TCPおよびSSLメトリックの表示 452
サービスの詳細を表示 453
フィルターを適用 453
設定オプションの使用 453
エラーを分析する 454
HTTPトランザクションの詳細を表示 455
サービスグラフでしきい値を設定する 455
単一しきい値 456
二重しきい値 457
サービスの詳細を表示 457
メトリックの詳細 458
バックエンドPodの詳細を表示 458
トラブルシューティングのためのイングレスの詳細を表示 459
分散トレース 462
前提条件 463
サービス追跡の詳細を表示 467
トランザクションの詳細を表示する 467
サービスグラフの部分データまたはデータなしの診断詳細を表示する 469

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

データなしの診断 469

部分的なデータに関する診断 470

トラブルシューティング 470

アプリケーションのサービスグラフ 470

アプリケーションビュー 471

ネットワーク機能ビュー 471

アクティブなトランザクションがない場合のサービスグラフビュー 471

メトリックの分析 472

クライアントメトリクス 472

ネットワーク機能メトリクス 472

サービスメトリクス 472

NetScalerメトリック（GSLBアプリケーションのみ） 473

サービスグラフ内のすべてのアプリケーションの全体像 473

クライアントメトリクスの表示 474

NetScalerの詳細を表示 474

個別のアプリケーションを表示 475

マイクロサービスアプリケーションを表示する 476

検索バーで結果をフィルタリング 477

StyleBooks 479

StyleBookのカテゴリ 481

デフォルトおよびカスタムStyleBook 481

パブリックおよびプライベートStyleBook 481

プライベートとしてマークされたStyleBookの例 482

StyleBookの表示 482

カスタムStyleBookをダウンロード 483

カスタムStyleBookを更新 483

カスタムStyleBookを削除する 484

StyleBookの依存関係を表示する 485


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

StyleBookの依存関係を表示するには 485
順方向の依存関係 485
逆方向の依存関係 485
設定パックに対するNetScaler構成の監査 486
構成パックのサポートバンドルをダウンロードする 486
StyleBookのタグを作成する 487
CLIコマンドを使用してStyleBookを設定するには 488
StyleBookをクローンする 488
外部リポジトリからStyleBookをインポートして同期する 488
リポジトリを追加し、外部リポジトリからStyleBookをインポートする 490
GitHub/GitLabからStyleBookとConfigPackをインポートする手順 491
デフォルトのStyleBookを使用する 491
デフォルトのスタイルブックから構成を作成するには 491
Webアプリケーションファイアウォール StyleBook 493
アプリケーションファイアウォール構成の展開 493
すべてのデフォルトStyleBookを非表示にする 496
PrometheusアナリティクスStyleBook 497
前提条件 497
StyleBooks Configuration Builderを使用したNetScaler®アプリケーション構成の移行 498
移行された構成間での構成エンティティの共有 499
サポートされているNetScaler機能 499
NetScalerアプリケーション構成を移行するためのStyleBookを作成する 500
制限事項 503
ビジネスアプリケーションのStyleBook 504
SSO Google Apps スタイルブック 504
SSO Googleアプリ StyleBookを展開するには 505
SSO Office 365 スタイルブック 509
SSO Microsoft Office 365 StyleBookを展開するには 510

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

マイクロソフト スカイプ for ビジネス スタイルブック 514
主要コンポーネント 514
企業におけるNetScalerインスタンスの構成 515
マイクロソフト エクスチェンジ StyleBook 521
Microsoft Exchange StyleBookを使用して構成されるNetScaler機能 521
前提条件 522
マイクロソフト エクスチェンジ StyleBook の構成 522
Microsoft SharePoint スタイルブック 524
前提条件 524
Microsoft SharePoint 2016 StyleBook によって構成される NetScaler 機能 524
SharePoint StyleBook構成の展開 526
NetScalerインスタンスで定義されたオブジェクトの表示 528
Microsoft ADFS プロキシ StyleBook 529
NetScaler を ADFS プロキシとして使用する利点 529
Oracle e-ビジネス StyleBook 534
Oracle E-Business Suite 12.2の構成を作成するには 534
Citrix StoreFront™ スタイルブック 535
Citrix StoreFrontアプリケーションの構成を作成する 535
カスタムStyleBookを作成して使用する 536
開始する前に 536
StyleBookの構造 537
ロードバランシング仮想サーバーを作成するためのStyleBook 539
ヘッダー 539
コンポーネント 544
StyleBookを構築する 546
基本的なロードバランシング構成を作成するためのStyleBook 548
ヘッダー 549
コンポーネント 552

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

出力 556
StyleBook を構築する 557
複合StyleBookを作成する 561
StyleBookを構築する 562
カスタムStyleBookでGUI属性を使用する 566
カスタムStyleBookをインポートする 567
StyleBookをインポートするには 568
カスタムStyleBookを検索する 571
構成パックの作成と編集 572
構成パックの作成 572
StyleBook の外部で作成された構成を再利用し、ConfigPack 間で構成を共有する 573
config packのStyleBookを変更する 573
config packのエクスポートまたはインポート 576
設定パックを下書きとして保存する 578
コンフィグパックのスケジュールを作成する 578
設定パックからターゲットインスタンスをデタッチする 579
StyleBookを作成する 580
NetScaler Consoleにファイルをアップロードするための StyleBookを作成する 584
StyleBook構成 584
StyleBookを構築する - 1 584
StyleBookを構築する - 2 586
ファイルをアップロードするための構成を作成する 588
NetScaler ConsoleにSSL証明書と証明書キーファイルをアップロードするための StyleBookを作成する 589
StyleBook構成 589
SSLファイルをアップロードするための構成の作成 592
StyleBookを作成する 593
StyleBookを使用して証明書ストアからSSL証明書を管理する 597

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

パラメータ 597
コンポーネント 598
StyleBook を構築する 599
StyleBookで定義された仮想サーバーでアナリティクスを有効にし、アラームを設定する 604
インスタンスロール 606
ターゲットロールセクション 606
「default」ロール 607
ロールを持つコンポーネント 608
StyleBookを構築する 611
APIの使用 614
非CRUD操作を実行するStyleBookを作成する 616
非CRUD操作のサポート 617
StyleBookのconfig packを別のStyleBookに移行する 618
config packを移行する 618
StyleBookを構築する 620
データソースの管理 624
NetScalerインスタンスをデータソースとして使用する 625
コレクションなしで組み込みデータソースを使用する 625
コレクションで組み込みデータソースを使用する 628
ターゲットNetScalerインスタンスをデータソースとして使用する 635
ターゲットNetScalerインスタンスをデータソースとして使用するStyleBookの例 635
カスタムデータソースを使用する 637
データソースタイプを追加する 638
データソースタイプの下にコレクションスキーマを追加する 638
データソースを追加する 638
コレクションデータを追加する 639
コレクションなしでカスタムデータソースを使用する 639
コレクションでカスタムデータソースを使用する 641

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

APIを使用してStyleBookから構成を作成する 645
例1 645
例 2 648
例 3 651
例 4 653
設定の更新 655
設定の削除 657
APIを使用して、証明書とキーファイルをアップロードするための構成を作成する 658
APIを使用して、あらゆるファイルタイプをアップロードする構成を作成する 660
APIを使用してカスタムStyleBookをインポートする 661
APIを使用してカスタムStyleBookをダウンロードする 663
APIを使用してカスタムStyleBookを削除する 664
StyleBooks の文法 665
ヘッダー 667
StyleBookのインポート 669
パラメータ 670
「名前」 670
「ラベル」 671
「説明」 671
'タイプ' 671
'ネットワーク' 674
「動的割り当て」 674
「キー」 675
「必須」 675
'許可される値' 676
'デフォルト' 677
「パターン」 679
「最小値」 679

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

'最大値' 680
'最小長' 680
'最大長' 680
'最小項目数' 681
'最大項目数' 681
'GUI' 682
「カラム」 682
「更新可能」 682
「'collapse_pane'」 682
「レイアウト」 688
「依存パラメータ」 689
Parameters-default-sources コンストラクト 691
パラメータソースコンストラクト 696
パラメータ条件 697
'オーグメント・アロード・バリュー' 698
'show' または 'hide' 698
'セット・デフォルト' 699
'セットリクワイアード' 700
'セットアロードバリュー' 700
'セットラベル' 701
'セットディスクリプション' 701
'コラプス・ペイン' または 'エクスパンド・ペイン' 702
'セット・パターン' 702
ネストされたパラメータ条件 703
置換 704
置換マップ 712
置換リストを反復処理する 712
コンポーネント 715

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

ヘルパーコンポーネント 718
オプションのプロパティ 720
プロパティーズ・デフォルト・ソース 構成要素 722
コンポーネントのプロパティの計算 724
ネストされたコンポーネント 725
条件コンストラクト 727
繰り返し構成要素 729
リピート条件構文 732
ネストされた繰り返し 733
出力 736
パラメータリファレンス 737
親参照 739
コンポーネントリファレンス 741
置換リファレンス 743
変数参照 743
操作 744
アナリティクス 749
ターゲット仮想サーバーとインサイトタイプ 752
アラーム 753
式 757
算術式 757
文字列式 757
リスト式 757
関係式 758
論理式 - ブール 758
逐語的な文字列式 759
ターゲット式 760
式の型検証 761

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

インプレース補間 763
補間内で許可される型 764
単純な補間 765
自動型変換 765
連続補間 766
ネストされた補間 766
quotewrap を使用した補間 766
組み込み関数 767
文字列() 767
int() 関数 768
bool() 関数 768
len() 関数 768
min() 関数 769
max() 関数 769
bin() 関数 770
oct() 関数 770
hex() 関数 770
ローワー() 770
アッパー() 770
サム() 770
pow() 関数 771
ip() 771
base64.encode() 772
base64.decode() 772
イグジスツ() 772
フィルター() 772
if-then-else() 関数 773
join() 関数 774

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

split()関数 774
マップ() 775
quotewrap() 関数 776
replace() 関数 776
trim()関数 777
truncate() 関数 777
distinct() 関数 777
url.encode() 777
url.decode() 778
is-ipv4() 関数 778
is-ipv6() 関数 778
startswith() 関数 778
endswith() 関数 778
contains() 関数 779
substring() 関数 779
複数() 780
反転() 780
依存関係の検出 781
循環依存関係 783
セキュリティ 785
アプリケーションセキュリティダッシュボード 785
脅威インデックスの詳細 786
安全性インデックスの詳細 786
統合セキュリティダッシュボード 787
保護されたアプリケーション 788
保護されていないアプリケーションの保護を設定する 788
アプリケーションセキュリティ違反の詳細を表示 794
前提条件 794

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

APIセキュリティ 795
API分析を表示 795
APIエンドポイントの分布 795
APIインスタンス 796
APIエンドポイント 796
認証失敗 796
さまざまなAPIインサイトを表示する 797
APIエンドポイントを検出する 799
APIエンドポイントを表示する 800
ゲートウェイ 801
Gateway Insight 801
注意点 802
制限事項 802
Gateway Insightを有効にする 803
NetScaler Consoleバージョン**13.0 Build 41.x以降**の場合 804
GUIを使用してNetScaler GatewayアプライアンスでAppFlow認証、承認、および監査ユーザー名ログを有効にする 804
Gateway Insightレポートの表示 804
EPA、SSO、認証、承認、およびアプリケーション起動の失敗を表示するには 805
セッションモード、クライアント、およびユーザー数の概要を表示するには 805
ユーザーのGateway Insightレポートを表示する 805
ユーザーの詳細を表示するには 805
アプリケーションのGateway Insightレポートを表示する 807
アプリケーションの詳細を表示するには 807
ゲートウェイのGateway Insightレポートを表示する 808
ゲートウェイの詳細を表示するには 808
レポートのエクスポート 808
レポートをエクスポートするには 809

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

Gateway Insight のユースケース 809

ユーザーが NetScaler Gateway アプライアンスまたは内部 Web サーバーにログインできない 809

認証の失敗 810

EPAの失敗 811

SSO障害 812

NetScaler Gatewayに正常にログオンした後、ユーザーが仮想アプリケーションを起動できない 812

新しいアプリケーションを正常に起動した後、ユーザーはそのアプリケーションによって消費された合計バイト数と帯域幅を表示したいと考えています 813

ユーザーはNetScaler Gatewayに正常にログオンしましたが、内部ネットワーク内の特定のネットワークリソースにアクセスできません 814

異なるユーザーが異なるNetScaler Gateway展開を使用しているか、または異なるアクセスモードでNetScaler Gatewayにログオンしている可能性があります。管理者は、展開タイプとアクセスモードに関する詳細を表示できる必要があります 814

Gateway Insight の問題のトラブルシューティング 815

Gateway Insight 構成チェックリスト 815

NetScaler と NetScaler Console 間の接続チェックリスト 815

NetScalerチェックリストでのレコード生成 816

NetScaler Consoleでのレコードの検証 816

NetScaler ConsoleでのLogstreamログの検証 816

Gateway Insight カウンター 817

NetScalerログのAppFlowレコード 817

Citrixテクニカルサポートへのお問い合わせ 819

既知の問題 819

HDX™ インサイト 819

パフォーマンス低下の根本原因の特定 820

シナリオ1 820

シナリオ2 821

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

HDX Insightのジオマップ 822
ユースケース 823
制限事項 823
HDX™ Insight データ収集の有効化 823
LANユーザーモードで展開されたNetScalerを監視するためのデータ収集の有効化 824
シングルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする 827
ダブルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする 829
Optimal Gatewayに使用される仮想サーバーでHDX Insightを構成する 830
トランスペアレントモードで展開されたNetScalerを監視するためのデータ収集を有効にする 836
シングルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする 839
トランスペアレントモードで展開されたNetScalerを監視するためのデータ収集を有効にする 840
ダブルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする 843
LANユーザーモードで展開されたNetScalerを監視するためのデータ収集を有効にする 848
HDX™ Insight のしきい値を作成し、アラートを設定する 851
使用例 852
HDX™ Insight レポートとメトリクスの表示 854
ユーザービューのレポートとメトリクス 855
アプリケーションビューのレポートとメトリック 867
デスクトップビューのレポートとメトリクス 874
インスタンスビューのレポートとメトリック 886
ライセンスビューレポートとメトリック 891
アプリケーションビューのレポートとメトリック 891
デスクトップビューのレポートとメトリック 898

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

ユーザービューのレポートとメトリクス 910
インスタンスビューのレポートとメトリック 922
ライセンスビューレポートとメトリクス 926
HDX™ Insight の問題のトラブルシューティング 926
HDX Insight 構成チェックリスト 927
NetScalerとNetScaler Console間の接続チェックリスト 927
NetScalerにおけるHDX/ICAトラフィックのレコード生成チェックリスト 928
エラーカウンター 936
nstraceの検証 941
NetScaler Consoleチェックリストにおけるレコードの入力 941
Citrixテクニカルサポートに連絡する前に 941
既知の問題 942
インフラストラクチャ 943
インフラストラクチャ分析 943
インフラストラクチャ分析 944
インスタンススコア 944
健全性インジケーター 944
NetScalerの容量の問題を表示する 946
ヘルスインジケーターの値 947
インフラストラクチャ分析ダッシュボード 948
サークルパックビュー 949
インスタンスの円 949
グループ化されたインスタンスの円 949
クラスター化されたインスタンスの円 950
Circle Pack の使用方法 951
表形式ビュー 951
概要パネルの使用方法 952
インスタンス情報 953

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

トラフィックプロファイル 954
設定パネルの使用方法 954
表示 954
スコアしきい値 954
ダッシュボードでデータを視覚化する方法 955
Infrastructure Analytics でインスタンスの詳細を表示 956
NetScalerインスタンスのキャパシティ問題を表示する 960
キャパシティの問題を解決するための推奨アクションを表示 961
新しいインジケーターによる強化されたインフラストラクチャ分析 962
表形式ビュー 964
異常の詳細を表示 964
インスタンス管理 964
インスタンスを追加する 965
インスタンスダッシュボードの使用方法 965
グローバルに分散されたサイトを監視する 966
ユースケース 967
ジオマップの構成 968
タグを作成してインスタンスに割り当てる方法 970
タグとプロパティの値を使用してインスタンスを検索する方法 971
NetScaler VPXインスタンスを検索するには 972
NetScaler® Console を介した集中型 GeoIP DB アップデート 973
制限事項 973
NetScaler Console を介した集中型 GeoIP DB 更新の構成 974
NetScalerインスタンスの管理パーティションを管理する 975
NetScaler高可用性ペアを作成する 978
NetScalerインスタンスのバックアップと復元 980
インスタンスのバックアップ設定を構成する 981
NetScaler Consoleを使用してNetScalerインスタンスを復元する 984

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

セカンダリNetScalerインスタンスへのフェールオーバーを強制する 986
セカンダリNetScalerインスタンスをセカンダリのままにするように強制する 987
インスタンスグループを作成する 988
NetScaler Consoleを使用してインスタンスグループを作成するには 988
マップされていないインスタンスを識別してグループに追加するには 988
NetScaler Console を使用して SDX に NetScaler VPX インスタンスをプロビジョニングする 989
ステップ 1 - VPX インスタンスを追加する 989
ステップ2 - ライセンスの割り当て 990
ステップ 3 - リソースの割り当て 991
ステップ4 - インスタンス管理の追加 994
ステップ5 - ネットワーク設定の指定 994
ステップ6 - 管理VLAN設定の指定 996
プロビジョニングされたVPXインスタンスの表示 997
VMware ESX上にNetScaler VPXインスタンスをプロビジョニングする 997
前提条件 997
NetScaler VPXファイルをテンプレートに変換する 998
NetScaler ConsoleがVMware vCenterにアクセスするための権限を作成する 998
NetScaler Console でサイトを作成する 999
VMware ESX でインスタンスをプロビジョニングする 1000
複数のNetScaler VPXインスタンスを再検出する 1001
インスタンスの管理を解除する 1002
インスタンスへのルートをトレースする 1002
NetScalerが所有するIPアドレスを表示する 1003
NetScalerが所有するIPアドレスをエクスポートする 1003
NetScalerが所有するIPアドレスのエクスポートをスケジュールする 1004
あるNetScalerインスタンスから別のインスタンスへの構成のレプリケート 1005
あるインスタンスから他のNetScalerインスタンスに構成をレプリケートするには 1006

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

SSL証明書管理 1006
エンタープライズSSLポリシー設定 1007
NetScaler Console証明書の仕組み 1007
SSL証明書管理のユースケース 1008
SSL証明書のインストール 1008
証明書の有効期限に関する通知設定 1008
証明書の更新 1009
SSL証明書のリンクとリンク解除 1010
監査ログ 1010
ACMEプロトコルを使用した証明書の自動更新 1011
NetScaler® ConsoleでのACMEサポート 1011
ACME統合のための設定手順 1013
発行と更新 1020
証明書の発行 1022
サードパーティ統合 1023
制限事項 1025
自動証明書更新に関する問題のトラブルシューティング 1025
ゼロタッチ証明書管理 1026
証明書のアップロード 1027
ゼロタッチ証明書管理を有効にする 1027
SSLフィルターモードのサポート 1028
フィルターモード設定の構成 1029
SSLダッシュボードを使用する 1030
SSL証明書を監視するには 1030
SSL証明書の監査証跡を表示するには 1032
SSLダッシュボードでSSL証明書を削除するには 1032
SSLダッシュボードでデフォルトのNetScaler証明書を除外するには 1033
SSLファイルの表示、アップロード、ダウンロード 1033

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

SSL証明書チェーンの表示 1034
SSL証明書の有効期限切れ通知を設定する 1034
インストール済み証明書を更新する 1036
NetScalerインスタンスにSSL証明書をインストールする 1036
証明書署名要求 (CSR) を作成する 1038
SSL証明書をリンクおよびリンク解除する 1040
エンタープライズポリシーの構成 1041
NetScalerインスタンスからSSL証明書をポーリングする 1041
NetScaler Console証明書ストアを使用してSSL証明書を管理する 1042
証明書ストアにSSL証明書を追加する 1042
証明書ストア内のSSL証明書を更新する 1043
証明書ストアからSSL証明書を削除する 1044
NetScaler® インスタンスにSSL証明書をインストールする 1044
NetScaler インスタンスから証明書をインポートする 1044
中間アップロードなしでサーバー証明書を更新する 1045
高可用性展開におけるデータベースのカスタム証明書と暗号の管理 1046
NetScaler Consoleにデータベース証明書をインストールする 1046
インストールされているデータベース証明書を管理する 1047
データベースの暗号スイートを構成する 1048
イベント 1048
イベントダッシュボードを使用する 1049
イベントのイベント期間を設定する 1050
イベントフィルターをスケジュールする 1050
イベントのメール通知を繰り返し設定する 1051
イベントを抑制する 1052
イベントルールを作成する 1053
ステップ1 - イベントルールを定義する 1054
ステップ2 - イベントの重大度を選択する 1055

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

ステップ3 - イベントカテゴリを指定する 1055
ステップ 4 - NetScalerインスタンスの指定 1055
ステップ 5 - 障害オブジェクトの選択 1056
ステップ 6 - 詳細フィルターの指定 1056
ステップ7 - イベントルールアクションの追加 1057
NetScalerインスタンスで発生するイベントの報告された重大度を変更する 1064
イベント概要の表示 1065
イベントメッセージを表示 1065
イベントの重要度とSNMPトラップの詳細を表示 1066
NetScaler syslogメッセージの表示とエクスポート 1067
NetScaler Consoleをsyslogサーバーとして構成する 1068
syslogメッセージの表示と検索 1068
syslogメッセージのエクスポートとスケジュール 1069
syslogメッセージを抑制する 1069
フィルターを作成してsyslogメッセージを抑制する 1070
フィルターの無効化 1070
インスタンスイベントのパージ設定を構成する 1071
ネットワーク機能 1071
ロードバランシングエンティティのレポートを生成する 1072
結合されたロードバランシングレポートを生成する 1073
個別の負荷分散エンティティレポートを生成する 1074
ネットワーク機能レポートのエクスポートまたはエクスポートのスケジュール設定 1074
ネットワークレポート 1076
ネットワークレポートダッシュボード 1077
ネットワークレポートのエクスポート 1079
集計を適用してネットワークレポートデータを表示する 1080
NetScaler Consoleでネットワークレポートのしきい値を管理する方法 1082
ネットワークレポートのパフォーマンスポーリング間隔を設定する 1084

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

ネットワークレポートのプルーニング設定 1084
構成ジョブ 1084
構成テンプレート 1085
インスタンス 1085
ファイル 1086
記録と再生 1086
関連情報 1086
構成ジョブの作成 1086
記録と再生を使用して構成ジョブを作成する 1090
構成ジョブを使用して、あるインスタンスから複数のインスタンスに構成をレプリケートする 1092
構成ジョブで変数を使用する 1093
修正コマンドから構成ジョブを作成する 1097
あるNetScalerインスタンスから別のインスタンスへ、実行中および保存済みの構成を複製する 1098
実行済み構成ジョブを再利用する 1099
構成ジョブでSCP (put) コマンドを使用する 1100
構成テンプレートを使用する 1103
マスター構成テンプレートを使用する 1103
組み込みテンプレートを使用して作成されたジョブをスケジュールする 1109
NetScalerからPrometheusへのメトリクスエクスポートを設定するジョブをスケジュールする 1110
構成テンプレートを使用して監査テンプレートを作成する 1113
組み込みテンプレートを使用して構成されたジョブを再スケジュールする 1114
構成ジョブで構成監査テンプレートを再利用する 1115
構成テンプレートのインポートとエクスポート 1117
構成監査 1119
監査レポートの表示 1119

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

インスタンス全体の構成変更を監査する 1123
ネットワーク構成に関する構成アドバイスを取得する 1126
NetScaler® インスタンスの構成監査をポーリングする 1128
ConfigChange SNMPトラップの構成監査差分を生成する 1128
アップグレードジョブ 1129
アップグレード前の検証 1131
NetScaler Consoleによって実行されるアップグレード前チェック 1131
NetScalerによって実行されるアップグレード前チェック 1132
NetScalerインスタンスのアップグレードをスケジュールする 1132
NetScaler SDXインスタンスのアップグレードをスケジュールする 1136
NetScaler BLXインスタンスのアップグレードをスケジュールする 1136
Autoscale™グループのアップグレードをスケジュールする 1139
NetScalerインスタンスのHAペア設定をスケジュールする 1140
HAペアインスタンスのクラスターへの変換をスケジュールする 1141
ジョブを使用してNetScaler®インスタンスをアップグレードする 1142
事前検証チェック 1142
NetScaler高可用性ペア 1143
NetScalerクラスター 1143
NetScalerインスタンスをアップグレードするためのアップグレードメンテナンスジョブを作成する 1144
スケジュールされたアップグレードジョブの一時停止または再開 1149
失敗したアップグレードジョブを再試行する 1150
NetScalerディスク容量のクリーンアップ 1151
NetScaler®高可用性ペアのアップグレードジョブのスケジュール設定 1152
NetScalerアップグレードジョブの結合差分レポートをダウンロードする 1153
セキュリティアドバイザリ 1153
セキュリティアドバイザリのランディングページ 1154
セキュア構成の推奨事項 1155

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

CVE検出 1155
ファイル整合性監視 1155
今すぐスキャン 1156
スキャン履歴 1156
影響を受けるNetScaler 1156
設定 1157
セキュアな構成の推奨事項 1158
重要度に基づく優先順位付け 1158
詳細なインスタンスレベルビューの利点 1158
構成推奨事項の修復 1159
CVE検出 1162
インスタンスビュー 1163
CVEビュー 1165
CVEリポジトリ 1165
注意事項 1166
ファイル整合性監視 1167
コンソール検出 1168
デバイスレポート 1170
NetScaler Consoleにおける侵害の痕跡の検出 1170
前提条件 1170
利点 1170
セキュリティアドバイザリを介してサポートされるCVE 1171
最新のサポートされているCVE 1171
サポートされているCVE 1173
CVE-2026-88771の脆弱性を特定して修正する 1176
CVE-2026-88771を修正する 1177
CVE-2026-88772の脆弱性を特定して修正する 1177
CVE-2026-88772を修正する 1178

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

CVE-2026-88773の脆弱性を特定し、修正する 1178
CVE-2026-88773を修正する 1179
CVE-2026-88774の脆弱性を特定し、修正する 1179
CVE-2026-88774を修正する 1180
CVE-2026-88775 の脆弱性を特定し、修正する 1180
CVE-2026-88775 を修正する 1180
CVE-2026-88776の脆弱性を特定し、修正する 1181
CVE-2026-88776を修正する 1181
CVE-2026-88777の脆弱性を特定し、修正する 1182
CVE-2026-88777を修正する 1182
CVE-2026-88778 の脆弱性を修正する 1182
CVE-2026-88778 を修正する 1183
CVE-2026-19490の脆弱性を特定して修正する 1184
CVE-2026-19490を修正する 1185
CVE-2026-19489の脆弱性を特定し、修正する 1185
CVE-2026-19489を修正する 1186
CVE-2026-13474の脆弱性を修正する 1186
CVE-2026-13474を修正する 1186
CVE-2026-10817の脆弱性を特定して修復する 1188
CVE-2026-10817を修復する 1189
CVE-2026-10816の脆弱性を特定し、修正する 1189
CVE-2026-10816を修正する 1190
CVE-2026-8655 の脆弱性を特定して修復する 1190
CVE-2026-8655 を修復する 1190
CVE-2026-8452 の脆弱性を特定し、修正する 1191
CVE-2026-8452 を修正する 1191
CVE-2026-8451の脆弱性を特定して修正する 1192
CVE-2026-8451を修正する 1192

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

CVE-2026-4368 の脆弱性を特定し、修正する 1192
CVE-2026-4368 を修正する 1193
CVE-2026-3055 の脆弱性を特定して修正する 1193
CVE-2026-3055 を修正する 1194
CVE-2025-12101 の脆弱性を特定し、修復する 1194
CVE-2025-12101 を修復する 1195
CVE-2025-8424 の脆弱性を特定して修正する 1195
CVE-2025-8424 を修正する 1196
CVE-2025-7776 の脆弱性を特定し、修正する 1197
CVE-2025-7776 を修正する 1198
CVE-2025-7775の脆弱性を特定し、修復する 1198
CVE-2025-7775を修復する 1199
CVE-2025-6543の脆弱性を特定し、修復する 1200
CVE-2025-6543を修復する 1201
CVE-2025-5349の脆弱性を特定し、修復する 1201
CVE-2025-5349を修復する 1202
CVE-2025-5777の脆弱性を修復する 1203
CVE-2025-5777を修復する 1203
CVE-2024-8535の脆弱性を修正する 1206
CVE-2024-8535を修正する 1206
CVE-2020-8300の脆弱性に対処する 1209
CVE-2020-8300に対処する 1209
シナリオ 1214
CVE-2021-22927およびCVE-2021-22920の脆弱性に対処する 1216
CVE-2021-22927およびCVE-2021-22920に対処する 1216
シナリオ 1221
CVE-2021-22956の脆弱性を特定して修正する 1222
CVE-2021-22956の影響を受けるインスタンスを特定する 1223

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

CVE-2021-22956を修正する 1223
CVE-2022-27509の脆弱性を特定し、修正する 1226
CVE-2022-27509の影響を受けるインスタンスを特定する 1227
CVE-2022-27509を修正する 1227
セキュリティアドバイザリにおけるサポートされていないCVE 1228
アップグレードアドバイザリ 1229
アップグレードアドバイザリを表示 1230
推奨ビルドを設定する 1230
NetScalerインスタンスをアップグレードする 1231
オーケストレーション 1233
VMware NSX マネージャー 1234
OpenStack: NetScalerインスタンスの統合 1235
OpenStack Neutron LBaaS用NetScalerドライバー 1235
NetScaler ConsoleとOpenStackの相互登録 1235
OpenStackのテナント 1236
配置ポリシー 1236
サービスパッケージ 1236
LBaaS V1およびLBaaS V2でサポートされる機能 1236
ユースケースシナリオ 1237
NetScaler ConsoleとOpenStackワークフローの統合 1238
OpenStack: NetScalerインスタンスの統合 1239
前提条件 1242
NetScaler ConsoleとOpenStackでの事前構成タスク 1243
Horizon を使用して LBaaS V1 を構成する 1252
コマンドラインを使用してLBaaS V2を構成する 1252
レイヤー7コンテンツスイッチングの構成 1257
OpenStackでのNetScaler VPXインスタンスの手動プロビジョニング 1265
OpenStack上でのStyleBookを使用したNetScaler VPXインスタンスのプロビジョニング 1267



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

OpenStack環境におけるVPXチェックイン/チェックアウトライセンスおよびプールライセンスのサポート 1269
管理パーティションの共有VLANサポート 1270
トライアルライセンスのワークフロー 1271
OpenStack Heatサービスとの統合 1272
サービスパッケージの分離ポリシー 1276
柔軟なポリシーベースのデバイス割り当て 1277
NSX Manager: NetScalerインスタンスの手動プロビジョニング 1281
前提条件 1281
VMware ESXiのハードウェア要件 1282
VMware NSXの構成 1282
NetScaler Console で NetScaler VPX インスタンスを追加する 1283
NetScaler ConsoleへのVMware NSX Managerの登録 1284
NetScaler Consoleでのサービスパッケージの作成 1284
エッジのロードバランサーサービス挿入の実行 1285
NSX ManagerでのL2ゲートウェイの表示 1287
割り当てられたNetScalerの表示 1287
StyleBookを使用したNetScaler VPXインスタンスの構成 1288
ロードバランサー構成の表示 1288
ロードバランサーサービスの削除 1289
NSX Manager: NetScalerインスタンスの自動プロビジョニング 1289
概要 1289
前提条件 1290
NetScaler ConsoleとNetScalerインスタンスの高可用性展開 1290
NetScaler Console HAエンドポイントの詳細設定 1290
VMware NSX ManagerをNetScaler Consoleに登録する 1291
NetScaler Consoleでのライセンスのアップロード 1291
NetScaler Console で NetScaler VPX イメージをアップロードする 1292

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

NetScaler Console でサービスパッケージを作成する 1292
Edge へのロードバランサーサービス挿入の実行 1294
VMware NSX Manager GUIでNetScaler VPXの負荷分散サービスを構成する 1296
NetScaler Console GUIでのNetScaler VPXの負荷分散サービスの設定 1297
NetScaler VPXインスタンスでの仮想サーバーとサービスグループの作成の確認 1297
ロードバランシングサービスの削除 1298
NetScaler Console で Kubernetes Ingress 構成を管理する 1298
開始する前に 1299
Kubernetesクラスターを管理するためのシークレットトークンでNetScaler Consoleを構成する 1300
NetScaler ConsoleにKubernetesクラスターを追加する 1300
設定 1302
IPアドレス管理 (IPAM) の構成 1302
外部 IP アドレスプロバイダーの追加 1302
外部プロバイダーとしてのInfoblox DDI 1304
ネットワークを追加する 1305
割り当てられたIPアドレスを表示する 1306
アプリケーションイベント通知を受信するためのアクションポリシーを構成する 1306
アクションポリシーの構成 1308
検索バーを使用する 1317
監査ログオプションを使用する 1318
可観測性統合 1318
Splunkとの統合 1318
Splunkを構成して、オンプレミスのNetScaler Consoleからデータを受信する 1319
NetScaler Consoleオンプレミスを構成してSplunkにデータをエクスポートする 1322
Splunkでダッシュボードを表示 1324
New Relic との統合 1325
前提条件 1325

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

New Relicダッシュボード 1327
Microsoft Sentinel との統合 1328
Log Analytics ワークスペースを構成する 1328
Microsoft Entra アプリケーションを作成する 1329
データ収集エンドポイントを構成する 1330
データエクスポート用のテーブルを作成する 1331
NetScaler Consoleでサブスクリプションを作成する 1344
Microsoft Azureでログを表示する 1345
デフォルトスキーマを使用して、Prometheus へのインサイトのエクスポートのためにNetScaler® インスタンスを構成する 1346
失敗した構成のログを表示する 1347
NetScaler®メトリックと監査ログのSplunkへのエクスポートを構成する 1347
失敗した構成のログを表示 1348
アクセス制御リスト 1349
使用ガイドライン 1349
ACL の構成方法 1349
ACL 機能を有効にする 1349
ACLルールを作成する 1349
ACLルールを有効にする 1351
ACLルールのその他のアクション 1351
ACLルールを無効にする 1351
ACLルールを編集する 1351
ACLルールを削除する 1352
ACLルールの優先順位を振り直す 1352
トラブルシューティング 1353
インフラストラクチャの管理と監視のためにNetScaler Console監査ログを使用する 1353
NetScalerインスタンス関連の監査ログ 1353
NetScaler Consoleサービスをsyslogサーバーとして構成する 1354

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

NetScaler Console関連の監査ログ 1354
監査ログとシェルログを監視するためのsyslogサーバーの構成 1354
アプリケーション関連の監査ログ 1355
NetScalerライセンス 1356
ライセンスアクティベーションサービス 1356
LASのNetScalerバージョン互換性 1358
LASへの移行 1359
Cloud ConnectでLASをアクティブ化 1359
NetScalerインスタンスをLASにライセンス供与または移行する 1361
ライセンスアクティベーションBLOBの動作 1365
ライセンス猶予期間アラート 1365
ConsoleオンプレミスとConsoleサービス間の接続が切断された場合のNetScalerの動作の更新 1365
LASライセンスワークフロー中にLASに送信される情報 1367
LASに移行したNetScaler Consoleオンプレミス環境（クラウド接続済み）を監視するためのベストプラクティス 1368
前提条件 1368
Console on-premises LASアクティベーションブロブの有効期限を監視する 1369
GUIを使用して最終更新日を監視する 1369
NetScalerインスタンスのLASアクティベーションBLOBの有効期限を監視する (オンプレミスでクラウド接続されたConsoleを介してライセンス供与されたNetScaler) 1371
CLIを使用してNetScalerインスタンスのステータスを表示する 1371
通知 1371
ライセンスエンタイトルメントの有効期限を監視する 1373
通知 1373
メールベースの通知 1373
ライセンス管理 1374
LASベースのライセンス 1375

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

ライセンスサーバーポート 1375
ライセンス有効期限情報 1376
通知設定 1376
LASのRBACサポート 1379
手動で管理されるエンタイトルメント (ファイルベースのライセンス) 1379
ライセンスファイル 1379
重要な注意事項 1381
ライセンスサーバーのポート設定 1382
ライセンスの有効期限情報 1383
通知設定 1383
FlexedおよびPooledライセンスの最小および最大容量 1386
表1. MPXでサポートされるFlexed容量 1388
表2A. ビルド13.0-47.xより前のNetScaler SDXバージョンでサポートされるFlexed容量 1389
表2B. NetScaler SDX バージョン13 (ビルド13.0-47.x以降)、バージョン13.1 (ビルド51.xより前)、およびバージョン14.1 (ビルド12.xより前) のサポートされるFlexed容量 1390
表 2C. NetScaler SDX バージョン 13.1 (ビルド 51.x 以降) およびバージョン 14.1 (ビルド 12.x 以降) でサポートされるFlexed容量 1391
表3. NetScaler CPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス 1393
表4. ハイパーバイザーおよびクラウドサービス上のNetScaler VPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス数 1393
表5. NetScaler BLXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス 1394
表 6. 異なるフォームファクターのゼロキャパシティライセンス要件 1394
Flexed容量ライセンス 1395
ゼロキャパシティハードウェア 1396
Z-capライセンスの管理とインストール 1397
スタンドアロンNetScaler VPXインスタンス 1397
スタンドアロンNetScaler CPXインスタンス 1398

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

スタンドアロンNetScaler BLXインスタンス 1399
帯域幅プール 1399
インスタンスプール 1399
ライセンスの構成 1400
LASベースのライセンス 1402
ステップ1: LASをアクティブ化し、エンタイトルメントを取得する 1402
ステップ2：NetScaler Console On-premにNetScalerインスタンスを追加する 1402
ステップ3：NetScalerインスタンスのライセンス供与または移行 1402
ステップ4：Flexedスループット容量の編集 1402
ライセンスのないMPXアプライアンスの特別なライセンス 1403
ライセンスアクティベーションブロブの動作 1404
ライセンス猶予期間アラート 1404
手動で管理されるエンタイトルメント（ファイルベースライセンス） 1404
はじめる前に 1404
ステップ1 - NetScaler Consoleでライセンスを適用する 1405
ステップ2 - NetScaler Consoleをライセンスサーバーとして登録し、ライセンスを割り当てる 1405
ステップ3 - NetScalerインスタンスのFlexedスループット容量を編集する 1407
NetScaler MPX-Z 1408
NetScaler SDX-Z 1408
NetScaler高可用性ペアのライセンス要件（LASとファイルベースライセンスの両方に共通） 1409
NetScaler Flexedライセンスの状態（LASとファイルベースライセンスの両方に共通） 1409
フレックスライセンスダッシュボード 1410
NetScalerインスタンスで割り当てられたスループット容量を編集する 1412
NetScalerインスタンスでライセンスを解放する 1413
Flexedライセンスレポート 1413
フレックス型ライセンスへの移行 1416

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

LASベースのライセンス 1417
手動で管理されるエンタイトルメント (ファイルベースライセンス) 1418
プール帯域幅ライセンスからFlexedライセンスへ 1418
プールされたvCPUからFlexed帯域幅容量へ 1419
固定サブスクリプションまたは永続ライセンスからFlexedライセンスへ 1420
CICOからFlexed帯域幅容量へ 1421
FlexedまたはPooledライセンスの有効期限切れと接続性の問題の動作シナリオ 1421
LASベースのライセンス 1422
期間満了前 1422
期間満了後 1422
接続の問題の動作シナリオ 1423
手動で管理されるライセンス（ファイルベースのライセンス） 1423
Flexedライセンスの種類 1423
シナリオ：MPXフォームファクター 1424
シナリオ：SDXフォームファクター 1424
シナリオ：VPX/BLX/CPXフォームファクター 1425
接続の問題の動作シナリオ 1425
NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとして構成する 1426
NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成する方法 1427
レガシーライセンス 1429
NetScaler プール型キャパシティ 1429
NetScalerプール型キャパシティライセンスの仕組み 1430
ゼロキャパシティハードウェア 1431
スタンドアロンNetScaler VPXインスタンス 1432
スタンドアロン NetScaler CPX インスタンス 1433
スタンドアロン NetScaler BLX インスタンス 1433
帯域幅プール 1433

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

インスタンスプール 1434
NetScaler Console ライセンスサーバー 1434
NetScaler プール型キャパシティを設定する 1440
サポートされているハードウェアおよびソフトウェアのバージョン 1441
NetScaler プール容量の状態 1441
ステップ1 - NetScaler Consoleでライセンスを適用する 1442
ステップ2 - NetScaler Consoleをライセンスサーバーとして登録する 1442
ステップ3 - NetScalerインスタンスにプールライセンスを割り当てる 1445
NetScalerインスタンスでプールされたキャパシティを構成する 1447
NetScaler VPX の永続ライセンスを NetScaler Pooled capacity にアップグレードする 1448
前提条件 1449
NetScaler VPX高可用性ペアの永続ライセンスをNetScalerプール容量にアップグレードする 1451
NetScaler MPX の永続ライセンスを NetScaler Pooled Capacity にアップグレードする 1453
NetScaler MPX高可用性ペアにおける永続ライセンスのNetScalerプール容量へのアップグレード 1456
NetScaler SDXの永続ライセンスをNetScalerプール容量にアップグレードする 1459
クラスターモードのNetScalerインスタンスにおけるNetScalerプール容量 1462
NetScalerクラスターにNetScaler Pooled capacityを割り当てる 1463
CLIを使用してNetScalerクラスターにNetScalerプール容量を割り当てる 1464
NetScaler VPXおよびNetScaler BLXライセンスのチェックインとチェックアウト 1465
前提条件 1466
NetScaler Consoleでのライセンスのインストール 1467
確認 1467
NetScaler GUIを使用して、NetScaler VPXおよびNetScaler BLXライセンスをNetScalerインスタンスに割り当てる 1468
NetScaler CLIを使用してNetScalerインスタンスにNetScaler VPXおよびNetScaler BLXライセンスを割り当てる 1468

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

API を使用して NetScaler VPX および NetScaler BLX ライセンスを NetScaler インスタンスに割り当てる 1469
ライセンスサーバーの IP アドレスを更新する 1470
NetScaler VPX および NetScaler BLX のチェックイン/チェックアウトライセンスの有効期限チェックを設定する 1471
NetScaler仮想CPUライセンス 1472
NetScaler VPX の仮想 CPU ライセンス 1473
CLIを使用してNetScaler VPXライセンスでライセンスサーバーを構成する 1475
NetScaler Consoleでの仮想CPUライセンスの管理 1475
NetScaler CPXの仮想CPUライセンス 1476
問題発生時の予期される動作 1478
ライセンスサーバーが応答を停止する 1479
NetScaler プールインスタンスが応答を停止します 1480
ライセンスサーバーとNetScaler プールインスタンスの両方が応答を停止します 1480
NetScaler プールインスタンスがグレースフルシャットダウンします 1480
ネットワーク接続の問題 1481
猶予期間 1481
システム設定の管理 1482
ネットワーク構成 1482
システム構成 1483
システムメンテナンス 1485
データプルーニング 1485
バックアップ 1486
イベント通知 1487
SSL設定 1487
機能の構成 1488
システムバックアップ設定を構成する 1488
プロキシサーバー設定の構成 1489

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

注意点 1489
プロキシサーバーの構成 1489
CA証明書の管理 1490
プロキシ構成のサポート 1491
プロキシなし (直接インターネットアクセス) 1491
明示的フォワードプロキシ (非インターセプト) 1491
明示的なSSLインターセプトプロキシ 1492
透過的なSSLインターセプトプロキシ 1492
NTPサーバーを構成する 1492
NetScaler Console のアップグレード 1494
アップグレード前のチェック 1494
LASのアップグレード前チェックが失敗した場合のNetScaler Consoleアップグレードのブロック解除 1496
NetScaler Console のパスワードをリセットする方法 1497
NetScaler Consoleにアクセスするためのセカンダリ NICを構成する 1501
前提条件 1502
NetScaler Consoleでセカンダリ NICを構成する 1502
NetScaler® エージェントにアクセスするためのセカンダリ NIC の構成 1503
CLIを使用してIPV4 NICネットワークアドレスを変更する 1503
Syslogパージ間隔の設定 1504
システムのパージ設定とイベントのパージ設定を構成する 1505
NetScaler Console を使用してイベントのパージ設定を構成する 1506
非デフォルトユーザーのシェルアクセスを有効にする 1506
アクセスできないNetScaler Consoleサーバーを回復する 1507
NetScaler Consoleスタンドアロン展開でNetScaler Consoleデータベースリカバリスクリプトを使用する方法 1508
NetScaler Console高可用性展開でNetScaler Consoleデータベースリカバリスクリプトを使用する方法 1510

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

NetScaler Consoleサーバーにホスト名を割り当てる 1510
NetScaler Consoleサーバーをバックアップおよび復元する 1511
NetScaler Consoleの構成をバックアップする 1512
NetScaler Consoleのバックアップファイルを外部システムに転送する 1513
バックアップファイルからNetScaler Consoleの構成を復元する 1513
高可用性展開におけるNetScaler ConsoleのVMスナップショット 1514
NetScaler Consoleサーバーのスナップショットを取得する 1514
NetScaler Consoleサーバーのスナップショットを復元する 1515
監査情報の表示 1515
SSL設定を構成する 1517
CPU、メモリ、ディスク使用量を監視する 1517
通知設定の構成 1518
メール配布リストの作成 1518
SMS配信リストを作成する 1519
Slackプロファイルの作成 1519
PagerDutyプロファイルの作成 1520
ServiceNow プロファイルの表示 1521
テックサポートファイルを生成する 1521
暗号グループを構成する 1523
SNMPトラップ宛先、マネージャーコミュニティ、およびユーザーを作成する 1524
システムアラームの設定と表示 1525
ディスク使用率アラームにしきい値制限を追加する 1526
NetScalerエージェントのSNMPマネージャーとユーザーを作成する 1527
SNMP v2マネージャーを追加する 1527
SNMP v3マネージャーを追加する 1528
SNMPユーザーを追加する 1529
SNMPビューの管理 1529
エージェント設定の構成 1530

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

エージェントのキープアライブ間隔を設定する 1530
現在のパスワードなしでエージェントのパスワードを変更する 1530
データストレージ管理ダッシュボードを使用する 1531
データストレージを理解する 1532
データ取り込みアクティビティのステータス 1532
総ストレージ消費量 1533
ストレージ消費の傾向 1533
機能別のストレージ消費量 1535
ストレージ容量を管理する 1536
データプルーニングを実行する 1536
データ保持ポリシーの確認 1537
ストレージ制限超過時の通知 1538
データ保持ポリシー 1538
システムの削除設定を構成する 1538
インスタンスイベントの削除設定を構成する 1539
インスタンスsyslogの削除設定を構成する 1539
ネットワークレポートの削除設定を構成する 1539
API プロキシサーバーとしての NetScaler Console 1541
NetScaler Console が API プロキシサーバーとして機能する方法 1541
NetScaler ConsoleをAPIプロキシサーバーとして使用する方法 1543
例1：負荷分散仮想サーバーの統計情報を取得する 1546
例2：負荷分散仮想サーバーを作成する 1547
例3：負荷分散仮想サーバーを変更する 1547
例4：負荷分散仮想サーバーを削除する 1548
例5：NetScalerでCLI実行中の構成をダウンロードする 1548
よくある質問 1550
アナリティクス 1550

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

シングルホップモードで展開されたNetScaler GatewayインスタンスでEUEM仮想チャネルを有効にする必要がありますか? 1550

NetScaler ConsoleでWebアプリケーションおよび仮想デスクトップのトラフィックを監視するにはどうすればよいですか? 1550

NetScalerインスタンスを追加した後、NetScaler Consoleは自動的に分析情報の収集を開始します? 1551

分析を有効にするために、個々のNetScalerアプライアンスにアクセスする必要がありますか? 1551

分析を有効にするためにNetScalerインスタンスに一覧表示できる仮想サーバーの種類? 1551

NetScaler Consoleにディスクを追加するにはどうすればよいですか? 1551

NetScalerインスタンスでコレクターが構成されていないとはどういう意味ですか? 1552

クライアント側測定を有効にするとどうなりますか? 1552

認証 1552

認証要求の負荷分散とは何ですか? 1552

外部認証サーバーをカスケード接続する必要があるのはなぜですか? 1553

いくつの外部認証サーバーをカスケード接続できますか? 1553

外部認証が失敗した場合の代替手段はありますか? 1553

フォールバックローカル認証とは何ですか? 1553

外部ユーザーグループの抽出とは何ですか? 1553

グループ権限を割り当てる必要があるのはなぜですか? 1554

構成管理 1554

NetScaler Consoleを使用して、複数のNetScalerインスタンス間で同時に構成を実行できますか? 1554

NetScaler Consoleの構成ジョブとは何ですか? 1554

NetScaler Consoleの組み込みテンプレートを使用してジョブをスケジュールできますか? 1554

証明書管理 1555

NetScaler ConsoleからSSL証明書を削除すると、NetScalerインスタンスからも証明書が削除されますか? 1555

展開 1555

デフォルトのユーザー名とパスワードは何ですか? 1555

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

デフォルトのパスワードを変更する方法? 1555

パスワードをリセットする方法? 1556

HAペアで、プライマリノードのパスワードが変更され、その後「HAペアを解除」オプションが選択された場合、どのような動作になりますか? 1556

2つのスタンドアロンサーバーが異なるパスワードを持っている場合、これら2つのサーバーをHAペアに展開する際の影響? 1556

HA構成は完了しましたが、プライマリノードのGUIにアクセスできません。原因は何か? 1556

HA構成は完了しましたが、フローティングIPアドレスのGUIにアクセスできません。考えられる原因? 1556

NetScaler ConsoleスタンドアロンとNetScaler Console HAでサポートされているDB? 1557

セカンダリノードへの潜在的なデータ損失? 1557

プライマリノードがダウンした場合? 1557

障害が発生したノードを再インストールする方法? 1557

NetScaler ConsoleはSANストレージをサポートしていますか? 1557

NetScaler Consoleは追加ディスクをサポートしていますか? 1558

HAペアを無効にした後、設定されているフローティングIPアドレスはどうなりますか? 1558

再展開時に別のフローティングIPアドレスを指定できますか? 1558

セカンダリノードのGUIにアクセスできないのはなぜですか? 1558

プライマリノードが長期間ダウンした場合でも、フローティングIPアドレスのGUIを使用して構成を行うことはできますか? 1558

将来、プライマリノードのIPアドレス、セカンダリノードのIPアドレス、またはフローティングIPアドレスを変更する必要がある場合（たとえば、IPv6に変更する場合）、推奨される解決策は何ですか? 1558

NetScaler ConsoleはAMDプロセッサをサポートしていますか? 1559

展開（災害復旧） 1559

プライマリサイトとディザスタリカバリサイト間のレプリケーションはどのくらいの頻度で発生しますか? 1559

DRサイトでバックアップスクリプトを開始した後、プライマリサイトが復旧して完全に稼働するまで、DRサイトは一時的なプライマリサイトになりますか? 1559

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

HAペアの解除オプションが選択されている場合、両方のノードはスタンドアロンサーバーとして動作します。スタンドアロンサーバーにはDRサポートが適用されないため、HAペアの解除が選択された場合、DRサイトはどうなりますか? 1560

イベント管理 1560

NetScaler Consoleを使用して、管理対象のNetScalerインスタンスで生成されたすべてのイベントを追跡するにはどうすればよいですか? 1560

イベントルールとは何ですか? 1560

インスタンス管理 1561

NetScalerプール容量ライセンスを使用している場合、帯域幅割り当て後にNetScalerインスタンスがNetScaler Consoleに接続できないとどうなりますか? 1561

NetScaler Consoleにおけるデータセンターとは何ですか? 1561

NetScaler ConsoleでサポートされているNetScalerアプライアンスにはどのようなものがありますか? 1561

インスタンスプロファイルとは何ですか? 1562

NetScaler Consoleで複数のNetScaler VPXインスタンスを再検出できますか? 1562

NetScaler Console は NetScaler SDX にインストールできますか? 1562

パブリックIPアドレスを使用して、NetScaler Console ソフトウェアにNetScalerインスタンスを追加できますか? 1562

DRノードの資格情報が変更された場合、ディザスタリカバリノードを登録する方法? 1563

StyleBook 1563

StyleBookを使用して、異なるバージョンのNetScalerソフトウェアで実行されている異なるNetScalerインスタンスを構成できますか? 1563

StyleBookを使用して複数のNetScalerインスタンスを同時に構成しているときに、1つのNetScalerインスタンスの構成が失敗した場合の動作? 1563

NetScalerを介して作成されたNetScalerバックアップにおけるStyleBook適用構成の有無 1563

システム管理 1564

NetScaler Consoleサーバーにホスト名を割り当てることができます? 1564

NetScaler Consoleの構成をバックアップおよび復元できます? 1564

NetScaler Consoleのしきい値とアラートとは何ですか? 1564

NetScaler Consoleのテクニカルサポートファイルを生成できますか? 1564

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

syslogパージとは何ですか? 1565

NetScaler ConsoleでNTPサーバーを設定できますか? 1565

NetScaler Consoleのアクティブ/パッシブHA展開はどのバージョンからサポートされていますか? 1565

NetScaler Consoleのアクティブ-アクティブHAセットアップがあり、統合GUIアクセス用にロードバランシング仮想サーバーを備えたNetScalerアプライアンスを構成していました。この構成を更新するにはどうすればよいですか? 1565

ポート443を使用したNetScalerインスタンス上でのNetScaler Console HAペアのロードバランシングの構成? 1566

NetScaler Consoleサーバーのバックアップファイルを使用した別のNetScaler Consoleサーバーの構成の復元? 1566

NetScaler ConsoleがNetScalerインスタンスをバックアップした後、そのバックアップファイルを使用して、NetScaler Consoleを介して別のNetScalerインスタンスの構成を復元できますか? 1566

NetScaler ConsoleサーバーのNSIPアドレスを使用する代わりに、SNIPアドレスを使用してNetScalerインスタンスと通信するようにNetScaler Consoleを強制できますか? 1566

NetScaler ConsoleでNetScalerインスタンスをバックアップする場合、結果はフルバックアップですか、それともベーシックバックアップですか? 1567

NetScaler Consoleのトラブルシューティングガイドはありますか? 1567

NetScaler Console HAフェイルオーバー発生時のNetScalerインスタンスの管理方法? 1567

ダウンしたNetScaler Console HAノードが復旧した場合の動作? 1567

NetScalerインスタンスはNetScaler Console HAノード間でどのように分散されますか?1567

NetScaler Console HAフェイルオーバーが発生した場合、仮想サーバーライセンスはどのように管理されますか? 1567

NetScaler Console HAセットアップにはロードバランサーが必須ですか? 1568

NetScaler Consoleは外部データベースをサポートしていますか? 1568

NetScaler Consoleによって管理されているNetScalerインスタンスを、NetScaler Console HAのロードバランサーとして使用できますか? 1568

NetScaler Console HAノード間でどのようなデータが同期されますか? 1568

**index** 1569

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

しきい値とアラートを作成する 1569
NetScaler Consoleを使用してしきい値とアラートを作成するには 1570
Logstream の概要 1570
Logstreamをトランスポートモードとして有効にする 1571
ダッシュボード 1572
アウトバウンドトラフィックダッシュボード 1573
ネットワークからのアウトバウンドトラフィックを表示する 1573
ユーザーダッシュボード 1573
ユーザーアクティビティインベスティゲーター 1574
ユーザー トランザクション 1574
リスクスコア 1575
すべての違反 1576
違反カテゴリ 1576
セキュリティ違反ダッシュボード 1578
違反の詳細 1578
アプリケーションの概要 1579
違反カテゴリ 1579
WAF違反の詳細を表示 1581
ボット違反の詳細を表示 1582
イベント履歴の表示 1583
NetScalerインスタンスのバックアップと復元 1583
インスタンスのバックアップ設定を構成する 1584
NetScaler Console を使用して、選択した NetScaler インスタンスのバックアップを作成する 1587
NetScaler Console を使用して NetScaler インスタンスを復元する 1587
NetScaler Console を使用して NetScaler SDX アプライアンスを復元する 1588
ネットワーク違反の詳細 1590
HTTP スローロリス 1590

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

DNS スローロリス 1590
HTTPスローポスト 1591
NXDOMAINフラッド攻撃 1591
HTTP Desync攻撃 1592
ブライヒェンバッハー攻撃 1593
セグメントスマック攻撃 1594
SYNフラッド攻撃 1594
スモールウィンドウ攻撃 1595
SSL インサイト 1595
前提条件 1596
SSL Insightの設定 1597
AppFlow機能の有効化 1597
SSL Insight パラメータを有効にする 1599
SSL Insight メトリックを表示する 1599
ユースケース: SSLトランザクションの概要を取得する 1600
ユースケース：クライアントのSSLメトリクス 1601
Web Insight の問題のトラブルシューティング 1601
データなしの診断 1601
Web Insight ダッシュボードレポートに関連する問題 1602
設定の問題 1602
NetScalerとNetScaler Console間の接続の問題 1602
NetScaler®からAppFlowデータが受信されない 1603
ライセンスの問題 1603
観測ポイントIDの問題 1603
不足しているAppFlowパラメーターの問題 1604
カウンターを使用したトラブルシューティング 1605
Webトランザクションの分析を表示 1605
詳細なWebトランザクション 1606

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

イベントの表示 1606
イベントリストに列を追加する 1608
高度な検索 1608
検索を保存 1610
データをエクスポート 1610
デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順 1611
ソフトウェア要件 1611
始める前に 1611
ソフトウェア要件 1612
始める前に 1612
NetScaler Console で静的ルートを構成する 1613
GitHub からサンプルデプロイメントファイルをダウンロードする 1614
CPX YAMLファイルにパラメータを追加する 1614
NetScaler ConsoleにVPX、SDX、MPX、またはBLXインスタンスを追加する 1616
NetScaler ConsoleにKubernetesクラスターを追加する 1616
サンプルマイクロサービスアプリケーションを展開する 1618
CPXを展開し、NetScaler ConsoleにCPXを登録する 1618
ライセンス供与のために仮想サーバーの自動選択を有効にする 1618
WebトランザクションとTCPトランザクションの設定を有効にする 1619
マイクロサービスにトラフィックを送信する 1619
サービスメッシュトポロジを設定するための詳細な手順 1619
NetScaler Consoleで静的ルートを構成する 1620
必要なパラメータを構成する 1621
サンプルアプリケーションの展開 1623
NetScaler ConsoleでKubernetesクラスターを追加する 1625
ライセンス供与のために仮想サーバーの自動選択を有効にする 1626
Web トランザクションと TCP トランザクションの設定を有効にする 1627
マイクロサービスにトラフィックを送信する 1627

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

シングルティアまたは統合イングレストポロジを設定するための詳細な手順 1628
NetScaler ConsoleでVPX、SDX、MPX、またはBLXインスタンスを追加する 1628
NetScaler ConsoleでKubernetesクラスターを追加する 1628
データガバナンス (NetScaler Console の 14.1-8.x から 14.1-21.x ビルド向け) 1630
データカテゴリ 1630
データガバナンス (NetScaler ADM 14.1-4.42 またはそれ以前のビルドの場合) 1630
カスタマーIDの構成 1631
ワークフロー1 - 新規ユーザーの場合 1631
ワークフロー2 - 最新のADMバージョンにアップグレードする既存ユーザーの場合 1632
診断およびデータ収集 1632
データが収集される理由? 1633
このデータを使用できるのは誰ですか? 1633
お客様のデータをどのくらいの期間保持しますか? 1633
メンテナンススクリプトを使用したデータベースの最適化 1634
顧客ユーザーエクスペリエンス向上プログラム 1634
CUXIPで収集される使用状況データとは? 1634
CUXIPはどのように役立ちますか? 1635
CUXIPの仕組み? 1635
ADMでCUXIPを無効にするにはどうすればよいですか? 1635
プライバシーポリシーの変更 1635
参照 1635
Cloud Connect 用のオプションのテレメトリデータ 1635
NetScaler® Telemetry プログラムのオプションのテレメトリデータ 1640
NetScaler Console の機能使用状況 1640
Cloud Connect に必要なテレメトリーデータ 1647
NetScaler® テレメトリプログラムに必要なテレメトリデータ 1652
ライセンス 1653
高可用性 1657

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

NetScaler Console高可用性ノード間でライセンスはどのように同期されますか? 1658
オーケストレーション 1658
仮想サーバーライセンスのアップグレード 1658
検証 1659
仮想サーバーの管理 1659
仮想サーバーの自動ライセンスを無効にする 1660
ライセンス供与のためにサードパーティの仮想サーバーを選択する 1660
仮想サーバーライセンスを手動で適用する 1660
ポリシーベースの仮想サーバーライセンスを構成する 1661
ライセンスされた仮想サーバーを表示する 1661
アドレス指定不可能な仮想サーバーの自動ライセンスサポートを構成する 1662
システム通知設定を構成する 1662
_fix_ 1665

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

# リリースノート

NetScaler Console 14.1 のリリースノートでは、新しい機能、既存の機能の強化、およびビルドにおける既知の問題について説明しています。14.1 リリースのリリースノートドキュメントには、以下のセクションが含まれています。

- **新機能**: ビルドでリリースされた新しい機能と既存機能の強化。
- **既知の問題**: ビルドに存在する問題、および該当する場合はその回避策。
- **修正された問題**: ビルドで対処された問題。

**注:**

これらのリリースノートには、セキュリティ関連の修正は記載されていません。セキュリティ関連の修正とアドバイザリのリストについては、セキュリティ速報を参照してください。NetScaler Console Security Advisory は、CVE の特定と修正をサポートしています。最新および既存のサポートされている CVE の詳細については、セキュリティアドバイザリによるサポート対象 CVE を参照してください。

リリース 14.1 の特定のビルドのリリースノートドキュメントを表示するには、以下の表の対応するリンクをクリックしてください。ビルドのリリースノートが更新されると、公開日も更新されます。リリースノートの公開日は、ビルドの GA 日と同じではない場合があります。

| NETSCALER CONSOLE オンプレミスソフトウェアバージョン 14.1 のリリースノート | 公開日 |
|---|---|
| ビルド 14.1-73.36 | Sep 01, 2026 |
| ビルド 14.1-72.57 | May 27, 2026 |
| ビルド 14.1-66.72 | Apr 24, 2026 |
| ビルド 14.1-60.57 | Jan 20, 2026 |
| ビルド 14.1-56.71 | Dec 05, 2025 |
| ビルド 14.1-51.83 | Dec 05, 2025 |

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

| NETSCALER CONSOLE オンプレミスソフトウェアバージョン 14.1 のリリースノート | 公開日 |
| --- | --- |
| ビルド 14.1-47.46 | Jul 02, 2025 |
| ビルド 14.1-43.50 | Feb 27, 2025 |
| ビルド 14.1-38.53 | Dec 18, 2024 |
| ビルド 14.1-34.43 | Oct 28, 2024 |
| 「ビルド 14.1-29.63」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=14.1&build=29.63) | Aug 19, 2024 |
| 「ビルド 14.1-25.56」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=14.1&build=25.56) | Jul 09, 2024 |
| 「ビルド 14.1-21.60」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=14.1&build=21.60) | Apr 28, 2024 |
| 「ビルド 14.1-17.38」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=14.1&build=17.38) | Mar 18, 2024 |
| 「ビルド 14.1-12.34」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=14.1&build=12.34) | Dec 19, 2023 |
| 「ビルド 14.1-8.50」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on- | Oct 10, 2023 |

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

| NETSCALER CONSOLE オンプレミスソフトウェアバージョン 14.1 のリリースノート | 公開日 |
| --- | --- |
| prem%2520%28ADM%29&version=14.1&build=8.50) | |
| 「ビルド 14.1-4.42」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=14.1&build=4.42) | Aug 07, 2023 |

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

# NetScaler Console on-prem を Citrix Cloud に移行する

**NetScaler ADM 13.0 64.35 以降のバージョン** を Citrix Cloud に移行できます。NetScaler ADM が 12.1 以前のバージョンの場合は、まず **13.0 64.35 以降のバージョン** にアップグレードしてから Citrix Cloud に移行する必要があります。詳細については、アップグレード セクションを参照してください。

**注:**

NetScaler® ADM サービスは、NetScaler Console サービスに名称変更されました。製品のUIとドキュメントは現在、これらの変更を反映するために更新中です。この間、古い名前と新しい名前が混在して参照される場合があります。この移行期間中のご理解に感謝いたします。

Citrix Cloud™ を介した NetScaler Console サービスにより、以下が可能になります。

- 約2週間ごとに最新の機能更新を含む、より迅速なリリース。
- アプリケーションセキュリティとボット、パフォーマンス、使用状況に関する機械学習ベースの分析。
- ピーク期間と閑散期間の分析、アプリケーションセキュリティとボットに関する機械学習ベースの分析、アプリケーションCPU分析など、現在 NetScaler Console サービスでのみサポートされているその他のさまざまな機能。

移行を成功させるには、以下を行う必要があります。

- Citrix Cloud にアクセスできるように、NetScaler Console on-prem でインターネット接続があることを確認する
- NetScaler エージェントを構成する
- Citrix Cloud からクライアントおよびシークレットCSVファイルを取得する
- NetScaler Console のライセンスを検証する
- スクリプトを使用して移行する

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

NetScaler Console on-prem から NetScaler Console サービスに移行した後、再度 NetScaler Console on-prem を継続したい場合は、ロールバックスクリプトを使用できます。詳細については、NetScaler Console on-prem へのロールバック を参照してください。

## NetScalerエージェントを構成する

NetScalerインスタンスとNetScaler Consoleサービス間の通信を有効にするには、エージェントを構成する必要があります。NetScalerエージェントは、デフォルトで最新ビルドに自動的にアップグレードされます。エージェントのアップグレードに特定の時間を選択することもできます。詳細については、「エージェントアップグレード設定の構成」を参照してください。

- 既存のNetScaler Consoleオンプレミス（スタンドアロンまたはHAペア）にエージェントが構成されていない場合、NetScaler Consoleサービス用に少なくとも1つのエージェントを構成する必要があります。
- 既存のNetScaler Consoleオンプレミス（スタンドアロンまたはHAペア）がマルチサイト展開用にオンプレミスエージェントで構成されている場合、NetScaler Consoleサービス用に同数のエージェントを構成する必要があります。

エージェントの構成の詳細については、「はじめに」セクションを参照してください。

## Citrix Cloudからクライアントおよびシークレット CSVファイルを取得する

エージェントを構成したら、Citrix Cloudページからクライアントおよびシークレット CSVファイルを取得します。

1. citrix.cloud.comにログオンします
2. **ホーム**アイコンをクリックし、**IDおよびアクセス管理**を選択します
3. **APIアクセス**タブから、安全なクライアント名を入力し、**クライアントの作成**をクリックします。
4. IDとシークレットが生成されます。**ダウンロード**をクリックし、CSVファイルをNetScaler Consoleオンプレミスに保存します。

   たとえば、CSVファイルを/varディレクトリに保存します。

## NetScaler Consoleサービスライセンスを検証する

NetScalerサービスにはライセンスを取得する必要があります。

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

- NetScaler ConsoleサービスのVIPライセンスは、オンプレミスのVIPライセンス以上である必要があります。

  **注**

  VIPライセンスが少ない場合、仮想サーバーがランダムに選択され、NetScaler Consoleサービスに対するVIPレベルの構成が失敗します。

- NetScaler Consoleオンプレミス展開をライセンスサーバーとして使用している場合、移行前にライセンスをNetScaler Consoleサービスに再割り当てしてください。詳細については、「ライセンスファイルの再割り当て方法」を参照してください。
- NetScaler Consoleオンプレミスでプールされたライセンスを使用している場合、NetScaler Consoleサービス用のプールされたライセンスを取得し、その後、NetScalerインスタンスにライセンスを割り当てる必要があります。詳細については、「プールライセンスの構成」を参照してください。NetScaler Consoleからライセンス割り当てを変更できるサポート対象のNetScalerバージョンは次のとおりです。
  - NetScaler SDX: 13.0 74.11 以降のバージョン。
  - NetScaler VPXおよびMPX: 13.0 47.24 以降のバージョン、12.1 58.14 以降のバージョン、および11.1 65.10 以降のバージョン。

# スクリプトを使用した移行

- NetScaler Console 82.xビルドを使用すると、機能を選択して移行できます。
- NetScaler Console 76.x以降のビルドの場合、移行スクリプト ( `servicemigrationtool.py` および `config_collect_onprem.py` ) はビルドの一部として提供されており、`cd /mps/scripts` で入手できます。
- NetScaler Console 76.xより前のビルドの場合、移行スクリプトをダウンロードし、NetScaler Consoleオンプレミスにスクリプトをコピーする必要があります。

  注

  移行中にNetScaler Consoleオンプレミスがインターネットに接続されていることを確認してください。

1. SSHクライアントを使用して、NetScaler Consoleオンプレミスにログオンします。

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

注

NetScaler Console HAペアの場合、プライマリノードにログオンします。

2. **shell** と入力し、**Enter** を押して bash モードに切り替えます。
3. クライアントIDとシークレットのCSVファイルをコピーします。たとえば、ファイルを/varディレクトリにコピーします。

   CSVファイルをコピーした後、CSVファイルが存在するかどうかを検証できます。

   注

   NetScaler Console HAペアの場合、プライマリノードにCSVファイルをコピーします。

4. NetScaler Consoleオンプレミス**13.0 82.xxバージョン**の場合、移行を完了するには次のコマンドを実行します。

   a. `cd /mps/scripts`

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

   たとえば、`python servicemigrationtool.py /var/secureclient.csv`

   移行スクリプトを実行すると、ツールは次のオプションを表示します。

   指定した選択に基づいて、その機能のみがNetScaler Consoleサービスに移行されます。

   この例では、オプション1が選択されています。ツールは管理および監視（M&M）の移行を完了し、次のメッセージを表示します。

   **管理および監視 (M&M)** 機能には、以下が含まれます:

   - NetScalerインスタンス、タグ、インスタンスグループ、プロファイル、カスタムアプリ、構成ジョブ、SNMP、syslog構成。
   - サイト、IPブロック、ネットワークレポート、分析しきい値、通知設定、データプルーニング設定。
   - 構成監査テンプレート、ポーリング間隔、イベントルールと設定。

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

- RBACグループ、ロール、およびポリシー

**Analytics** 機能には、以下が含まれます:

- NetScalerインスタンスからのvserverごとのAppflow構成。
- SDWANデバイスごとのAppflow®構成。

注:

- 管理および監視 (M&M) 機能は、他の機能 (2、3、または 4) を選択した場合でも自動的に移行されます。
- 一度に指定できる機能は1つだけです。
- いずれかの機能の移行が完了した後、後で他の機能を移行したい場合、既に移行された機能はリストに表示されません。たとえば、最初に **Analytics** 機能を移行した場合、次回移行スクリプトを実行するときには、**StyleBooks**、**Pooled Licensing**、および **All** オプションのみが表示されます。
- プールライセンスを移行すると、vserverを含むすべてのタイプが移行されます。

5. NetScaler Consoleオンプレミス **13.0 76.xxバージョン** の場合、移行を完了するには次のコマンドを実行します:

   a. `cd /mps/scripts`

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

   例えば、`python servicemigrationtool.py /var/secureclient.csv`

6. NetScaler Console on-prem 13.0 76.xx バージョン以前の場合:

   a. 以下の場所から移行スクリプトをダウンロードします: `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

   ダウンロードしたファイルには、2つのバンドルスクリプト `servicemigrationtool_27.py` と `config_collect_onprem_27.py` が含まれています。

   b. 2つのスクリプトをNetScaler Console on-premに保存します。例えば、/var ディレクトリに保存します。

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

c. 移行するには、以下のコマンドを実行します:

i. `cd /var`

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

例えば、`python servicemigrationtool_27.py /var/secureclient.csv`

スクリプトを実行すると、前提条件がチェックされ、移行が続行されます。スクリプトはまずライセンスの利用可能性を確認します。オンプレミスライセンスよりもNetScaler Consoleサービスライセンスが少ない場合にのみ、以下のメッセージが表示されます。

**Y** を選択すると、VIPをランダムにライセンス付与して移行が続行されます。**N** を選択すると、スクリプトは移行を停止します。

プールされたライセンスサーバーに対してサポートされていないNetScalerインスタンスバージョンを使用している場合、以下のメッセージが表示されます:

**Y**を選択すると、ライセンスサーバーを変更して移行プロセスが続行されます。**N**を選択すると、スクリプトは残りの移行を続行するかどうかを尋ねます。**N**を選択すると、スクリプトは移行を停止します。

オンプレミス構成によっては、移行が完了するまで数分から数時間かかる場合があります。移行が完了すると、次のメッセージが表示されます。

すべてのNetScalerインスタンスとそのそれぞれの構成がNetScaler Consoleサービスに正常に移行されると、移行は成功です。移行が成功すると、オンプレミスのNetScaler Consoleは次のインスタンスイベントの処理を停止します。

- SSL証明書
- Syslogメッセージ
- バックアップ
- エージェントクラスター
- パフォーマンスレポート
- 構成監査
- `Emon`スケジューラ

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

# NetScaler Consoleオンプレミスへのロールバック

NetScaler Consoleオンプレミスにロールバックする場合は、前提条件が満たされていることを確認してください。

## 前提条件

NetScaler Consoleオンプレミス（NetScaler Consoleサービスへの移行前）が次の場合は、:

- プールライセンスサーバーとして使用する場合、NetScaler Console on-premに必要なプールライセンスがあることを確認してください。
- NetScalerエージェントで構成されている場合、エージェントが「UP」ステータスで利用可能であることを確認してください。

## ロールバックスクリプトを使用する

注

> ロールバック後、Analytics、SNMP、プールライセンスにおける同じ構成（移行前）がNetScaler Console on-premで再び利用可能になります。移行後にこれらの構成に変更を加えた場合、これらの変更はNetScaler Console on-premには反映されません。

- **NetScaler Console 82.xx以降**のビルドの場合、ロールバックスクリプトはビルドの一部として利用可能で、`/mps/scripts`でアクセスできます。
- **NetScaler Console 79.xxより前の**ビルドの場合、82.xビルドにアップグレードしてロールバックスクリプトを使用するか、ロールバックスクリプトをダウンロードしてNetScaler Console on-premにスクリプトをコピーすることができます。

1. SSHクライアントを使用して、NetScaler Console on-premにログオンします。
2. 「shell」と入力し、Enterキーを押してbashモードに切り替えます。
3. NetScaler Console **13.0 82.xx**ビルドの場合、ロールバックを完了するには次のコマンドを実行します。

   a. cd /mps/scripts

   b. python rollback_to_onprem.py `<path of ClientID/Secret File in NetScaler Console on-prem VM>` を実行します。

   例: `python rollback_to_onprem.py /var/ secureclient.csv.csv`

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

ツールがロールバック操作を開始し、続行するかどうかを尋ねるプロンプトが表示されます。続行するには「**Y**」と入力します。

ロールバックが完了すると、次のメッセージが表示されます。

ロールバック完了(/en-us/netscaler-application-delivery-management-software/media/rollback-complete.png)

4. 82.xxビルドより前のNetScaler Consoleの場合：

   a. 次の場所からロールバックスクリプトをダウンロードします。

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

   b. NetScaler Console 79.xxおよび76.xxビルドの場合、スクリプトを`/mps/scripts`に保存し、次のコマンドを実行してロールバックします。

      i. `cd /mps/scripts`

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

      例：`python rollback_to_onprem.py /var/ secureclient.csv`

   c. 76.xxビルドより前のNetScaler Consoleの場合、スクリプトをNetScaler Consoleオンプレミスに保存します。たとえば、`/var`の場所に保存し、次のコマンドを実行してロールバックします。

      i. `cd /var`

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

      例：`python rollback_to_onprem_27.py /var/secureclient.csv`

   ツールはロールバック操作を開始し、続行するかどうかを尋ねるプロンプトが表示されます。続行するには「**Y**」と入力します。

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

# よくある質問

## NetScaler Consoleサービス

### NetScaler agentは、オンプレミスのNetScaler agentと同様にオプションですか?

いいえ。NetScaler Consoleサービスではエージェントが必須であり、インスタンスとNetScaler Consoleサービス間のすべての通信はエージェントを介して行われます。オンプレミスのNetScaler Consoleではエージェントはオプションですが、帯域幅の消費を抑えるためだけにエージェントを構成できます。

### NetScaler Consoleサービスを使用する理由?

Citrix Cloudを介したNetScaler Consoleサービスは、新しい定期的なビルドを必要とせずに、以下の利点を提供します。

- オンプレミスのNetScaler Consoleよりも簡単なオンボーディングと低い総所有コストを実現するクラウドベースのSaaSサービス。
- 約2週間ごとに最新の機能更新を含む、より迅速なリリース。
- アプリケーションのセキュリティ、パフォーマンス、使用状況に関する機械学習ベースの分析。
- ピーク期間と閑散期間の分析、WAFとボット向けの機械学習ベースのアプリケーションセキュリティ分析、アプリケーションCPU分析など、現在NetScaler Consoleサービスでのみサポートされているその他のさまざまな機能。

### オンプレミスのNetScaler ConsoleがHAペアの場合、移行後にどうなりますか?

すべての構成はCitrix Cloudに移行されます。ディザスタリカバリノードの構成は不要です。

### 何らかの理由でエージェントがダウンした場合、どうなりますか?

エージェントが稼働するまで、潜在的なデータ損失が発生する可能性があります。ただし、エージェントのフェールオーバーが発生した場合に継続性を確保するために、マルチサイト展開用にNetScalerエージェントを構成することもできます。詳細については、「マルチサイト展開用にエージェントを構成する」を参照してください。

### インスタンスのバックアップも移行されますか?

バックアップは移行に含まれません。

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

### 履歴データも移行されますか?

履歴データは移行されません。データはオンプレミスのNetScaler Consoleからエクスポートできます。

### オンプレミスライセンスも移行されますか?

いいえ。オンプレミスライセンスファイルはNetScaler Consoleサービスでは使用できません。NetScaler Consoleサービス用のライセンスを取得する必要があります。詳細については、ライセンスを参照してください。オンプレミスのNetScaler Consoleでプールライセンスを使用している場合は、NetScaler Consoleサービス用のプールライセンスを取得し、インスタンスにライセンスを割り当てる必要があります。

### オンプレミスのNetScaler Consoleから移行されないものは何ですか?

以下の機能はNetScaler Consoleサービスに移行できません。

- **RBAC** – NetScaler Consoleサービスでは、ユーザーアクセスは管理者からの招待に基づいています。NetScaler Consoleサービスユーザーは Citrix Cloudにアカウントを持っている必要があります。そのため、オンプレミスのNetScaler Consoleユーザーは移行されません。
- **エクスポートスケジュール** – エクスポートスケジュールには、ドリルダウンやさまざまなページからのスケジュールなどの詳細が含まれます。これらの詳細なエクスポートスケジュールはすべて移行されません。
- **SSL証明書/キー/CSR** – NetScaler Consoleサービスは、NetScaler SSL証明書/キー/CSRのみを表示できます。そのため、オンプレミスのNetScaler Consoleにアップロードされた SSL証明書/キーはNetScaler Consoleサービスに移行されません。

### オンプレミスのNetScaler ConsoleはCitrix Directorと統合されています。この統合はどうなりますか?

NetScaler ConsoleとDirectorの統合は、現在、オンプレミスのNetScaler Consoleでのみサポートされています。

### 移行後のインスタンスのライセンス取得とアナリティクス有効化について?

NetScaler Consoleサービスのライセンスが、オンプレミスのVIPライセンス以上であることを確認する必要があります。ライセンスがすでにオンプレミスのNetScaler Console VIPよりも多い場合、仮想サーバーは自動的にライセンスされます。そうでない場合、ライセンスはランダムに割り当てられます。

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

# 移行ツール

### マイグレーションスクリプト実行後のエラーメッセージ表示とその原因?

失敗理由が記載されたログファイルが表示されます。適切な是正措置を講じて、マイグレーションスクリプトを再度実行できます。一般に、マイグレーションスクリプトを実行する前に、以下を確認してください。

- NetScaler® エージェントを構成する
- NetScaler Console サービスライセンスを取得する
- クライアントとセキュアなCSVファイルを保存した正しいパスをコピーする

### NetScalerインスタンスのバージョンが、プールライセンスの制限よりも低い場合、ライセンスサーバーを変更するために「Y」オプションを選択するとどうなりますか?

ライセンスサーバーの変更は、サポートされているNetScaler MPX、VPX、およびSDXバージョンでのみ行われます。

### マイグレーションスクリプトがNetScalerインスタンスに関する構成に失敗した場合、どうなりますか?

NetScalerインスタンスは、NetScaler Consoleオンプレミスセットアップで引き続き動作します。提示された失敗理由から必要な措置を講じ、マイグレーションスクリプトを再度実行できます。

### NetScalerインスタンスの一部がNetScaler Consoleサービスへの移行に失敗した場合の対応と、マイグレーションスクリプトの再実行による解決策?

はい。スクリプトを再実行すると、失敗したインスタンスのみが移行されます。たとえば、5つのインスタンスのうち2つが移動に失敗したとします。是正措置を講じてマイグレーションスクリプトを再実行すると、以前に正常に移動された3つのインスタンスには「Device already exists」というメッセージが表示されます。そして、以前に失敗した他の2つのインスタンスは正常に移行されます。

### マイグレーションステータスを確認するためのログファイルについて?

はい、`/var/mps/log/` ディレクトリにログファイルが生成されます。python3.7 を使用する NetScaler Console のログファイルは `servicemigrationtool.py.log` であり、python 2.7 を使用する NetScaler Console のログファイルは `servicemigrationtool_27.py.log` です。

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

### マイグレーションスクリプトの実行中にセッションが終了した場合、どうなりますか?

マイグレーションスクリプトを再実行できます。新しいセッションでは、前回のセッションで既に追加されたインスタンスは「Device already exists」と表示され、マイグレーションはさらに続行されます。

### NetScaler ConsoleサービスがオンプレミスのNetScaler Consoleよりも少ないライセンスしか持たず、移行スクリプトが開始された場合、どうなりますか?

移行スクリプトの実行後、ライセンスが少ないことに関する提案が表示され、続行するか停止するかを促されます。少ないライセンスで続行する場合、仮想サーバーは利用可能なライセンスからランダムにライセンス付与されます。

### オンプレミスのNetScaler ConsoleがNetScaler ConsoleサービスExpressアカウントに移行された場合、どうなります?

NetScaler ConsoleサービスExpressアカウントには、仮想サーバーライセンスが2つ、StyleBook構成パックが2つ、構成ジョブが2つしかありません。オンプレミスのNetScaler Consoleがこれらの構成よりも多く、Expressアカウントで移行を開始した場合、スクリプトはExpressアカウントに適用可能な前述の構成（仮想サーバーライセンス2つ、StyleBook構成パック2つ、構成ジョブ2つ）のみを移行できます。

### Citrix Cloudの招待ユーザー（Citrix Cloudアカウントを作成した管理者ユーザー以外）がNetScaler Consoleオンプレミス設定の移行を試みた場合、どうなります?

移行スクリプトは管理者が実行することをお勧めします。招待ユーザーには管理者権限（adminExceptSystem_group）がありません。その結果、グループ、ロール、ポリシーの移行が失敗し、「User doesn’t have permission」というメッセージが表示されます。

解決策として、管理者（Citrix Cloudアカウントを作成したユーザー）は、招待ユーザーに関連付けられているグループを「admin_group」に変更できます。

## ロールバックスクリプト

### NetScaler ConsoleオンプレミスHAペアでロールバックスクリプトが使用された場合、どうなりますか?

NetScaler ConsoleオンプレミスHAペアは、移行前に利用可能だったすべての構成で復元されます。

### ロールバックスクリプトの使用後、ディザスタリカバリノードはどうなりますか?

ディザスタリカバリノードも、移行前のすべての構成で復元されます。

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

# トラブルシューティング

移行スクリプトを初めて実行すると、前提条件がチェックされ、移行が開始されます。すべての前提条件が満たされている場合、移行はエラーなしで完了します。いずれかの前提条件が満たされていない場合、スクリプトは理由とともにエラーメッセージを表示します。エラーを修正した後、スクリプトを再度実行する必要があります。

注

「すでに存在します」というエラーメッセージが表示された場合、それは次のことを意味します。

- 移行スクリプトを複数回実行した可能性があり、一部の構成はすでにNetScaler Consoleサービスに移行されています。
- 移行スクリプトを実行する前に、NetScaler Consoleサービスで同じ構成を手動で作成した可能性があります。

次のいくつかのエラーメッセージを参照してください。

## NetScaler Consoleサービスに追加された手動プロファイル

**回避策**: 移行スクリプトを実行する前にNetScaler Consoleサービスで管理者プロファイルを作成した場合は、それらのプロファイルを削除し、移行スクリプトを再実行してください。

## NetScaler Consoleサービスに追加されたNetScalerデバイス

**回避策**: NetScaler Consoleで、インスタンスのステータスを確認し、問題なくインスタンスにアクセスできるか確認してください。問題が解決しない場合は、問題を修正し、移行スクリプトを再実行してください。

## NetScaler ConsoleサービスへのStyleBookカスタムテンプレートのインポート

**回避策**: このエラーメッセージは、すでに移行されたStyleBookの例です。移行スクリプトを実行する前に、NetScaler Consoleサービスで同じ名前、バージョン、名前空間を持つStyleBookを手動で作成した場合にも、このエラーが表示されることがあります。

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

## NetScaler Consoleサービスに追加された構成ジョブ

- [ ]

**回避策**: このエラーは、Expressアカウントを購読しており、2つ以上の構成ジョブがある場合に発生します。すべての構成ジョブを移行するには、有効なサブスクリプションを取得する必要があります。

## NetScaler Consoleサービスに追加されたIPブロック

- [ ]

**回避策**: NetScaler Consoleサービスで手動で作成されたIPブロックを削除し、移行スクリプトを再実行します。

## ネットワークダッシュボードレポートの追加ステータス

- [ ]

**回避策**: NetScaler Consoleサービスで手動で作成されたダッシュボードを削除し、移行スクリプトを再実行します。

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

# すべてのハウツー記事

NetScaler Application Delivery Management (NetScaler Console) の「ハウツー記事」は、NetScaler Console の機能に関する、シンプルで関連性が高く、実装が容易な記事です。これらの記事には、インスタンス管理、アプリケーション管理、StyleBooks、証明書管理、分析など、NetScaler Console の人気機能に関する情報が含まれています。

以下の表で機能名をクリックして、その機能のハウツー記事のリストを表示します。

| トピック | | | | |
|---|---|---|---|---|
| インスタンス管理 | イベント管理 | StyleBooks | 証明書管理 | NetScaler Console システム |
| | 構成管理 | 認証 | 分析 | ネットワーク機能 |

## インスタンス管理

グローバルに分散されたサイトを監視する方法

NetScalerインスタンスの管理パーティションを管理する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/manage-admin-partitions.html)

NetScaler Consoleにインスタンスを追加する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/configure/add-instances.html)

NetScaler Consoleでインスタンスグループを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/create-instance-groups.html)

NetScaler ConsoleでGeoマップのサイトを設定する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/configure-sites-geomaps.html)

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

NetScaler Consoleを使用して、セカンダリNetScalerインスタンスへのフェイルオーバーを強制する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/force-failover-secondary-netscaler-instance.html)

NetScaler Consoleを使用して、セカンダリNetScalerインスタンスをセカンダリのままにする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/force-secondary-to-stay-secondary.html)

NetScaler Consoleを使用してインスタンスをバックアップおよび復元する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/backup-restore-netscaler-instances.html)

複数のNetScaler VPXインスタンスを再検出する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/rediscover-multiple-vpx-instances.html)

NetScaler ConsoleでNetScalerインスタンスとエンティティをポーリングする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/overview/how-mas-communicates-with-managed-instances.html)

NetScaler Consoleでインスタンスの管理を解除する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/unmanage-instance.html)

NetScaler Consoleからインスタンスへのルートをトレースする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/trace-route-instance.html)

# 構成管理

NetScaler Consoleで構成ジョブを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-create.html)

構成ジョブでSCP (put) コマンドを使用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-use-scp-put-command.html)

NetScaler Consoleの組み込みテンプレートを使用して作成されたジョブをスケジュールする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-schedule-jobs-created-using-built-in-templates.html)

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

NetScaler Consoleで組み込みテンプレートを使用して構成されたジョブを再スケジュールする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reschedule-jobs.html)

実行済みの構成ジョブを再利用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reuse-executed-configuration-jobs.html)

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-upgrade-netscaler-instances.html)

NetScaler Consoleの構成ジョブで変数を使用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-use-variables.html)

NetScaler Consoleで構成テンプレートを使用して監査テンプレートを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/use-configuration-templates-to-create-audit-templates.html)

NetScaler Consoleで修正コマンドから構成ジョブを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-create-jobs-from-corrective-commands.html)

NetScaler Consoleで実行中および保存済みの構成コマンドをあるNetScalerインスタンスから別のインスタンスにレプリケートする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/replicate-running-saved-configuration-from-one-netscaler-to-another.html)

レコード・アンド・プレイを使用して構成ジョブを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/record-and-play.html)

構成ジョブを使用して、あるインスタンスから複数のインスタンスに構成をレプリケートする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/replicate-configuration.html)

NetScaler Consoleでマスター構成テンプレートを使用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/use-master-configuration-template.html)

NetScalerインスタンスの構成監査をポーリングする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/how-to-poll-configuration-audit-of-netscaler-instances.html)

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

構成ジョブで構成監査テンプレートを再利用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reuse-configuration-audit-templates.html)

構成テンプレートをインポートおよびエクスポートする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-import-and-export-configuration-templates.html)

ConfigChange SNMPトラップの構成監査差分を生成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/generate-configuration-audit-diff-for-configchange-snmp-traps.html)

## 証明書管理

NetScaler Consoleでエンタープライズポリシーを設定する方法

NetScaler ConsoleからNetScalerインスタンスにSSL証明書をインストールする方法

NetScaler Consoleからインストール済みの証明書を更新する方法

NetScaler Consoleを使用してSSL証明書をリンクおよびリンク解除する方法

NetScaler Consoleを使用して証明書署名要求 (CSR) を作成する方法

NetScaler ConsoleからSSL証明書の有効期限切れに関する通知を設定する方法

NetScaler ConsoleでSSLダッシュボードを使用する方法

NetScalerインスタンスからSSL証明書をポーリングする方法

## StyleBooks

StyleBooksのさまざまなグループを表示する方法

独自のStyleBooksを作成する方法

NetScaler Consoleでユーザー定義のStyleBooksを使用する方法

StyleBooksから構成を作成するためにAPIを使用する方法

StyleBookで定義されている仮想サーバーで分析を有効にし、アラームを設定する方法

NetScaler Consoleにファイルをアップロードするための StyleBookを作成する方法

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

APIを使用して任意のファイルタイプをアップロードする構成を作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/how-to-use-api-to-create-configurations-to-upload-any-file-type.html)

SSL証明書と証明書キーファイルをNetScaler Consoleにアップロードするstylebookを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks/how-to-create-stylebook-to-upload-ssl-certificate-and-key-files.html)

APIを使用して証明書とキーファイルをアップロードする構成を作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/how-to-use-api.html)

企業でMicrosoft Skype for Business StyleBookを使用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/business-application-stylebooks/microsoft-skype-business-stylebook.html)

企業でMicrosoft Exchange StyleBookを使用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/business-application-stylebooks/microsoft-exchange-stylebook.html)

企業でMicrosoft SharePoint StyleBookを使用する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/business-application-stylebooks/microsoft-sharepoint-stylebook.html)

# アナリティクス

インスタンスでアナリティクスを有効にする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/configure/enable-analytics-on-virtual-servers.html)

適応型しきい値を構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/analytics-how-to-articles/how-to-configure-adaptive-thresholds.html)

SLA管理を構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/analytics-how-to-articles/how-to-configure-sla-management.html)

アナリティクス用のデータベース集計を構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/analytics-how-to-articles/how-to-configure-database-summarization.html)

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

NetScaler Consoleを使用してしきい値とアラートを作成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/analytics-how-to-articles/how-to-create-thresholds-and-alerts-using-mas.html)

NetScaler ConsoleからアナリティクスのURLデータ収集を無効にする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/analytics-how-to-articles/how-to-disable-url-data-collection-for-analytics-mas.html)

## イベント管理

NetScaler Consoleでイベントのイベント期間を設定する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/events/how-to-set-event-age.html)

NetScaler Console を使用してイベントフィルターをスケジュールする方法

NetScaler Console からのイベントに対して繰り返しメール通知を設定する方法

NetScaler Console を使用してイベントを抑制する方法

イベントを監視するためにイベントダッシュボードを使用する方法

NetScaler Console でイベントルールを作成する方法

NetScaler インスタンスで発生するイベントの報告された重大度を変更する方法

NetScaler Console でイベントの概要を表示する方法

NetScaler Console で SNMP トラップのイベントの重大度とスキューを表示する方法

NetScaler Console を使用して syslog メッセージをエクスポートする方法

NetScaler Console で syslog メッセージを抑制する方法

インスタンスイベントのプルーン設定を構成する方法

## 認証

外部認証サーバーのフォールバックとカスケードを有効にする方法

RADIUS 認証サーバーを追加する方法

LDAP 認証サーバーを追加する方法

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

TACACS認証サーバーを追加する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/add-tacacs-authentication-server.html)

NetScaler Consoleで認証サーバーグループを抽出する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/extract-authentication-server-group.html)

フォールバックローカル認証を有効にする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/enable-fallback-local-authentication.html)

## NetScaler Consoleシステム

NetScaler Consoleをアップグレードする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-upgrade-netscaler-mas.html)

NetScaler Consoleのパスワードをリセットする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-reset-password.html)

NetScaler Consoleのテクニカルサポートファイルを生成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-generate-tech-support-file-for-mas.html)

シングルサーバー展開でNetScaler Consoleサーバーをバックアップおよび復元する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-backup-and-restore-configuration-on-mas.html)

HAペアでNetScaler Console構成をバックアップおよび復元する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-backup-and-restore-mas-configuration-in-ha-pair0.html)

NetScaler Consoleで非デフォルトユーザーのシェルアクセスを有効にする方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-enable-shell-access-for-non-default-users-mas.html)

NetScaler ConsoleでNTPサーバーを構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-configure-ntp-server-on-mas.html)

NetScaler ConsoleのSSL設定を構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-configure-ssl-settings-for-mas.html)

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

NetScaler Consoleのsyslogパージ間隔を構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-configure-syslog-purging-interval.html)

NetScaler Consoleの監査情報を表示する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-view-auditing-information-of-mas.html)

NetScaler Consoleのシステム通知設定を構成する方法(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-configure-system-settings-of-mas.html)

NetScaler Console の CPU、メモリ、ディスク使用量を監視する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-monitor-cpu-memory-disk-usage-of-mas.html)

NetScaler Console の暗号グループを構成する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-configure-cipher-group-for-mas.html)

NetScaler Console で SNMP トラップ、マネージャー、ユーザーを作成する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-create-snmp-traps-managers-users-mas.html)

NetScaler Console サーバーにホスト名を割り当てる方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-assign-host-name-to-mas-server.html)

NetScaler Console のシステムプルーニング設定を構成する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-system-prune-settings-mas.html)

NetScaler Console を使用してシステムバックアップ設定を構成する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-system-backup-settings.html)

NetScaler Console でシステムアラームを構成および表示する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-view-system-alarms-mas.html)

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

# ネットワーク機能

負荷分散エンティティのレポートを生成する方法](/ja-jp/netscaler-application-delivery-management-software/current-release/networks/network-functions/how-to-generate-reports-for-load-balancing-entities.html)

ネットワーク機能レポートをエクスポートまたはエクスポートをスケジュールする方法](/ja-jp/netscaler-application-delivery-management-software/current-release/networks/network-functions/export-or-schedule-export-of-reports.html)

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

# 概要

**注:**

14.1-17.xビルド以降、NetScaler ADMはNetScaler Consoleにブランド変更されました。それ以前のビルドでは、製品名はNetScaler ADMです。

NetScaler Consoleは、管理者に対しエンタープライズ全体の可視性を提供し、複数のインスタンスで実行する必要がある管理ジョブを自動化することで、運用を簡素化する集中管理ソリューションです。NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler CPX、NetScaler Gatewayを含むNetScaler製品を管理および監視できます。NetScaler Consoleを使用すると、単一の統合コンソールからグローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。

NetScaler Consoleは、Citrix Hypervisor、VMware ESXi、およびLinux KVM上で動作する仮想アプライアンスです。NetScaler Consoleは、Webアプリケーションおよび仮想デスクトップトラフィックに関する以下の詳細情報を収集することで、アプリケーションの可視性に関する課題に対処します。

- ユーザーセッションレベルの情報
- Webページのパフォーマンスデータ
- サイトのNetScalerインスタンスを介して流れるデータベース情報、および実用的なレポートを提供します。

NetScaler Consoleを使用すると、IT管理者は顧客の問題を数分でトラブルシューティングし、プロアクティブに監視できます。

## 機能とソリューション

NetScaler Consoleは、以下の機能を提供します。

### アプリケーション分析と管理

アプリケーションパフォーマンス分析

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

App Scoreは、アプリケーションのパフォーマンスがどの程度良好であるかを定義するスコアリングシステムの結果です。応答性、脅威に対する脆弱性の有無、すべてのシステムが稼働しているかどうかなど、アプリケーションのパフォーマンスが良好であるかを示します。

### アプリケーションセキュリティ分析

App Security Dashboardは、アプリケーションのセキュリティ状態を包括的に表示します。例えば、セキュリティ違反、シグネチャ違反、脅威インデックスなどの主要なセキュリティメトリックを表示します。App Security Dashboardはまた、検出されたNetScalerインスタンスに対するSYN攻撃、スモールウィンドウ攻撃、DNSフラッド攻撃などの攻撃関連情報も表示します。

## ネットワーク

### インスタンス

NetScalerおよびNetScaler Gatewayインスタンスを管理できます。

### インスタンスグループ

インスタンスを次のようにグループ化できます。

- 静的グループ: 設定ジョブなどのさまざまなタスクで使用できるデバイスグループを定義できます。
- プライベートIPブロック: 地理的な場所に基づいてインスタンスをグループ化できます。

### イベント管理

NetScalerインスタンスのIPアドレスがNetScaler Consoleに追加されると、NetScaler ConsoleによってNITROコールが送信され、インスタンスがトラップまたはイベントを受信するためのトラップ宛先として暗黙的に自身を追加します。

イベントは、管理対象のNetScalerインスタンスで発生するイベントまたはエラーを表します。

### 証明書管理

NetScaler Consoleは、証明書管理のあらゆる側面を効率化します。単一のコンソールを通じて、適切な発行者、鍵強度、正しいアルゴリズムを保証するための自動ポリシーを確立できるほか、未使用または間もなく期限切れになる証明書を厳密に監視できます。NetScaler Console SSLダッシュボードとその機能の使用を開始するには、SSL証明書とは何か、およびNetScaler Consoleを使用してSSL証明書を追跡する方法を理解する必要があります。

### 構成管理

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

NetScaler Consoleを使用すると、エンティティの作成、機能の構成、構成変更のレプリケーション、システムアップグレード、その他のメンテナンスアクティビティなど、複数のインスタンスで構成タスクを簡単に実行できる構成ジョブを作成できます。構成ジョブとテンプレートにより、最も反復的な管理タスクがNetScaler Console上の単一のタスクに簡素化されます。

### 構成監査

インスタンス全体の構成における異常を監視および特定できます。

- 構成アドバイス: 構成の異常を特定できます。
- 監査テンプレート: 特定の構成全体の変更を監視できます。

### ネットワークレポート

NetScaler Consoleでネットワークレポートを監視することで、リソース使用率を最適化できます。

## オーケストレーション

### クラウドオーケストレーション

NetScaler製品とOpenStackクラウドオーケストレーションの統合を可能にします。NetScaler ConsoleとOpenStackは相互のAPIを実装し、NetScalerインスタンスの負荷分散機能 (LBaaS) とOpenStackクラウドオーケストレーションの統合を可能にします。

オーケストレーション(/ja-jp/netscaler-application-delivery-management-software/current-release/orchestration.html)

NetScaler Console は、さまざまなベンダーの SDN コントローラーと統合することで、企業ネットワークにおける SDN をサポートします。NetScaler Console は、VMware NSX Manager と Cisco Application Policy Infrastructure Controller (APIC) の両方をサポートします。

# アーキテクチャ

NetScaler Consoleデータベースはサーバーと統合されており、サーバーはデータ収集、NITRO コールなどのすべての主要プロセスを管理します。データストアには、ホスト名、ソフトウェアバージョン、実行中および保存済みの構成、証明書の詳細、インスタンスに構成されたエンティティなど、インスタンスの詳細のインベントリがサーバーによって保存されます。少量のトラフィックを処理したり、データを限られた期間保存したりする場合は、単一サーバー展開が適しています。

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

現在、NetScaler Consoleは2種類のソフトウェア展開（単一サーバーと高可用性）をサポートしています。

次の図は、NetScaler Console内のさまざまなサブシステムと、NetScaler Consoleサーバーと管理対象インスタンス間の通信がどのように行われるかを示しています。



NetScaler Consoleのサービスサブシステムは、ポート80および443を使用して、GUIまたはAPIからNetScaler Console内のサブシステムに送信されるHTTPリクエストとレスポンスを処理するWebサーバーとして機能します。これらのリクエストは、IPC（プロセス間通信）メカニズムを使用して、メッセージバス（メッセージ処理システム）を介してサブシステムに送信されます。リクエストは制御サブシステムに送信され、制御サブシステムは情報を処理するか、適切なサブシステムに送信します。その他の各サブシステム（インベントリ、StyleBooks、データコレクター、構成、AppFlowデコーダー、AppFlow Analytics、パフォーマンス、イベント、エンティティ、SLAマネージャー、プロビジョナー、ジャーナル）には、特定の役割があります。

インスタンスプラグインは、NetScaler Consoleでサポートされている各インスタンスタイプに固有の共有ライブラリです。情報は、NITROコールを使用するか、SNMP、Secure Shell（SSH）、またはSecure Copy（SCP）プロトコルを介して、NetScaler Consoleと管理対象インスタンス間で転送されます。この情報はその後、内部データベース（データストア）で処理および保存されます。

## NetScaler Consoleがインスタンスを検出する方法

インスタンスとは、NetScaler Consoleから検出、管理、監視したいNetScalerアプライアンスまたは仮想アプライアンスのことです。これらのインスタンスを管理および監視するには、NetScaler Consoleサーバーに追加する必要があります。NetScaler Consoleには、次のNetScalerアプライアンスおよび仮想アプライアンスを追加できます。

- NetScalerインスタンス
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- NetScaler Gatewayインスタンス

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

インスタンスは、NetScaler Consoleサーバーを初めてセットアップするとき、または後で追加できます。

**注**

NetScaler Consoleは、通信にNetScalerインスタンスのNetScaler IP (NSIP) アドレスを使用します。NetScaler Consoleは、管理アクセスが有効になっているサブネットIP (SNIP) アドレスを持つNetScalerインスタンスも検出できます。NetScalerインスタンスとNetScaler Consoleの間で開いている必要があるポートについては、「ポート」を参照してください。

SNIPを使用してNetScaler HAペアを追加する場合は、NetScaler HAペアで独立ネットワーク構成 (INC) モードを有効にしてください。インスタンスの追加の詳細については、「インスタンスの追加」を参照してください。
NetScaler Consoleにインスタンスを追加すると、サーバーは暗黙的に自身をインスタンスのトラップ宛先として追加し、インスタンスのインベントリを収集します。

次の図は、NetScaler Consoleがインスタンスを暗黙的に検出し、追加する方法を示しています。

NetScaler ConsoleがNetScalerインスタンスを検出する様子(/en-us/netscaler-application-delivery-management-software/media/instancediscovery-console.png)

図に示すように、次の手順はNetScaler Consoleによって暗黙的に実行されます。

1. NetScaler Consoleは、インスタンスプロファイルの詳細を使用してインスタンスにログオンします。NetScaler Consoleは、NetScaler NITROコールを使用して、インスタンスのライセンス情報を取得します。ライセンス情報に基づいて、インスタンスがNetScalerインスタンスであるかどうか、およびNetScalerプラットフォームのタイプ（NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX、またはNetScaler Gatewayなど）を判別します。インスタンスの検出に成功すると、NetScaler Consoleデータベースに追加されます。

   インスタンスプロファイルに正しい資格情報が含まれていない場合、この手順は失敗する可能性があります。NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX、およびNetScaler Gatewayインスタンスの場合、ライセンスがインスタンスに適用されていない場合も、この手順は失敗する可能性があります。

   **注**

   HTTPを使用すると、ライセンスがインスタンスに構成されていなくても、すべてのインスタンスをNetScaler Consoleに追加できます。

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

2. NetScaler Consoleは、そのIPアドレスをインスタンス上のトラップ宛先リストに追加します。これにより、NetScaler ConsoleはNetScalerインスタンスで生成されたトラップを受信できます。

   インスタンス上のトラップ宛先の数がトラップ宛先の最大制限を超えると、この手順は失敗する可能性があります。インスタンスの最大制限は20です。

3. NetScaler Consoleは、NITROリクエストを送信してインスタンスからインベントリを収集します。ホスト名、ソフトウェアバージョン、実行中および保存済みの構成、証明書の詳細、インスタンスに構成されているエンティティなどのインスタンスの詳細を収集します。

   この手順は、ネットワークまたはファイアウォールの問題が原因で失敗する可能性があります。

   NetScaler Consoleにインスタンスを追加する方法については、「インスタンスの追加」を参照してください。

# ポーリングの概要

ポーリングとは、NetScaler ConsoleがNetScalerインスタンスから特定の情報を収集するプロセスです。組織のために、世界中に複数のNetScalerインスタンスを設定している場合があります。NetScaler Consoleを介してインスタンスを監視するには、NetScaler Consoleは、CPU使用率、メモリ使用率、SSL証明書、ライセンス機能、ライセンスの種類など、すべての管理対象NetScalerインスタンスから特定の情報を収集する必要があります。NetScaler Consoleと管理対象インスタンスの間で行われるポーリングには、次の種類があります。

- インスタンスポーリング
- インベントリポーリング
- パフォーマンスデータ収集
- インスタンスバックアップポーリング
- 構成監査ポーリング
- SSL証明書ポーリング
- エンティティポーリング

NetScaler Consoleは、NITROコール、Secure Shell (SSH)、Secure Copy (SCP) などのプロトコルを使用して、NetScalerインスタンスから情報をポーリングします。

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

## NetScaler Consoleが管理対象インスタンスとエンティティをポーリングする方法

NetScaler Consoleは、デフォルトで定期的に自動的にポーリングします。また、NetScaler Consoleでは、いくつかのポーリングタイプについてポーリング間隔を設定したり、必要に応じて手動でポーリングしたりすることもできます。

次の表に、ポーリングの種類、ポーリング間隔、使用されるプロトコルなどの詳細を示します。

| ポーリングの種類 | ポーリング間隔 | ポーリング情報 | 使用されるプロトコル | ポーリング間隔の設定 |
|---|---|---|---|---|
| **インスタンスのポーリング** | 1分ごと（デフォルト） | 状態、1秒あたりのHTTPリクエスト、CPU使用率、メモリ使用量、スループットなどの統計情報。 | NITROコール。 | いいえ |
| **インベントリのポーリング** | 60分ごと（デフォルト） | ビルドバージョン、システム情報、ライセンス機能、モードなどのインベントリの詳細。 | NITROコールとSSH | いいえ |
| **パフォーマンスデータ収集** | 5分ごと（デフォルト） | ネットワークレポート情報 | NITROコール | いいえ |
| **インスタンスバックアップポーリング** | 12時間ごと（デフォルト） | 管理対象NetScalerインスタンスの現在の状態のバックアップファイル | NITROコール、SSH、およびSCP。 | はい。**インフラストラクチャ > インスタンス > NetScaler** に移動します。インスタンスを選択し、**アクションの選択** リストから **バックアップ/復元** をクリックします。 |

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

| ポーリングの種類 | ポーリング間隔 | ポーリング情報 | 使用されるプロトコル | ポーリング間隔の設定 |
|---|---|---|---|---|
| **構成監査ポーリング** | 10時間ごと（デフォルト） | NetScalerインスタンスで発生する構成変更（例：実行中の構成と保存された構成） | SSH、SCP、およびNITROコール | はい。**インフラストラクチャ > 構成監査** に移動します。構成監査ページで、**設定** をクリックし、構成監査ポーリングのポーリング間隔を設定します。 |
| | | | | 構成監査を手動でポーリングし、インスタンスのすべての構成監査をNetScaler Consoleに即座に追加できます。これを行うには、**インフラストラクチャ > 構成監査** に移動し、**今すぐポーリング** をクリックします。**今すぐポーリング** ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。 |
| **SSL証明書ポーリング** | 24時間ごと（デフォルト） | NetScalerインスタンスにインストールされて | NITROコールとSCP | はい。**Infrastructure > SSL Dashboard** に |

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

| ポーリングの種類 | ポーリング間隔 | ポーリング情報 | 使用されるプロトコル | ポーリング間隔の設定 |
|---|---|---|---|---|
| | | いるSSL証明書。 | | 移動します。SSL Dashboard ページで、**Settings** をクリックしてポーリング間隔を設定します。 |
| | | | | SSL証明書を手動でポーリングし、インスタンスのすべての証明書を NetScaler Consoleに即座に追加できます。これを行うには、**Infrastructure > SSL Dashboard** に移動し、**Poll Now** をクリックします。**Poll Now** ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。 |
| **エンティティポーリング** | | | | |
| すべてのインスタンス | 720分ごと（デフォルト） | インスタンスに構成されているすべてのエンティティ。エン | NITROコール | はい。30分から1440分の間で設定できます。設定するには、 |

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

| ポーリングの種類 | ポーリング間隔 | ポーリング情報 | 使用されるプロトコル | ポーリング間隔の設定 |
|---|---|---|---|---|
| | | ティティとは、NetScalerインスタンスにアタッチされているポリシー、仮想サーバー、サービス、またはアクションのいずれかです。エンティティポーリングを有効にするには、「NetScaler Console機能の有効化または無効化」を参照してください。 | | **Infrastructure > Network Functions** に移動します。Networks Functionページで、**Settings** をクリックしてポーリング間隔を設定します。 |
| | | | | エンティティを手動でポーリングし、インスタンスのすべてのエンティティをNetScaler Consoleに即座に追加できます。これを行うには、**Infrastructure > Network Functions** に移動し、**Poll Now** をクリックします。**Poll Now** ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスを |

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

| ポーリングの種類 | ポーリング間隔 | ポーリング情報 | 使用されるプロトコル | ポーリング間隔の設定 |
|---|---|---|---|---|
| | | | | ポーリングできます。 |
| 選択されたNetScalerインスタンス | 15分ごと（デフォルト） | デフォルトのポーリングサイクルがトリガーされる前に変更が行われたNetScalerインスタンスのみをポーリングします。 | NITROコール | はい。5分から60分の間で設定できます。**Infrastructure > Network Functions** に移動し、**Settings** をクリックして、**Delay time for Network Functions** テキストボックスに時間を指定します。 |

**注**

ポーリングに加えて、管理対象のNetScalerインスタンスによって生成されたイベントは、インスタンスに送信されるSNMPトラップを介してNetScaler Consoleによって受信されます。たとえば、システム障害や構成の変更があった場合にイベントが生成されます。

インスタンスのバックアップ中、SSLファイル、CA証明書ファイル、NetScalerテンプレート、データベース情報などがNetScaler Consoleにダウンロードされます。構成監査中、ns.confファイルがダウンロードされ、ファイルシステムに保存されます。管理対象のNetScalerインスタンスから収集されたすべての情報は、データベース内に内部的に保存されます。

## インスタンスをポーリングするさまざまな方法

NetScaler Consoleが管理対象インスタンスに対して実行するポーリングのさまざまな方法は次のとおりです。

- インスタンスのグローバルポーリング
- インスタンスの手動ポーリング
- エンティティの手動ポーリング

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

### インスタンスのグローバルポーリング

NetScaler Consoleは、ユーザーが設定した間隔に応じて、ネットワーク内のすべての管理対象インスタンスを自動的にポーリングします。デフォルトのポーリング間隔は30分ですが、**Infrastructure > Network Functions** > **Settings** に移動して、要件に応じて間隔を設定できます。

### インスタンスの手動ポーリング

NetScaler Consoleが多数のエンティティを管理している場合、ポーリングサイクルはレポートの生成に時間がかかり、空白の画面が表示されたり、システムが以前のデータを表示したままになったりする可能性があります。

NetScaler Consoleでは、自動ポーリングが行われない最小ポーリング間隔期間があります。新しいNetScalerインスタンスを追加したり、エンティティが更新されたりした場合、NetScaler Consoleは次のポーリングが行われるまで、新しいインスタンスやエンティティへの更新を認識しません。また、その後の操作のために仮想IPアドレスのリストをすぐに取得する方法はありません。最小ポーリング間隔期間が経過するまで待つ必要があります。新しく追加されたインスタンスを検出するために手動でポーリングを行うことはできますが、これによりNetScalerネットワーク全体がポーリングされ、ネットワークに大きな負荷がかかります。ネットワーク全体をポーリングする代わりに、NetScaler Consoleでは、いつでも選択したインスタンスとエンティティのみをポーリングできるようになりました。

NetScaler Consoleは、1日の設定された時間に情報を収集するために、管理対象インスタンスを自動的にポーリングします。選択されたポーリングにより、NetScaler Consoleがこれらの選択されたインスタンスにバインドされたエンティティの最新ステータスを表示するために必要な更新時間が短縮されます。

**NetScaler Consoleで特定のインスタンスをポーリングするには:**

1. NetScaler Consoleで、**Infrastructure > Network Functions** に移動します。
2. **Network Functions** ページの右上隅にある **Poll Now** をクリックします。
3. ポップアップページ **Poll Now** は、ネットワーク内のすべてのNetScalerインスタンスをポーリングするか、選択したインスタンスをポーリングするオプションを提供します。
    a. **All Instances** タブ - **Start Polling** をクリックして、すべてのインスタンスをポーリングします。
    b. **Select Instances** タブ - リストからインスタンスを選択します
4. **Start Polling** をクリックします。

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

NetScaler Consoleは手動ポーリングを開始し、すべてのエンティティを追加します。

## エンティティの手動ポーリング

NetScaler Consoleでは、特定のインスタンスにバインドされている一部の選択されたエンティティのみをポーリングすることもできます。たとえば、このオプションを使用して、インスタンス内の特定のエンティティの最新ステータスを知ることができます。このような場合、更新された1つのエンティティのステータスを知るために、インスタンス全体をポーリングする必要はありません。エンティティを選択してポーリングすると、NetScaler Consoleはそのエンティティのみをポーリングし、NetScaler Console GUIのステータスを更新します。

仮想サーバーがDOWN状態である例を考えてみましょう。その仮想サーバーの状態は、次の自動ポーリングが行われる前にUPに変わっている可能性があります。仮想サーバーの変更されたステータスを表示するには、その仮想サーバーのみをポーリングして、正しい状態がGUIにすぐに表示されるようにしたい場合があります。

ステータスの更新について、以下のエンティティをポーリングできるようになりました: サービス、サービスグループ、負荷分散仮想サーバー、キャッシュ削減仮想サーバー、コンテンツスイッチング仮想サーバー、認証仮想サーバー、VPN仮想サーバー、GSLB仮想サーバー、およびアプリケーションサーバー。

**注**

仮想サーバーをポーリングすると、その仮想サーバーのみがポーリングされます。サービス、サービスグループ、サーバーなどの関連エンティティはポーリングされません。すべての関連エンティティをポーリングする必要がある場合は、エンティティを手動でポーリングするか、インスタンスをポーリングする必要があります。

**NetScaler Consoleで特定のエンティティをポーリングするには：**

例として、このタスクはロードバランシング仮想サーバーのポーリングに役立ちます。同様に、他のネットワーク機能エンティティもポーリングできます。

1. 「ネットスケーラー コンソール」で、**Infrasturcture > Network Functions > Load Balancing > Virtual Servers** に移動します。
2. 状態がDOWNと表示されている仮想サーバーを選択し、**Poll Now** をクリックします。仮想サーバーのステータスがUPに変わります。

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

# NetScaler® テレメトリプログラム

Citrixは、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンステレメトリデータとNetScalerの展開および機能使用状況のテレメトリデータを収集します。記載されているNetScalerテレメトリプログラムに準拠するために、必要なライセンスおよび機能使用状況データを自動または手動でアップロードできますこちら。NetScaler Consoleの構成および機能使用状況データも、Citrix製品およびサービスの管理、測定、改善のために収集されます。既存のNetScaler Consoleのお客様は、NetScalerテレメトリプログラムに準拠していることを確認する必要があります。NetScalerの機能使用状況データを送信することで、NetScalerの運用全体を改善および簡素化し、製品およびサービスの強化をサポートするために、NetScalerインスタンスをNetScaler Consoleに追加することを強くお勧めします。詳細はこちら。

必要なテレメトリデータは、次の方法でアップロードできます。

- **自動収集モード** - このモードは、**14.1-25.56以降 / 13.1-53.22以降**のビルドにアップグレードすると、デフォルトで有効になります。自動モードでは、自動有効化されたチャネル（エンドポイントURL）を使用するためのアウトバウンド接続が作成され、テレメトリデータが自動的にアップロードされます。エンドポイントURLに到達可能であることを確認するだけで済みます。アップロードは自動的に行われるため、前提条件が失敗しない限り、お客様側での操作は不要です。詳細については、「自動収集モード」を参照してください。
- **手動収集モード** - このモードは、自動モードが無効になっている場合にのみ有効になります。NetScaler ConsoleオンプレミスのNetScalerテレメトリホームページから必要なテレメトリデータをダウンロードし、30日以内にNetScaler Consoleサービスへの初回アップロードを完了する必要があります。以降のアップロードは、準拠を維持するために90日ごとに行う必要があります。詳細については、「手動収集モード」を参照してください。

自動テレメトリモードを使用して必要なデータを自動的にアップロードすることをお勧めしますが、自動モードを無効にして手動でアップロードすることもできます。自動モードと手動モードの両方で、NetScalerテレメトリプログラムに準拠するためにデータアップロードが必要です。オプションのテレメトリデータをデータアップロードに含めないように選択できますが、必要なライセンスコンプライアンスおよび機能使用状況のテレメトリデータは、自動モードと手動モードの両方で提供する必要があります。

準拠を維持するには、最後の正常なアップロードからの日数が90日を超えてはなりません。

NetScalerテレメトリプログラムの一環として、管理対象のNetScalerインスタンスに以下の構成がプッシュされました。

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

- AppFlow構成: `enable ns feature AppFlow`
- テレメトリメトリックプロファイル構成: `add analytics profile telemetry_metrics_profile -type timeseries -outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300`

**注:**

テレメトリを最適に収集するために、最新のNetScaler Consoleビルドにアップグレードすることをお勧めします。

- **14.1-43.x / 13.1-57.x**ビルド以降、NetScaler Consoleは、NetScalerインスタンスにテレメトリメトリックプロファイル構成が存在する場合、それを削除します。テレメトリメトリックプロファイル構成の削除は、NetScalerインスタンスの既存の機能には影響しません。
- NetScalerまたはNetScaler Consoleの分析機能を使用していない場合は、次のコマンドを使用してAppFlow構成を削除できます。

  `disable ns feature AppFlow`

以下の表は、最新ビルドおよび以前のビルドにおけるAppFlow®およびテレメトリメトリックプロファイル構成の詳細を示しています。

| ビルド | テレメトリプログラムの一部としてプッシュされた構成 | テレメトリモード | 必要なアクション |
|---|---|---|---|
| 14.1-43.x / 13.1-57.x | いいえ | 自動および手動 | 構成はNetScalerインスタンスにプッシュされず、テレメトリメトリックプロファイル構成が存在する場合はNetScalerインスタンスから削除されます。NetScalerまたはNetScaler Consoleの分析機能を使用していない場合は、AppFlow構成を削除するために `disable ns` |

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

| ビルド | テレメトリプログラムの一部としてプッシュされた構成 | テレメトリモード | 必要なアクション |
| --- | --- | --- | --- |
| | | | `feature AppFlow` を使用できます。 |
| 14.1-29.x / 13.1-55.x | いいえ | 自動および手動 | 構成はNetScalerテレメトリプログラムの一部としてプッシュされません。これらの構成がNetScalerインスタンスに存在し、それらを削除したい場合は、NetScalerで `rm analytics profile telemetry_metrics _profile` コマンドを実行してテレメトリメトリックプロファイル構成を削除し、`disable ns feature AppFlow` を使用してAppFlow構成を削除してください。 |
| 14.1-25.56 / 13.1-53.22 | はい。AppFlowとテレメトリメトリックプロファイル構成の両方 | 自動化（すべての前提条件が満たされている場合） | 設定はNetScalerテレメトリプログラムの一部としてプッシュされますが、24時間ごとにチェックされるわけではありません。これらの設定を削除するには、NetScalerで `rm analytics profile telemetry_metrics _profile` コマンドを実行してテレメトリメトリックプロファイル設定を削除 |

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

| ビルド | テレメトリプログラムの一部としてプッシュされた構成 | テレメトリモード | 必要なアクション |
|---|---|---|---|
| | | | し、`disable ns feature AppFlow`を使用してAppFlow設定を削除します。 |
| | | 自動化（いずれかの前提条件が満たされていない場合）または手動 | NetScaler Consoleは、これらの設定が不足している場合、24時間ごとにこれらの設定をチェックし続け、NetScalerインスタンスにプッシュします。設定がプッシュされないようにするには、自動モード（すべての前提条件が満たされている場合）であるか、最新ビルドにアップグレードする必要があります。 |

**注記:**

- Gatewayテレメトリの場合、`/nsconfig/.telemetry.conf`ファイルは次のコマンドで更新されます。NetScaler Consoleは、このコマンドが不足している場合、1時間ごとにこのコマンドをチェックして追加します。

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

- 一部のテレメトリパラメータは、NetScaler ConsoleからNetScalerインスタンスにプッシュされるスクリプトを介して収集されます。これらのスクリプトは読み取り専用であり、NetScalerの何も変更しません。
- 電子メールアドレス、ユーザー名、IPアドレスなど、テレメトリを通じて収集された情報は、一方向ハッシュアルゴリズムを使用してソースで情報をハッシュ化することにより、安全に仮

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

名化されます。その結果、Citrixはこれらの値にアクセスしたり読み取ったりすることはできません。このテレメトリデータは、論理的な資産照合の目的のみに使用されます。

次の表は、NetScalerテレメトリプログラムの一部として収集されるパラメータの詳細を示します。

| カテゴリ | 説明 | 何のために使用しますか？ | 必須/オプション |
|---|---|---|---|
| ライセンス、およびNetScalerの展開と使用状況のテレメトリ | ライセンスの資格、割り当て、使用状況、およびNetScalerのハイレベルな展開データ、NetScalerの機能使用状況に関する情報。 | ライセンスコンプライアンス、およびサービスの管理、測定、改善のため。 | 必須 |
| NetScaler Consoleの展開と機能使用状況のテレメトリ | Consoleの展開と機能使用状況に関する情報。 | サービスの管理、測定、改善のため。 | オプション |

オプションおよび必須のテレメトリパラメータのリストの詳細については、データガバナンスを参照してください。

Citrixは、**2024年6月18日**から3か月以内に、最新のNetScaler Consoleビルド（14.1-25.56以降 / 13.1–53.22以降）に移行することを要求しています。NetScaler Console 14.1-25.56以降 / 13.1–53.22以降にアップグレードした後、テレメトリモードのいずれか（自動または手動）がアクティブに機能している必要があります。手動レポートを選択した場合を除き、自動テレメトリレポートを許可するために必要に応じてファイアウォールを調整することに同意するものとします。

**注意点:**

- テレメトリモジュールは、NetScaler上で複数のSSHコマンドを実行し、NetScaler ConsoleのSSHユーティリティを使用して応答の出力を読み取ります。以下のいずれかの条件が満たされると、SSHユーティリティが正常に機能せず、テレメトリが失敗します。
  - NetScaler OSのホスト名に「#」文字が含まれている。
  - NetScalerのmotd（message of the day）に「#」文字が含まれている。
  - NetScalerのPS1プロンプトに「#」文字が含まれている。
- 最新のビルド (14.1–25.56以降 / 13.1–53.22以降) に、**2024年9月18日**までに移行することを確実にしてください。

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

- 手動テレメトリモードを選択した場合、最初のアップロードは、上記のビルドへの移行から30日以内、かつ2024年10月18日までに完了する必要があります。その後、NetScaler Consoleオンプレミスが NetScalerテレメトリプログラムに準拠するためには、手動テレメトリのアップロードを90日ごとに実行する必要があります。

Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrixサポートを一時停止または終了する場合があります。これらの要件は、法律または規制によって禁止されている範囲では適用されません。詳細については、Citrix License Telemetry FAQを参照してください。

# テレメトリ収集モード

## 自動テレメトリ収集モード

このモードは、NetScaler Console on-prem 14.1-25.53 / 13.1-53.22 以降のビルドにアップグレードすると、デフォルトで有効になります。

自動テレメトリ収集モードの前提条件:

- インターネット接続があること、またはCitrix Cloudにアクセスできるように NetScaler Console on-premでプロキシサーバーが構成されていることを確認してください。詳細については、「システム要件」を参照してください。
- 次のエンドポイントURLに到達可能であることを確認してください:
  - ダウンロードサービスURL: `https://download.citrixnetworkapi.net`
  - サービスURL: `https://adm.cloud.com` (14.1-43.x以前のビルドでのみ必要)。
  - 自動有効化チャネル: `https://safehaven.adm.cloud.com`
- 次のポートが開いていることを確認してください:

| ポート | タイプ | 詳細 | 通信方向 |
|---|---|---|---|
| 5140 | UDP | NetScaler Gateway テレメトリデータを受信するポート | ネットスケーラーからネットスケーラーコンソールへ |

14.1-25.53または13.1-53.22ビルドにアップグレードし、**NetScaler Telemetry**ページに移動した後、次のポップアップウィンドウで**次へ**をクリックします。



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

## 手動テレメトリ収集モード

手動テレメトリ収集モードを使用するには、まず**Security Advisory**を無効にし、次に縦の省略記号をクリックして**無効にする**を選択する必要があります。



ポップアップウィンドウで、**データを手動でアップロードすることに同意します**をクリックして、自動テレメトリ収集を無効にします。テレメトリ収集モードは自動的に**手動**に変更されます。手動テレメトリモードでは、新しいCVEアップデートは利用できず、既存または最後に更新されたCVEでのみSecurity Advisoryを使用できます。

手動モードを選択した後、30日以内にテレメトリをダウンロードし、NetScaler Consoleサービスで最初のアップロードを完了する必要があります。その後のアップロードは90日ごとに行う必要があります。

**注:**

90日間のテレメトリデータを保存するために、最大2 GBのNetScaler Consoleディスクスペースが使用されます。

**NetScaler Telemetry**ホームページから、**Download Telemetry**をクリックして、必要なテレメトリデータを含むバンドル(.tgz)ファイルをダウンロードします。



テレメトリファイルをダウンロードした後、NetScaler Consoleサービスにアップロードする必要があります。NetScaler Consoleサービスにアップロードするには:

1. Citrix Cloud (citrix.cloud.com) にログオンします。Citrix Cloudアカウントをお持ちでない場合は、新しいアカウントにサインアップしてください。詳細については、「Citrix Cloudアカウントの作成」(https://docs.citrix.com/ja-jp/citrix-cloud/overview/signing-up-for-citrix-cloud/signing-up-for-citrix-cloud.html)を参照してください。
2. アカウントを選択します。
3. **NetScaler Console Service**で、**Manage**をクリックします。
4. Consoleサービスアカウントを設定します。
5. NetScaler Consoleサービスで、**Settings > Console on-prem telemetry upload**に移動します。
6. **Upload Telemetry**をクリックし、ダウンロードした(.tgz)ファイルを選択してアップロードプロセスを完了します。

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

7. 手動モードを選択してから30日以内に最初のアップロードを完了します。その後、同じ手順を繰り返し、90日ごとにテレメトリファイルをアップロードします。

   **注:**

   - ファイルが有効な(.tgz)形式でない場合、または整合性チェックに合格しない場合、アップロードは失敗します。再度ダウンロードしてアップロードを再試行することをお勧めします。問題が解決しない場合は、カスタマーケアにお問い合わせください。
   - オプションのテレメトリデータのアップロードを無効にできます。無効にするには、まず**NetScaler Telemetry**ページで**Security Advisory**を無効にし、次に**Settings > Administration > Enable or disable the Console feature data sharing**に移動して、**I agree to share Console feature usage data**チェックボックスをオフにする必要があります。

   - NetScaler Consoleオンプレミスでは、アップロード期限の7日前にリマインダーバナーが表示されます。

# テレメトリ収集とアップロードの問題をトラブルシューティングするための診断

リリース14.1ビルド56.xより前は、診断機能はこれらのエンドポイントURLへのアウトバウンド接続を検査し、到達可能状態にあるかどうかを知らせるのに役立ちました。NetScaler On-prem リリース14.1ビルド56.x以降では、コレクターレベル（コンソール）とデバイスレベル（個々のNetScalerインスタンス）の両方で、テレメトリ収集とアップロードの問題を特定し、トラブルシューティングするための強化された診断機能が提供されます。

## リリース14.1ビルド56.x以降の診断動作

注:

リリース14.1ビルド56.x以降、テレメトリ診断機能は、コレクターレベル（コンソール）とデバイスレベル（個々のNetScalerインスタンス）の両方で、テレメトリ収集とアップロードの問題を特定し、トラブルシューティングするために強化されています。

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

すべての管理対象NetScalerインスタンスは、コンプライアンスを維持するためにテレメトリデータを送信する必要があります。しかし、接続または構成の問題により、テレメトリのアップロードと収集が失敗することがあります。 Console on-prem のNetScalerテレメトリページにある診断機能は、両方のレベルで問題を迅速に特定し、トラブルシューティングするのに役立ちます。

- コレクターレベル（コンソール）：データが正常にアップロードされたかどうかを確認します。
- デバイスレベル（個々のNetScalerインスタンス）：NetScalerインスタンスからデータが収集されたかどうかを確認します。

NetScaler テレメトリ診断(/en-us/netscaler-application-delivery-management-software/media/netscaler-diagonstic.png)

### 仕組み

診断プロセスに関わる大まかな手順は次のとおりです。

- 自動実行：診断は24時間ごとに自動的に実行されます。
- オンデマンド実行：ユーザーは必要に応じて、特に問題の修正を試みた後に、手動で診断を実行できます。
- ステータスインジケーター：結果は明確なステータスで表示されます。
  - 成功：問題は検出されませんでした。
  - 要対応: 1つ以上の問題でユーザーの操作が必要です。

**注:**

**詳細を表示**をクリックするか、エラーが強調表示されている領域をクリックして、詳細なエラーログと軽減手順を確認してください。

### コレクターレベル (コンソール) の診断

このセクションでは、NetScaler Console が管理対象デバイスからデータを正常に収集し、必要な宛先にアップロードしているかどうかを確認します。

| チェックフィールド | 説明 |
| --- | --- |
| 実行時間 | 管理対象のNetScalerインスタンスからの最後のテレメトリ収集のタイムスタンプ。 |

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

| チェックフィールド | 説明 |
| --- | --- |
| パッケージバージョン | このチェックでは、Console on-prem にインストールされているテレメトリパッケージのバージョンを特定し、最新のデータセットが収集されていることを確認します。 |
| Evergreenダウンロードステータス | (自動モードのみ) Console on-prem は、ダウンロードサービスURLから更新されたテレメトリスクリプトパッケージを24時間ごとにチェックします。情報 (i) アイコンにカーソルを合わせると、障害の具体的な原因が表示されます。軽減手順の詳細については、障害ステータスをクリックしてください。 |
| 接続ステータス | (自動モードのみ) 必要なURLがホワイトリストに登録され、到達可能であることを確認します。例えば、プロキシの誤設定による接続の問題は、コンソールがこれらのURLに到達するのを妨げます。情報(i)アイコンにカーソルを合わせると、到達不能の具体的な原因が表示されます。軽減策の詳細については、**到達不能ステータス**をクリックしてください。 |
| | - ダウンロードサービスURL: 最新のテレメトリパッケージダウンロードのソース。 |
| | - 自動有効化チャネルURL: テレメトリデータをアップロードするための宛先。 |

### デバイスレベル (NetScaler) 診断

コンソールは、管理対象の各NetScalerインスタンスにテレメトリ収集スクリプトをプッシュし、データを収集し、アップロードのために準備することで、デバイスレベルの診断を実行します。

デバイステレメトリ詳細テーブルは、このプロセスの結果を以下のように提供します。

- デバイスの詳細
- テレメトリステータス
- エラーコードとエラーメッセージ

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

詳細なエラー情報と軽減策については、赤くハイライトされたエラーの詳細をクリックしてください。

**軽減策**: 各エラーコードは、軽減策テーブルの推奨される解決策にマッピングされています。問題の修正には、推奨事項に従ってください。

### エラーテーブルマッピング

| エラーコード | エラーメッセージ | お客様の対応 |
|---|---|---|
| **1161** | サーバーホスト名の解決に失敗しました | サーバーアドレスを解決できません。ネットワークおよびNetScalerコンソールサーバー/エージェントの**DNSサーバー設定**を確認してください。 |
| **1162** | サーバーアドレスを解決できません。ネットワークおよびNetScalerコンソールサーバー/エージェントの**DNSサーバー設定**を確認してください。 | サーバーに接続できません。**ファイアウォール、プロキシ設定、およびネットワーク接続**を確認してください。また、URL `download.citrixnetworkapi.net` がネットワークまたはプロキシ経由でアクセス可能であることを確認してください。 |
| **1165** | プロキシエラー | **プロキシ設定**を確認し、プロキシ経由でネットワーク接続が機能していることを確認してください。 |
| **1166** | プロキシ認証に失敗しました | NetScalerコンソールで**プロキシ資格情報**を確認してください。 |
| **1170** | SSL証明書の検証に失敗しました。 | ネットワークで**SSLインターセプター**を使用している場合は、NetScalerコンソールに適切な**ルート証明書がインス** |

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

| エラーコード | エラーメッセージ | お客様の対応 |
| --- | --- | --- |
| | | **トールされている**ことを確認してください。 |
| **1171** | SSL証明書の有効期限が切れました | **SSL証明書の有効期限が切れました。** |
| **1172** | SSL証明書の検証に失敗しました。 | ネットワークで**SSLインターセプター**を使用している場合は、NetScalerコンソールに適切な**ルート証明書がインストールされている**ことを確認してください。 |
| **1173** | SSL証明書の検証に失敗しました。 | これは**自己署名証明書**が原因である可能性があります。ネットワークで**SSLインターセプター**を使用している場合は、NetScalerコンソールに適切な**ルート証明書がインストールされている**ことを確認してください。 |
| **1261** | サーバーのホスト名の解決に失敗しました | サーバーアドレスを解決できません。ネットワークおよびNetScalerコンソールサーバー/エージェントの**DNSサーバー設定**を確認してください。 |
| **1262** | リクエスト接続タイムアウト | サーバーに接続できません。**ファイアウォール、プロキシ設定、およびネットワーク接続**を確認してください。両方のURL (`download.citrixnetworkapi.net`, `safehaven.adm.cloud.com`) がネットワークまたはプロキシ経由でアクセス可能であることを確認してください。 |

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

| エラーコード | エラーメッセージ | お客様の対応 |
| --- | --- | --- |
| **1265** | プロキシエラー | **プロキシ設定**を確認し、プロキシ経由でネットワーク接続が機能していることを確認してください。 |
| **1266** | プロキシ認証に失敗しました。 | NetScalerコンソールで**プロキシ資格情報**を確認してください。 |
| **1270** | SSL証明書の検証に失敗しました | ネットワークで**SSLインターセプター**を使用している場合は、適切な**ルート証明書がNetScalerコンソールにインストールされている**ことを確認してください。 |
| **1271** | SSL証明書の有効期限が切れました。 | サーバーの**SSL証明書の有効期限が切れました。** |
| **1272** | SSL証明書の検証に失敗しました | ネットワークで**SSLインターセプター**を使用している場合は、適切な**ルート証明書がインストールされている**ことをNetScalerコンソールで確認してください。 |
| **1273** | SSL証明書の検証に失敗しました | これは**自己署名証明書**が原因である可能性があります。ネットワークで**SSLインターセプター**を使用している場合は、適切な**ルート証明書がインストールされている**ことをNetScalerコンソールで確認してください。 |
| **1361** | サーバーのホスト名の解決に失敗しました | サーバーアドレスを解決できません。ネットワークおよびNetScalerコンソールサーバー/エージェントの**DNSサーバー構成**を確認してください。 |

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

| エラーコード | エラーメッセージ | お客様の対応 |
| --- | --- | --- |
| **1362** | リクエスト接続がタイムアウトしました。 | サーバーに接続できません。**ファイアウォール、プロキシ設定、およびネットワーク接続**を確認してください。URL `safehaven.adm.cloud.com` がネットワークまたはプロキシ経由でアクセス可能であることを確認してください。 |
| **1365** | プロキシエラー | **プロキシ設定**を確認し、プロキシ経由でネットワーク接続が機能していることを確認してください。 |
| **1366** | プロキシ認証に失敗しました | NetScalerコンソールで**プロキシ資格情報**を確認してください。 |
| **1370** | SSL証明書の検証に失敗しました。 | ネットワークで**SSLインターセプター**を使用している場合は、NetScalerコンソールに適切な**ルート証明書がインストールされている**ことを確認してください。 |
| **1371** | SSL証明書の有効期限が切れました | サーバーの**SSL証明書の有効期限が切れました**。 |
| **1372** | SSL証明書の検証に失敗しました。 | ネットワークで**SSLインターセプター**を使用している場合は、NetScalerコンソールに適切な**ルート証明書がインストールされている**ことを確認してください。 |
| **1373** | SSL証明書の検証に失敗しました。 | これは、**自己署名証明書**が原因である可能性があります。ネットワークで**SSLインターセプター**を使用している場合は、適切な**ルート証明書がインストールされている**ことを |

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

| エラーコード | エラーメッセージ | お客様の対応 |
| --- | --- | --- |
| | | NetScalerコンソールで確認してください。 |
| **2000** | このデバイスではテレメトリがスキップされました。 | これは、このデバイスが**別のNetScaler Console/Service/Agentによって管理されている**ためである可能性があります。他のコレクターがテレメトリデータを正常に送信していることを確認してください。 |
| **2100** | インスタンスの状態がダウンしているか、到達できません。 | **インスタンスが実行中で到達可能である**ことを確認してください。 |
| **2250** | SSH認証エラー | NetScalerコンソールで、そのデバイスの**デバイスプロファイルが適切に構成されている**ことを確認してください。 |
| **2251** | SSH接続がタイムアウトしたか、拒否されました。 | 接続がファイアウォールまたはネットワークポリシーによって一時的にブロックされているか、デバイスに到達できない可能性があります。**ネットワーク接続を確認**し、**SSHポートにアクセスできる**ことを確認してください。 |
| **2252** | ホストキーの検証に失敗しました | 管理者とサーバーのIDを確認し、古いキーを削除してください: `ssh-keygen -R <server_address>`。 |
| **2350** | SSH認証エラー。 | NetScalerコンソールで、デバイスの**デバイスプロファイルが適切に構成されている**ことを確認してください。 |

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

| エラーコード | エラーメッセージ | お客様の対応 |
| --- | --- | --- |
| **2351** | SSHがデバイスへの接続に失敗しました | 接続がファイアウォールまたはネットワークポリシーによって一時的にブロックされているか、デバイスに到達できない可能性があります。**ネットワーク接続を確認**し、**SSHポートがアクセス可能である**ことを確認してください。 |

## リリース14.1ビルド56.x以前の診断動作

リリース14.1ビルド51.x以前では、診断機能はこれらのエンドポイントURLへのアウトバウンド接続を検査し、到達可能かどうかを知らせます。

- エンドポイントURLが到達可能な状態であることを確認したら、**NetScaler® Telemetryページに移動**をクリックします。
- いずれかの前提条件が満たされない場合、診断チェックは到達できないエンドポイントを表示し、URLが到達可能であることを確認する必要があります。詳細を表示するには、**前提条件を表示**をクリックします。
- エンドポイントURLに到達可能かどうかを確認するには、**診断の実行**をクリックして診断を実行できます。
- 何も対策を講じない場合、オンプレミスのNetScaler ConsoleはNetScalerテレメトリプログラムに準拠していない可能性があります。

自動有効化チャネルの一部として、NetScaler Consoleオンプレミスで最新のCVEアップデートを含む**セキュリティアドバイザリ**機能を使用できます。セキュリティアドバイザリ機能を使用すると、NetScalerインスタンスを危険にさらしているCVEを特定し、修正を推奨できます。NetScalerインスタンスに影響を与えている最新のCVEの詳細は、セキュリティアドバイザリで確認できます。詳細については、「セキュリティアドバイザリ」を参照してください。

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

**注：**

セキュリティアドバイザリを無効にすることもできます。**セキュリティアドバイザリ**を無効にするか、自動テレメトリモードをオプトアウトするか、または前提条件のいずれかが失敗した場合、新しいCVEアップデートは利用できず、既存または最後に更新されたCVEでのみセキュリティアドバイザリを使用できます。

自動テレメトリ収集が正常に有効になると、最初のアップロードは24時間以内に行われます。その後のアップロードは24時間ごとに自動的に行われます。アップロードが完了すると、ステータスは**成功**に変わります。

アップロードが失敗した場合は、エンドポイントURLに到達可能であることを確認してください。ステータスが到達可能と表示されていてもアップロードが失敗する場合は、カスタマーケアにお問い合わせください。

## テレメトリアップロードの通知

デフォルトでは、テレメトリアップロードのメール通知が有効になっています。メール通知を受信するための前提条件は、メール配信リストを設定することです。詳細については、「通知設定の構成」を参照してください。管理者として、次のシナリオでメール通知を受信します。

- **テレメトリ収集の失敗** - 問題が解決されるまで、24時間ごとにメール通知が送信されます。通知には、問題の影響を受けるNetScalerおよびConsoleのIPアドレスが含まれます。
- **自動モードによるアップロードの失敗** - 問題が解決されるまで、24時間ごとにメール通知が届きます。
- **手動アップロードの期限が迫っている場合**（手動モードが有効な場合のみ） - イベント中に1通、アップロード完了後に1通のメール通知が届きます。
- **手動アップロードの期限超過** (手動モードが有効な場合のみ) - イベント中に1通のメール通知が届き、アップロード完了後に別のメールが届きます。

**注:**

NetScalerデバイスでのテレメトリ収集に関する問題の通知は、ユーザーがコンソールユーザーインターフェイスにログインするたびにバナーとして表示されます。

以下は、NetScalerデバイスでのテレメトリ収集失敗に関するメールおよびバナー通知の例です。

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



メール通知を無効にできます。無効にするには：

1. **設定 > 管理 > イベント通知とダイジェストの構成**に移動します。
2. **イベント通知 > システム通知の構成**で、**TelemetryMonitoring**を検索し、この通知を削除して、**保存**をクリックします。



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

# データガバナンス

既存のすべてのNetScaler Consoleのお客様は、自動モードまたは手動モードのいずれかで必要なテレメトリデータをアップロードすることにより、NetScalerテレメトリプログラムに準拠する必要があります。NetScalerテレメトリプログラムは、14.1-25.53以降/13.1-53.22以降のビルドから有効になります。詳細については、NetScalerテレメトリプログラムを参照してください。

Citrixは、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンステレメトリデータとNetScaler®の展開および機能使用状況テレメトリデータを収集します。NetScaler Consoleの構成および機能使用状況データも、Citrix製品およびサービスの管理、測定、改善のために収集されます。

自動テレメトリ収集モードでは、NetScaler Consoleオンプレミスで**セキュリティアドバイザリ**機能を使用でき、オプションのテレメトリパラメータが収集されます。オプションのパラメータは無効にできますが、必須のパラメータは無効にできません。

**注記:**

- NetScaler Console **14.1-25.53以降** / **13.1-53.22以降**のビルドにアップグレードすると、以下の構成がNetScaler Consoleを介してNetScalerインスタンスに自動的にプッシュされます。この構成は、NetScalerインスタンスでテレメトリメトリックを収集および保存します。

```
enable ns feature AppFlow

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

- 手動モードまたは自動モード（前提条件が満たされていない場合）の場合、NetScaler Consoleは24時間ごとに上記の構成をチェックし続け、この構成が欠落している場合はNetScalerインスタンスにプッシュします。構成がプッシュされないようにするには、自動モード（すべての前提条件が満たされている場合）にするか、今後のビルド（**14.1-29.x**または**13.1-55.x**）にアップグレードする必要があります。

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

- `/nsconfig/.telemetry.conf` ファイルは、Gatewayテレメトリの以下のコマンドで更新されます。NetScaler Consoleは1時間ごとにこのコマンドをチェックし、このコマンドが欠落している場合は追加します。

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

- 一部のテレメトリパラメータは、NetScaler ConsoleからNetScalerインスタンスにプッシュされるスクリプトを介して収集されます。これらのスクリプトは読み取り専用であり、NetScalerの何も変更しません。
- テレメトリを介して収集される情報（メールアドレス、ユーザー名、IPアドレスなど）は、一方向ハッシュアルゴリズムを使用してソースで情報をハッシュすることにより、安全に仮名化されます。その結果、Citrixはこれらの値にアクセスしたり読み取ったりすることはできません。このテレメトリデータは、論理的な資産マッチングの目的でのみ使用されます。

次の表に、NetScalerテレメトリプログラムの一部として収集されるパラメータの詳細を示します。

| カテゴリ | 説明 | 何のために使用しますか？ | 必須/オプション |
|---|---|---|---|
| ライセンス、およびNetScalerの展開と使用状況のテレメトリ | ライセンスの資格、割り当て、使用状況、高レベルのNetScaler展開データ、およびNetScaler機能の使用状況に関する情報。 | ライセンスコンプライアンス、およびサービスの管理、測定、改善のため。 | 必須 |
| NetScaler Consoleの展開と機能使用状況のテレメトリ | Consoleの展開と機能使用状況に関する情報。 | サービスの管理、測定、改善のため。 | オプション |

オプションパラメーターを無効にするには：

1. NetScaler Consoleオンプレミスで、**NetScaler Telemetry** に移動し、**Security Advisory** を無効にします。
2. **Settings > Administration > Enable or disable the Console feature data sharing** に移動し、**I agree to share Console feature usage data** チェックボックスをオフにします。

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

NetScaler Consoleが14.1-8.xから14.1-21.xビルドの場合、Cloud Connectを構成し、Security Advisory機能を有効にすると、データ収集が有効になります。詳細については、「Cloud Connectのデータガバナンス」を参照してください。

NetScaler Consoleが14.1-4.x以前のバージョンの場合、Citrix Cloudで顧客IDを作成して、NetScaler Consoleオンプレミス展開からCitrix Cloudアカウントに、NetScaler Consoleの健全性、ステータス、その他のメトリックに関する重要な統計を送信できます。Citrixは、NetScaler Consoleの使用状況を把握するために統計を収集します。詳細については、「顧客IDのデータガバナンス」を参照してください。

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

# IoC情報の利用条件

IoC情報（以下に定義）を利用することにより、お客様は、その利用条件として以下を認識し、同意するものとします。

Citrix Systems, Inc. および/またはその関連会社（以下「Citrix」）は、組織が自社の環境が侵害されている可能性があるかどうかを判断するのに役立つように、侵害の痕跡（Indicators of Compromise）ロジックスクリプトおよび侵害の痕跡に関する関連ガイダンス（総称して「IoC情報」）を開発しました。

IoC情報は、脅威アクターが関連環境を標的とする際に使用する可能性のあるすべての手法、戦術、または手順（以下「TTP」）を網羅しているわけではありません。さらに、脅威アクターはTTPとインフラストラクチャを頻繁に変更します。これらの理由およびその他の理由により、IoC情報は法医学的価値が限定的である可能性があり、実際の侵害を特定できない場合があります。お客様の環境を評価するために、経験豊富なフォレンジック調査員のサービスを利用することを強くお勧めします。

IoC情報は現状有姿で提供されます。Citrixは、IoC情報に関して、明示的か黙示的かを問わず、IoC情報にエラーがないこと、または商品性や特定の目的への適合性の条件を満たしていることを含め、いかなる保証または表明も行いません。

IoC情報はCitrixの機密情報および専有情報であり、これらの資料の受領者とCitrixとの間で締結されている適用される秘密保持契約の条件に従うものとします。Citrixの書面による事前の明示的な許可なく、IoC情報のいかなる部分も、いかなる形式または手段によっても、複製、再配布、または第三者に送信することはできません。

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

# NetScaler Consoleライセンス

## ライセンス

NetScaler Consoleは、`https`プロトコルを介してインスタンスが検出された場合、NetScalerインスタンスを管理および監視するために、検証済みのNetScalerライセンスを必要とします。

NetScaler Consoleは、以下のライセンスエディションをサポートしています。NetScaler Consoleライセンスの購入については、NetScalerの営業担当者またはパートナーにお問い合わせください。

**Expressエディション** – Expressエディションライセンスを使用すると、任意の数のインスタンスを管理および監視できます。デフォルトでは、Expressエディションライセンスが適用されます。

**Advancedエディション** - 検出されたアプリケーションを管理し、購入した仮想サーバーと無料の仮想サーバーの分析を表示できます。

**注意点**:

- **ビルド13.1-9.x以前**の場合、最大30個の検出されたアプリケーションまたは仮想サーバーを管理し、分析を表示できます。30個の検出されたアプリケーションまたは30個の仮想サーバーを超える場合は、Advancedライセンスを購入して適用する必要があります。たとえば、100個の仮想サーバーライセンスを購入した場合、最大130個の仮想サーバーライセンスを使用する権利があります。
- **ビルド13.1-12.x以降**の場合、最大2つの検出されたアプリケーションまたは仮想サーバーを管理し、分析を表示できます。2つの検出されたアプリケーションまたは2つの仮想サーバーを超える場合は、Advancedライセンスを購入して適用する必要があります。たとえば、100個の仮想サーバーライセンスを購入した場合、最大102個の仮想サーバーライセンスを使用する権利があります。

**13.1-12.xから14.1-17.xまでのビルドへのアップグレード後**:

- すべてのExpressデフォルトの無料仮想サーバーは30日間機能し続けます。30日以内に2つの仮想サーバーを選択し、2つのデフォルトライセンスを適用できます。アップグレード後30日以内にユーザーが何も操作しない場合、NetScaler Consoleはランダムに2つの仮想サーバーにライセンスを適用し、残りの仮想サーバーのライセンスを解除します。これらの仮想サーバーを有効にするには、新しいAdvancedライセンスを購入して適用する必要があります。

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

- アップグレード後、NetScaler Consoleの動作は以下の通り変更されます。
  - NetScaler Consoleは、必要なアクションを実行するためにさらに30日間猶予を与えます。
  - 30日間の期間中、30個のExpress無料仮想サーバーに対する新しい仮想サーバーの割り当てはブロックされます。
    - たとえば、12.xにアップグレードする前の利用可能な仮想サーバーライセンスの数が30で、使用されていたライセンス済み仮想サーバーが20のみだった場合、30日間の期間中は20個の仮想サーバーのみを使用でき、残りの10個の仮想サーバーにライセンスを付与することはできません。
  - ただし、30日間の期間中、管理者としてAdvanced NetScaler Consoleライセンスを適用し、新しい仮想サーバーを割り当てることができます。

以下の表にライセンスの詳細を示します。

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| **アプリケーション** | アプリケーションダッシュボード | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の仮想サーバー2台が対象です。 | アプリケーションダッシュボード上のNetScaler Web App Firewall関連情報には、Premium (または) Advanced with App Firewallライセンスが必要です。 |
| | Webインサイト | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の仮想サーバー2台が対象です。 | 該当なし |
| | サービスグラフ | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の仮想 | 該当なし |

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

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| | | | サーバー2台の権利があります。 | |
| | 構成 > StyleBooks | 無制限 | 無制限 | 該当なし |
| **セキュリティ** | セキュリティダッシュボード | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の仮想サーバー2台の権利があります。 | セキュリティダッシュボード上のNetScaler Web App Firewall関連情報には、Premium (または) Advanced with App Firewallライセンスが必要です。 |
| | セキュリティ違反 | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の2つの仮想サーバーの資格があります。 | Premium (または) Advanced (App Firewallライセンス付き) |
| | ユーザーとエンドポイント | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の2つの仮想サーバーの資格があります。 | NA |
| **ゲートウェイ** | HDX インサイト | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の2つの仮想サーバー | Advanced (レポート作成 < 1時間) Premium |

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

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| | | | の資格があります。 | (レポート作成 = 無制限) |
| | Gateway インサイト | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の2つの仮想サーバーの資格があります。 | Advanced (レポート作成 < 1時間) Premium (レポート作成 = 無制限) |
| **インフラストラクチャ** | インフラストラクチャ分析 | 無制限 | 無制限 | 該当なし |
| | インスタンス | 無制限 | 無制限 | 該当なし |
| | SSLダッシュボード | 無制限 | 無制限 | 該当なし |
| | イベント | 無制限 | 無制限 | 該当なし |
| | ネットワーク機能 | 無制限 | 無制限 | 該当なし |
| | ネットワークレポート | 無制限 | 無制限 | 該当なし |
| | プールライセンス | 無制限 | 無制限 | 該当なし |
| | 構成 > 構成ジョブ、構成テンプレート、および構成アドバイス | 無制限 | 無制限 | 該当なし |
| | アップグレードジョブ | 無制限 | 無制限 | 該当なし |
| | オーケストレーション | 無制限 | 無制限 | 該当なし |

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

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| **設定** | RBACと外部認証 (インスタンスレベル) | 無制限 | 無制限 | NA |
| | RBACと外部認証 | 無制限 | 無制限 | NA |

*NetScaler ConsoleサポートとのCitrix Director統合の場合 – Citrix DirectorにはPremiumライセンスが必要です。

より多くの仮想サーバー用のライセンスは、10個の仮想サーバーパックで利用できます。有効なライセンスを取得し、NetScaler Console GUIを介してNetScaler Consoleサーバーにライセンスを追加できます。

## 高可用性

NetScaler Consoleサーバーには、VIP、CICO、およびプールされたキャパシティライセンスを含めることができます。ライセンスがNetScaler Consoleサーバーに発行されると、ライセンスはサーバーのホストIDにバインドされます。別のNetScaler Consoleサーバーにライセンスを割り当てることは制限されています。

NetScaler Consoleの高可用性ペアをライセンスサーバーとして構成する場合、プライマリサーバーとセカンダリサーバーは同じライセンスファイルを持っている必要があります。したがって、NetScaler Consoleの高可用性展開では、NetScaler Consoleは両方のサーバーに同じライセンスファイルを割り当てることをサポートしています。

**注**

- NetScaler Consoleリリース12.1-49.x以前をインストールしている場合、セカンダリノードでのライセンスを維持するために30日間が与えられます。30日後、元のライセンスを再ホストするためにCitrixに連絡する必要があります。
- リリース12.1-50.x以降では、NetScaler Consoleライセンスはセカンダリノードに自動的に同期されます。
- プールされたライセンスは、リリース12.1-50.x以降でセカンダリノードに自動的に同期されます。

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

### NetScaler Consoleの高可用性ノード間でライセンスはどのように同期されますか?

フェイルオーバーが発生すると、セカンダリサーバーがプライマリサーバーの役割を引き継ぎます。プライマリサーバーの実際のホストIDは、新しいプライマリサーバーの仮想ホストIDとして構成されます。ライセンスファイルは、仮想ホストIDを使用して新しいプライマリサーバーを認識します。

- **実際のホストID** - このIDは、NetScaler ConsoleサーバーのMACアドレスから生成されます。各NetScaler Consoleスタンドアロン展開には、一意のホストIDがあります。
- **仮想ホストID** - このIDは、HA展開中に自動生成されます。NetScaler Consoleプライマリサーバーの実際のホストIDは、セカンダリサーバーの仮想ホストIDとして使用されます。このIDは、NetScaler Consoleデータベースに暗号化された形式で保存され、このIDへの変更は制限されています。仮想ホストIDは、実際のホストIDよりも優先されます。

NetScaler Console高可用性ノード間で同期されたライセンス(/en-us/netscaler-application-delivery-management-software/media/license-ha-support-console.png)

Node-1がプライマリサーバーで、Node-2がセカンダリサーバーであると仮定します。Node-1の仮想ホストIDはNode-2と同期されます。

1. Node-1で利用可能なライセンスファイルはNode-2に同期されます。
2. Node-1上の新しいライセンスファイルは、定期的にNode-2に同期されます。
3. NetScaler Consoleは、ライセンス容量の倍増を避けるため、ライセンスサーバーがNode-1でのみ実行されるようにします。
4. NetScalerインスタンスは、フローティングIPアドレスを使用してNode-1からライセンスをチェックアウトします。

ライセンスはNetScalerインスタンスにロックされます。NetScaler Console HAからライセンスをチェックアウトするには、インスタンスは特定のNetScalerNetScaler IPアドレスを必要とします。ライセンスを担当するプライマリサーバーにライセンスを適用すると、そのインスタンスの将来のすべてのライセンスに適用されます。ライセンスをインストールしたサーバーからのみライセンスを削除できます。

## オーケストレーション

オーケストレーションモジュールはライセンスとは独立しており、常に利用可能です。

## 仮想サーバーライセンスのアップグレード

NetScaler Consoleのライセンスをアップグレードして、NetScalerでホストされているより多くの仮想サーバーを監視および管理できます。

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

**NetScalerライセンスをアップグレードするには：**

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Infrastructure > Pooled Licensing**に移動します。
3. **License Files**に移動し、次のいずれかのオプションを選択します。

   - **ローカルコンピューターからライセンスファイルをアップロードします**。ライセンスがすでにローカルコンピューターに存在する場合は、**Browse**をクリックし、ライセンスを割り当てるために使用するライセンスファイル（.lic）を選択します。**Finish**をクリックします。
   - **ライセンスアクティベーションコードを使用します**。Citrixは、購入したライセンスのライセンスアクセスコードをメールで送信します。テキストボックスにライセンスアクセスコードを入力し、**Get Licenses**をクリックします。

   **注**

   このオプションを選択する場合、NetScaler Consoleはインターネットに接続されているか、プロキシサーバーが利用可能である必要があります。

4. ライセンス設定ページから、いつでもライセンスを追加できます。

## 検証

**Settings > Licensing & Analytics Configuration**に移動して、NetScaler Consoleにインストールされているライセンスを確認できます。

## 仮想サーバーの管理

NetScaler Consoleを介して管理および監視したい仮想サーバーまたはサードパーティの仮想サーバーを選択できます。

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

**留意事項**

- デフォルトでは、NetScaler Consoleは、各仮想サーバーのポーリングサイクル後に、仮想サーバーに自動的にランダムにライセンスを付与します。
- NetScaler Consoleで検出された仮想サーバーの総数が、インストールされている仮想サーバーライセンスの数よりも少ない場合、NetScaler Consoleは、デフォルトで、すべての仮想サーバーにライセンスを付与します。

仮想サーバーを手動で選択するには、またはライセンス付与を特定の仮想サーバーに制限するには、まず仮想サーバーの自動ライセンス付与を無効にし、その後、管理したい仮想サーバーを選択する必要があります。

### 仮想サーバーの自動ライセンス付与を無効にする

1. **設定 > ライセンスと分析の構成** に移動します。

   ダッシュボードには、利用可能な仮想サーバーライセンス、管理対象の仮想サーバー（仮想サーバータイプを含む）、およびライセンスの有効期限情報が表示されます。
2. **仮想サーバーライセンスの割り当て** で、**自動ライセンス付与仮想サーバー** と **アドレス指定不可能な仮想サーバーの自動選択** を無効にします。



### ライセンス付与するサードパーティ製仮想サーバーを選択する

1. **設定 > ライセンスと分析の構成** に移動します。

   ダッシュボードには、利用可能な仮想サーバーライセンス、管理対象の仮想サーバー（仮想サーバータイプを含む）、およびライセンスの有効期限情報が表示されます。
2. **サードパーティ製仮想サーバーの概要** で、**サードパーティ製仮想サーバーの自動選択** を無効にします。



## 仮想サーバーライセンスを手動で適用する

個々の仮想サーバーに手動でライセンスを適用できます。

1. **仮想サーバーライセンス割り当て**で、**ライセンスの構成**を選択します。

   **すべての仮想サーバー**ページが表示されます。

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

2. プロパティ `Licensed: No` を使用して、ライセンスのない仮想サーバーをフィルタリングします。
3. ライセンスを適用する仮想サーバーを選択します。
4. **ライセンス**をクリックします。

## ポリシーベースの仮想サーバーライセンスを構成する

仮想サーバーにライセンスを適用するポリシーを構成できます。このポリシーは、自動ライセンスを適用する仮想サーバーの数を制御します。また、選択したインスタンスの仮想サーバーにのみライセンスを適用します。

**ポリシーの編集**をクリックすると、以下を指定できます。

- ライセンスを適用するために、CPXインスタンスの仮想サーバー制限を個別に設定します。NetScaler Consoleは、指定された制限までCPXインスタンスの仮想サーバーにライセンスを適用します。

  **重要**

  この制限は、サイドカー展開タイプを除くCPXインスタンスに適用されます。

  サイドカー展開タイプのCPXインスタンスを表示するには、プロパティ `License Type: Freely Managed` を使用して仮想サーバーをフィルタリングします。
- ライセンスを適用するために、選択したNetScalerインスタンス（MPX/VPX/BLX）の仮想サーバー制限を設定します。NetScaler Consoleは、指定された制限までNetScalerインスタンスの仮想サーバーにライセンスを適用します。
- 仮想サーバーライセンスを適用する優先NetScalerインスタンスを選択します。したがって、NetScaler Consoleは選択したインスタンスの仮想サーバーにのみライセンスを適用できます。

仮想サーバーにライセンスを適用するためのポリシーを編集する(/en-us/netscaler-application-delivery-management-software/media/configure-license-policy.png)

## ライセンスされた仮想サーバーを表示する

ライセンスが仮想サーバーに適用された後、ライセンスされた仮想サーバーまたはサードパーティの仮想サーバーを表示できます。

1. **設定 > ライセンスと分析の構成** に移動します。

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

2. **Virtual Servers License Summary** の **Total Licensed** セクションで仮想サーバーの種類をクリックします。

## アドレス指定不可能な仮想サーバーの自動ライセンスサポートを構成する

NetScaler Console は、デフォルトでは、アドレス指定不可能な仮想サーバーにライセンスを自動的に適用しません。アドレス指定不可能な仮想サーバーにライセンスを付与するには、自動ライセンスオプションを無効にし、アドレス指定不可能な仮想サーバーを手動で選択する必要があります。これにより、ライセンスを適用する際に、最初にアドレス指定不可能なサーバーを手動で選択する手間が増えます。また、新しいアドレス指定不可能な仮想サーバーがネットワークに追加されるたびに、手動で選択する必要があります。

NetScaler Console には、**Virtual Server License Allocation** の下にオプションがあります。**Auto-select non addressable Virtual Servers** オプションを有効にすると、アドレス指定不可能な仮想サーバーにライセンスが自動的に適用されます。

**注**

- NetScaler Console は、デフォルトでは、ライセンス付与のためにアドレス指定不可能な仮想サーバーを自動的に選択しません。
- アプリケーション分析 (App Dashboard) は、ライセンスされたアドレス指定不可能な仮想サーバーで現在サポートされている唯一の分析機能です。

# ライセンス

**14.1-21.x**ビルド以降、ライセンスされたVIPの概念は削除されました。NetScaler Consoleオンプレミスでは、無制限のVIPが利用可能になりました。VIPライセンスSKUはまもなく販売終了 (EOS) および更新終了 (EOR) となるため、NetScaler Console仮想サーバーライセンスを購入する必要はなくなりました。

以下の表にライセンスの詳細を示します。

| 機能 | オプション | NETSCALERライセンス |
| --- | --- | --- |
| **アプリケーション** | アプリケーションダッシュボード | アプリケーションダッシュボードのNetScaler Web App Firewall関連情報には、Premium (または) Advanced |

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

| 機能 | オプション | NETSCALERライセンス |
| --- | --- | --- |
| | | with App Firewallライセンスが必要です。 |
| | ウェブインサイト | 該当なし |
| | サービスグラフ | 該当なし |
| | 構成 > StyleBooks | 該当なし |
| **セキュリティ** | セキュリティダッシュボード | セキュリティダッシュボード上のNetScaler Web App Firewall関連情報には、Premium (または) Advanced with App Firewallライセンスが必要です。 |
| | セキュリティ違反 | Premium (または) Advanced with App Firewallライセンス |
| | ユーザーとエンドポイント | NA |
| **ゲートウェイ** | HDX インサイト | Advanced (レポート作成 < 1 時間) Premium (レポート作成 = 無制限) |
| | ゲートウェイ インサイト | Advanced (レポート作成 < 1 時間) Premium (レポート作成 = 無制限) |
| **インフラストラクチャ** | インフラストラクチャ分析 | NA |
| | インスタンス | NA |
| | SSLダッシュボード | NA |
| | イベント | NA |
| | ネットワーク機能 | NA |
| | ネットワークレポート | NA |
| | プールライセンス | NA |

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

| 機能 | オプション | NETSCALERライセンス |
| --- | --- | --- |
| | 構成 > 構成ジョブ、構成テンプレート、構成アドバイス | NA |
| | アップグレードジョブ | NA |
| | オーケストレーション | NA |
| **設定** | RBACと外部認証 (インスタンスレベル) | NA |
| | RBACと外部認証 | NA |

*NetScaler ConsoleサポートとのCitrix Director統合の場合、Citrix DirectorはPremiumライセンスを持っている必要があります。

## 高可用性

NetScaler Consoleサーバーには、VIP、CICO、およびプールされたキャパシティライセンスを含めることができます。ライセンスがNetScaler Consoleサーバーに発行されると、ライセンスはそのサーバーのホストIDにバインドされます。別のNetScaler Consoleサーバーにライセンスを割り当てることは制限されています。

NetScaler Consoleの高可用性ペアをライセンスサーバーとして構成した場合、プライマリに適用されたライセンスファイルはセカンダリに同期されます。

**注：**

- リリース12.1-50.x以降では、NetScaler Consoleライセンスはプライマリからセカンダリノードに自動的に同期されます。

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

# システム要件

NetScaler Console をインストールする前に、ソフトウェア要件、ブラウザ要件、ポート情報、ライセンス情報、および制限事項を理解しておく必要があります。

## NetScaler Console の要件

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| | **注:** NetScaler Console の展開には、ソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。 |
| ストレージ容量 | 必要なデフォルトのストレージ容量は 120 GB です。実際のストレージ要件は、NetScaler Console のサイジング見積もりによって異なります。 |
| | NetScaler Console のストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。追加できるディスクは 1 つだけです。 |
| | 初期展開時にストレージを見積もり、追加のディスクを接続することをお勧めします。 |
| | 詳細については、「NetScaler Console に追加ディスクを接続する方法」を参照してください。 |
| 仮想ネットワークインターフェース | 1 |
| スループット | 1 Gbpsまたは100 Mbps |

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

# NetScaler Consoleオンプレミスエージェントの要件

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| ストレージ容量 | 30 GB |
| 仮想ネットワークインターフェース | 1 |
| スループット | 1 ギガビット/秒 |

**注**

AMDプロセッサは以下でサポートされています。

- **NetScaler Console 13.1 ビルド 4.43 以降。**
- **NetScaler agent 13.1 build 17.42以降。**

# NetScaler Consoleの機能に必要なNetScalerの最小バージョン

**重要**

NetScaler Consoleのバージョンとビルドは、NetScalerのバージョンとビルドと**同等かそれ以降**である必要があります。たとえば、NetScaler Console 12.1 Build 50.39をインストールしている場合、NetScaler 12.1 Build 50.28/50.31以前がインストールされていることを確認してください。

| NETSCALER CONSOLEの機能 | NETSCALERソフトウェアバージョン |
| --- | --- |
| StyleBooks | 10.5以降 |
| OpenStack/CloudStackのサポート | 11.0以降（パーティションが必要な場合） |
| | 共有仮想LAN上のパーティションが必要な場合は、11.1以降 |

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

| NETSCALER CONSOLEの機能 | NETSCALERソフトウェアバージョン |
|---|---|
| NSXサポート | 11.1ビルド47.14以降 (VPX) |
| Mesos/Marathonサポート | 10.5以降 |
| バックアップ/復元 | NetScalerの場合、10.1以降 |
| | NetScaler SDXの場合、11.0以降 |
| 監視/レポートおよびジョブを使用した構成 | 10.1以降 |
| **分析機能** | |
| ウェブインサイト | 10.5以降 |
| HDXインサイト | 10.1以降 |
| WAFセキュリティ違反 | 11.0.65.31以降 |
| ゲートウェイインサイト | 11.0.65.31以降 |
| キャッシュインサイト | 10.5以降* |
| SSLインサイト | 12.0以降 |

* 統合キャッシュメトリクスは、バージョン11.0ビルド66.xを実行しているNetScalerインスタンスではNetScaler Consoleでサポートされていません。

# NetScaler Consoleアナリティクスの要件

## NetScaler Console機能に必要なCitrix Virtual Apps and Desktopsの最小バージョン

| NETSCALER CONSOLE機能 | シトリックス バーチャル アプリケーションズ アンド デスクトップ バージョン |
|---|---|
| HDXインサイト | シトリックス バーチャル アプリケーションズ アンド デスクトップ 7.0 以降 |

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

**注**

NetScaler Gateway機能 (バージョン9.3および10.xではAccess Gateway Enterpriseとしてブランド化されています) がNetScalerインスタンスで利用可能である必要があります。
NetScaler Consoleは、スタンドアロンのAccess Gateway Standardアプライアンスをサポートしていません。

NetScaler Consoleは、Citrix Virtual AppsまたはCitrix Virtual Desktopsで公開され、Citrix Workspaceを介してアクセスされるアプリケーションのレポートを生成できます。ただし、この機能はWorkspaceがインストールされているオペレーティングシステムに依存します。現在、NetScalerは、iOSまたはAndroidオペレーティングシステムで実行されているCitrix Workspaceを介してアクセスされるアプリケーションまたはデスクトップのICAトラフィックを解析しません。

## HDX™ Insightでサポートされているシンクライアント

- Dell Wyse Windowsベースのシンクライアント
- Dell Wyse Linuxベースのシンクライアント
- Dell Wyse ThinOSベースのシンクライアント
- 10ZiG Ubuntuベースのシンクライアント
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

## HDX Insightに必要なNetScalerインスタンスライセンス

NetScaler ConsoleがHDX Insight用に収集するデータは、監視対象のNetScalerインスタンスのバージョンとライセンスによって異なります。HDX Insightレポートは、リリース10.5以降を実行しているNetScaler PremiumおよびAdvancedアプライアンスでのみ表示されます。

| NETSCALER Rライセンス/期間 | 5分 | 1時間 | 1 日 | 1 週間 | > 1 か月 |
|---|---|---|---|---|---|
| 標準 | いいえ | いいえ | いいえ | いいえ | いいえ |
| 高度 | はい | はい | いいえ | いいえ | いいえ |
| プレミアム | はい | はい | はい | はい | はい |

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

# サポートされているハイパーバイザー

次の表に、NetScaler Console でサポートされているハイパーバイザーを示します。

| ハイパーバイザー | バージョン |
| --- | --- |
| XenServer | 7.1、7.4、および 8.0 |
| ヴイエムウェア ESX | 6.0、6.5、6.7、7.0、8.0 (14.1-21.x 以降)、および 8.0.2b (14.1-25.x 以降) |
| マイクロソフト Hyper-V | 2012 R2、2016、2019、および2022 |
| 汎用KVM | RHEL 7.4、RHEL 8.0、Ubuntu 16.04、および Ubuntu 18.04 |
| Nutanix ハイパーバイザー (AHV) | 6.5.2 (14.1-38.x以降) |

# サポートされているオペレーティングシステムとWorkspaceのバージョン

次の表に、NetScaler Consoleでサポートされているオペレーティングシステムと、各システムで現在サポートされているCitrix Workspaceのバージョンを示します。

| オペレーティングシステム | WORKSPACEのバージョン |
| --- | --- |
| Windows | 4.0 スタンダードエディション |
| Linux | 13.0.265571以降 |
| Mac | 11.8、ビルド238301以降 |
| HTML5 | 1.5 |
| Chrome アプリ | 1.5 |

# 対応ブラウザ

次の表に、NetScaler Console でサポートされている Web ブラウザを示します。

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

| WEB ブラウザ | バージョン |
| --- | --- |
| マイクロソフトエッジ | 79 以降 |
| グーグルクローム | 51 以降 |
| サファリ | 10 以降 |
| モジラファイアフォックス | 52以降 |

# 対応ポート

NetScaler Console は、NetScaler と通信するために NetScaler IP (NSIPとして知られる) アドレスを使用します。NetScaler インスタンスと NetScaler Console の間の仲介役としてエージェントを使用できます。これらのサーバーとの通信を確立するには、必要なポートを開きます。

- NetScaler から NetScaler Console への AppFlow およびログストリーム通信には、サブネット IP アドレス (SNIPとして知られる) が使用されます。
- NetScaler から NetScaler Console へのライセンス関連の通信には、NSIP アドレスが使用されます。
- SNIP アドレスが管理アクセス用に有効になっており、NetScaler Console に SNIP アドレスを使用して NetScaler が追加されている場合、イベントおよび Syslog の送信元 IP アドレスとして SNIP アドレスが使用されます。

**注**

NetScaler を高可用性モードで構成している場合、NetScaler Console は NetScaler と通信するために NSIP を使用し、必要なポートは同じままです。

**エージェントレス展開のネットワークポート図:**

**NetScaler® エージェントを含む展開のネットワークポート図:**

**NetScaler Console 高可用性展開のネットワークポート図:**

2つの NetScaler Console サーバーが 高可用性モード で設定されている場合、インスタンスを追加する際:

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

- NetScaler Console は、プライマリ IP アドレスを介して NetScaler と通信します。
- NetScaler は、NetScaler Console のフローティング IP アドレスを介して NetScaler Console との接続を確立します。これは、NetScaler がすべての SNMP、Syslog、および Analytics トラフィックを NetScaler Console のフローティング IP アドレスに転送することを意味します。

以下のセクションでは、必要なポートとその目的について説明します。

- NetScaler Console サーバー
- NetScaler エージェント
- NetScaler インスタンス
- 外部サーバー

## NetScaler Console サーバーのポート

次の表は、NetScaler Console サーバーで開いている必要があるポートについて説明しています。

| ポート | タイプ | 詳細 | 通信方向 |
|---|---|---|---|
| 80/443/5454/22 | TCP | 高可用性モードの NetScaler Console ノード間の通信およびデータベース同期のデフォルトポート。**注:** このポートはNetScalerテレメトリにも使用されます。 | NetScaler Consoleプライマリノードから NetScaler Consoleセカンダリノード |
| 443/8443/7443 | TCP | NetScalerエージェントとNetScaler Console間の通信用ポート。 | NetScalerエージェントがNetScaler Consoleとの通信を開始します。その後、NetScaler Consoleとエージェントは相互にやり取りします。 |
| 27000 および 7279 | TCP | NetScaler Consoleライセンスサーバーと NetScalerインスタンス間の通信用ライセンスポート。これら | NetScaler から NetScaler Console まで |

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

| ポート | タイプ | 詳細 | 通信方向 |
| --- | --- | --- | --- |
| | | のポートは、NetScalerプールライセンスにも使用されます。 | |
| 5005 | UDP | HAノード間でハートビートを交換するためのポート。 | NetScaler Consoleプライマリノードからセカンダリノード。NetScaler Consoleセカンダリノードからプライマリノード。 |
| 5140 | UDP | NetScaler Gatewayテレメトリデータを受信するためのポート。 | NetScaler から NetScaler Console |

NetScaler Console と NetScaler インスタンスが通信にエージェントを使用しない場合は、NetScaler Console サーバーで次のポートを開きます。

| ポート | タイプ | 詳細 | 通信の方向 |
| --- | --- | --- | --- |
| 80/443 | TCP | NetScaler Console から NetScaler インスタンスへの NITRO 通信のため。 | NetScaler エージェントから NetScaler へ、および NetScaler から NetScaler エージェントへ |
| 4739 | UDP | NetScaler インスタンスから NetScaler Console への AppFlow 通信のため。 | NetScalerから NetScalerエージェントへ |
| 162 | UDP | NetScalerインスタンスからNetScaler ConsoleにSNMPイベントを受信するため。 | NetScalerから NetScalerエージェントへ |

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

| ポート | タイプ | 詳細 | 通信の方向 |
|---|---|---|---|
| 514 | UDP | NetScalerインスタンスからNetScaler Consoleにsyslogメッセージを受信するため。 | NetScalerからNetScalerエージェントへ |
| 5557/5558 | TCP | NetScalerからNetScaler Consoleへのログストリーム通信（WAFセキュリティ違反、Web Insight、HDX Insight用）。 | NetScaler からNetScaler Consoleへ |
| 5563 | TCP | NetScalerインスタンスからNetScaler Consoleへ、NetScalerメトリック（カウンター）、システムイベント、および監査ログメッセージを受信するため | NetScaler からNetScaler Console |

## エージェント用ポート

次の表は、エージェントで開いている必要があるポートについて説明しています。

| ポート | タイプ | 詳細 | 通信方向 |
|---|---|---|---|
| 80/443 | TCP | NetScaler ConsoleからNetScalerインスタンスへのNITRO通信用。 | NetScalerエージェントからNetScalerへ、およびNetScalerからNetScalerエージェントへ |
| 4739 | UDP | NetScalerインスタンスからNetScaler ConsoleへのAppFlow通信用。 | NetScalerからNetScalerエージェント |

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

| ポート | タイプ | 詳細 | 通信方向 |
| --- | --- | --- | --- |
| 162 | UDP | NetScalerインスタンスからNetScaler ConsoleへSNMPイベントを受信するため。 | NetScalerからNetScalerエージェント |
| 514 | UDP | NetScalerインスタンスからNetScaler Consoleへsyslogメッセージを受信するため。 | NetScalerからNetScalerエージェント |
| 5557/5558 | TCP | NetScalerからNetScaler Consoleへのログストリーム通信用（WAFセキュリティ違反、Web Insight、HDX Insight用）。 | ネットスケーラーからネットスケーラーコンソールへ |

## NetScalerインスタンス用ポート

次の表に、NetScalerインスタンスで開いておく必要があるポートを示します。

| ポート | タイプ | 詳細 | 通信の方向 |
| --- | --- | --- | --- |
| 80/443 | TCP | NetScaler ConsoleからNetScalerインスタンスへのNITRO通信用。高可用性モードで展開されたNetScaler Consoleサーバー間のNITRO通信用。 | NetScaler ConsoleからNetScalerへ、およびNetScalerからNetScaler Consoleへ |
| 22 | TCP | NetScaler ConsoleからNetScalerインスタンスへのSSH通信用。高可用性モードで展開されたNetScaler Console | NetScaler ConsoleからNetScalerへ。または、NetScalerエージェントからNetScalerへ。 |

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

| ポート | タイプ | 詳細 | 通信の方向 |
| --- | --- | --- | --- |
| | | サーバー間の同期用。また、このポートはNetScaler Consoleエージェントと NetScaler間のSSH通信に必要です。 | |
| 予約済みポートなし | ICMP | NetScaler Consoleと NetScalerインスタンス間、または高可用性モードで展開されたセカンダリ NetScaler Console サーバー間のネットワーク到達性を検出するため。 | NetScaler Console から NetScaler |
| 161 | UDP | NetScaler インスタンスからイベントをポーリングするため。 | NetScaler Console から NetScaler |

## NetScaler 組み込みエージェント用のポート

次の表は、NetScaler 組み込みエージェントで開いておく必要があるポートについて説明しています。

| ポート | タイプ | 詳細 | 通信方向 |
| --- | --- | --- | --- |
| 443 | TCP | NetScaler Console から NetScaler 組み込みエージェントへのすべての通信用 | NetScaler Console から NetScaler 組み込みエージェント、および NetScaler 組み込みエージェントから NetScaler Console |

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

**注:**

NetScaler Consoleの高可用性展開では、NetScaler Consoleからのすべての通信はプライマリノードのIPアドレスを使用します。

## 外部サーバー用ポート

次の表は、外部サーバーで開いている必要があるポートについて説明します。

| ポート | タイプ | 詳細 | 通信方向 |
|---|---|---|---|
| 25 | TCP | NetScaler Consoleからユーザーへ SMTP通知を送信するため。 | NetScaler Consoleからユーザーへ。 |
| 389/636 | TCP | 認証プロトコルのデフォルトポート。NetScaler ConsoleとLDAP外部認証サーバー間の通信用。 | NetScaler Console と LDAP 外部認証サーバー間 |
| 123 | UDP | 複数のタイムソースと同期するためのデフォルトのNTPサーバーポート。 | NetScaler Console と NTP サーバー間 |
| 1812 | RADIUS | 認証プロトコルのデフォルトポート。NetScaler Console と RADIUS 外部認証サーバー間の通信用。 | NetScaler Console と RADIUS 外部認証サーバー間 |
| 49 | TACACS | 認証プロトコルのデフォルトポート。NetScaler Console と TACACS 外部認証サーバー間の通信用。 | NetScaler Console と TACACS 外部認証サーバー間 |

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

## 制限事項

NetScaler ADM 12.1 以降では、IPアドレスのIPv6形式がサポートされています。IPv6を設定するには、**設定 > 管理** に移動し、**ネットワーク構成** の下にある **IPアドレス、セカンドNIC、ホスト名、およびプロキシサーバー** を選択し、**IPv6** を有効にし、IPv6構成の詳細を入力して、**保存** をクリックします。

以下の表は、IPv6でサポートされている機能とサポートされていない機能のリストを示しています。

| IPV6でサポートされている機能 | IPV6でサポートされていない機能 |
|---|---|
| NetScaler ADM GUIの管理アクセス | 高可用性フローティングIP |
| NetScalerの管理アクセス | IPv6をサポートするADCから受信したSyslog |
| 登録とインベントリ | IPv6をサポートするADC上のStyleBook |
| ネットワークダッシュボード | アナリティクス |
| SSLダッシュボード | プールライセンス |
| 構成ジョブ | |
| 構成監査 | |
| ネットワーク機能 | |
| ネットワークレポート | |
| ADCインスタンスのバックアップと復元 | |
| NetScalerインスタンスからのSNMPイベント | |

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

# はじめに

このドキュメントでは、NetScaler Console をオンプレミスに初めて展開してセットアップする手順について説明します。このドキュメントは、Citrix ネットワークデバイス（NetScaler および NetScaler Gateway）を管理するネットワーク管理者およびアプリケーション管理者を対象としています。NetScaler Console を使用して管理するデバイスの種類に関係なく、このドキュメントの手順に従ってください。

NetScaler Console の既存ユーザーである場合は、サーバーを最新リリースの NetScaler Console に(/ja-jp/netscaler-application-delivery-management-software/current-release/upgrade.html)する前に、リリースノート、システム要件、およびライセンスの詳細を確認することをお勧めします。

## ステップ 1 - システム要件の確認

データセンターに NetScaler Console を展開する前に、ソフトウェア要件、ブラウザ要件、ポート情報、ライセンス情報、および制限事項を確認してください。

- **ライセンス情報**。ライセンスなしで任意の数のインスタンスとエンティティを追加できます。ただし、ライセンスを適用しない場合、分析情報を表示できる仮想サーバーは2つのみです。2つを超える仮想サーバーの分析を表示するには、適切なライセンスを購入する必要があります。詳細はこちら。
- **オペレーティングシステムとレシーバーの要件**。サポートされているオペレーティングシステムに適切なレシーバーバージョンがあることを確認するために、この情報を確認してください。詳細はこちら。
- **ブラウザの要件**。NetScaler Console GUI にアクセスするには、必要なブラウザと正しいバージョンがあることを確認する必要があります。詳細はこちら。
- **ポート**。NetScaler Console が NetScaler インスタンスと通信するために必要なポートが開いていることを確認してください。詳細はこちら。
- **NetScaler インスタンスの要件**。NetScaler Console のさまざまな機能は、異なる NetScaler ソフトウェアバージョンでサポートされています。NetScaler インスタンスが正しいバージョンにアップグレードされていることを確認するために、この情報を確認してください。詳細はこちら。

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

# ステップ 2 - NetScaler Console の展開

アプリケーションとネットワークインフラストラクチャを管理および監視するには、まずいずれかのハイパーバイザーに NetScaler Console をインストールする必要があります。NetScaler Console は、シングルサーバーとして、または高可用性モードで展開できます。NetScaler Insight Center を使用している場合は、NetScaler Console に移行して、分析機能に加えて、管理、監視、オーケストレーション、およびアプリケーション管理の機能を利用できます。

- **シングルサーバー展開**。NetScaler Console のシングルサーバー展開では、データベースがサーバーと統合され、単一のサーバーがすべてのトラフィックを処理します。NetScaler Console は、Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、および Linux KVM で展開できます。以下を参照してください。
  - Citrix Hypervisor を使用した NetScaler Console
  - Microsoft Hyper-V を使用した NetScaler Console
  - VMware ESXiと連携したNetScaler Console
  - Linux KVMサーバーと連携したNetScaler Console
- **高可用性展開。** 2つのNetScaler Consoleサーバーの高可用性展開 (HA) は、中断のない運用を提供します。高可用性セットアップでは、両方のNetScaler Consoleノードをアクティブ/パッシブモードで、同じサブネット上に同じソフトウェアバージョンとビルドを使用して展開し、同じ構成にする必要があります。HA展開では、NetScaler Consoleプライマリノードでフローティングアドレスを構成する機能により、個別のNetScalerロードバランサーが不要になります。詳細については、「[高可用性展開での構成。

  ```
  ](deploy/high-availability-deployment.md)」を参照してください。
  ```

# ステップ3 - NetScaler Consoleへのインスタンスの追加

NetScaler Consoleでは、オンプレミスまたはクラウドに展開されているすべてのNetScalerインスタンスを検出、管理、監視できます。これらのインスタンスを管理および監視するには、NetScaler Consoleサーバーにインスタンスを追加する必要があります。NetScaler Consoleには、次のインスタンスを追加できます。

- NetScaler
  - NetScaler MPX
  - NetScaler VPX

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

- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- ネットスケーラー ゲートウェイ

NetScaler Consoleサーバーにインスタンスを追加すると、サーバーは暗黙的にインスタンスと通信し、これらのインスタンスのインベントリを収集します。

詳細はこちら

## ステップ4 - 仮想サーバーでの分析の有効化

アプリケーショントラフィックフローの分析データを表示するには、特定のアプリケーションのトラフィックを受信する仮想サーバーで分析機能を有効にする必要があります。

詳細はこちら

## ステップ5 - NetScaler ConsoleでNTPサーバーを構成する

NetScaler Consoleのクロックを NTPサーバーと同期させるには、NetScaler ConsoleでNetwork Time Protocol (NTP) サーバーを構成する必要があります。NTPサーバーを構成することで、NetScaler Consoleのクロックがネットワーク上の他のサーバーと同じ日付と時刻の設定を持つことが保証されます。

詳細はこちら

## ステップ6 - NetScaler Consoleの最適なパフォーマンスのためのシステム設定を構成する

NetScaler Consoleを使用してインスタンスとアプリケーションの管理と監視を開始する前に、NetScaler Consoleサーバーの最適なパフォーマンスを確保するためのいくつかのシステム設定を構成することをお勧めします。

- **システムアラームを構成する**。システムアラームを構成して、重大または主要なシステム問題に確実に気づくようにします。たとえば、CPU使用率が高い場合や、サーバーへのログイン失敗が複数回発生した場合に通知を受けたい場合があります。
- **システム通知を構成する**。さまざまなシステム関連機能について、選択したユーザーグループに通知を送信できます。NetScaler Consoleで通知サーバーを設定し、電子メールおよびショートメッセージサービス (SMS) ゲートウェイサーバーを構成して、ユーザーに電子メー

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

ルおよびテキスト通知を送信できます。これにより、ユーザーログインやシステム再起動などのシステムレベルのアクティビティが通知されます。

- **システムパージ設定を構成する**。NetScaler Consoleサーバーのデータベースに保存されるレポートデータの量を制限するために、NetScaler Consoleがネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと (00:00) にパージされます。
- **システムバックアップ設定を構成する**。NetScaler Consoleは、毎日00:30にシステムを自動的にバックアップします。デフォルトでは、3つのバックアップファイルが保存されます。システムのバックアップ数を増やしたい場合があります。
- **インスタンスバックアップ設定を構成する**。NetScalerインスタンスの現在の状態をバックアップすると、インスタンスが不安定になった場合にバックアップファイルを使用して安定性を復元できます。これは、アップグレードを実行する前に特に重要です。デフォルトでは、12時間ごとにバックアップが取得され、3つのバックアップファイルがシステムに保持されます。
- **インスタンスイベントパージ設定を構成する**。NetScaler Consoleサーバーのデータベースに保存されるイベントメッセージデータの量を制限するために、NetScaler Consoleがネットワークレポートデータ、イベント、監査ログ、およびタスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと (00:00) にパージされます。
- **インスタンスsyslogパージ設定を構成する**。データベースに保存されるsyslogデータの量を制限するために、syslogデータをパージする間隔を指定できます。NetScaler Consoleから次のsyslogデータが削除されるまでの日数を指定できます。
  - 一般的なSyslogデータ
  - AppFirewall データ
  - NetScaler Gateway データ。

  詳細はこちら

# 次のステップ

NetScaler Console を展開して設定したら、インスタンスとアプリケーションの管理と監視を開始できます。

**NetScaler インスタンスとアプリケーションの管理。** すべての NetScaler Console 機能は NetScaler インスタンスでサポートされています。いずれかの機能の使用を開始できます。

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

# 強化されたグラフィカルユーザーインターフェイス

NetScaler Consoleのグラフィカルユーザーインターフェイス (GUI) は、いくつかの主要な機能により、豊かなエクスペリエンスを提供します。これらの機能は以下を提供します。

- **最適化された画面スペース:** ユーザーは好みに応じてサイドバーを表示または非表示にできます。
- **お気に入りへのクイックアクセス:** 頻繁に使用するメニュー項目をピン留めして、より迅速なナビゲーションを実現します。
- **サブメニューの視認性の向上:** メニュー項目にカーソルを合わせるとサブメニューが表示され、利用可能なすべてのオプションがより明確に表示されます。
- **サブメニュー構造の改善:** 一貫した3レベルのサブメニューシステムにより、NetScaler Console全体でシームレスなナビゲーションが保証され、統一されたエクスペリエンスが提供されます。

このページでは、NetScaler Console GUIの機能について説明し、豊かなユーザーエクスペリエンスを提供します。

## ホバーで表示するメニュー

以前は、セカンダリレベルのサブメニューはツリー構造で表示されていました。NetScaler Console GUIは、ホバー時にセカンダリメニューが表示され、サブメニューが明らかになるシームレスなナビゲーションを提供します。このナビゲーションにより、スクロールすることなくすべてのサブメニューオプションが表示され、表示エクスペリエンスが向上します。



## 合理化されたメニュー階層

メニュー階層は最大3レベルに合理化されています。以前は3レベルを超えて表示されていたサブメニューは、3レベルに配置されるようになりました。以下のナビゲーションが更新されました。

- **インフラストラクチャ > 構成**
- **NetScaler® ライセンス > プールライセンス**

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

- **ゲートウェイ > HDX™ Insight**

## 更新されたサブメニューラベル

このナビゲーションアプローチに合わせて、一部のサブメニュー名が変更されました。画面ナビゲーションの変更とサブメニューラベルの更新は次のとおりです。

### インフラストラクチャ > 構成

構成ノードの変更(/en-us/netscaler-application-delivery-management-software/media/configuration-node-changes.png)

| 以前の画面ナビゲーション | 変更された画面ナビゲーション | サブメニューラベルに変更はありますか？ |
|---|---|---|
| **構成 > 構成ジョブ > ジョブ** | **構成 > 構成ジョブ** | はい |
| **構成 > 構成ジョブ > 構成テンプレート** | **構成 > 構成テンプレート** | いいえ |
| **構成 > 構成監査 > 概要** | **構成 > 構成監査** | はい |
| **構成 > 構成監査 > 監査テンプレート** | **構成 > 監査テンプレート** | いいえ |
| **構成 > 構成監査 > 構成アドバイス** | **構成 > 構成アドバイス** | いいえ |

### NetScalerライセンス > プールライセンス

ライセンスノードの変更(/en-us/netscaler-application-delivery-management-software/media/licensing-node-changes.png)

| 以前の画面ナビゲーション | 変更された画面ナビゲーション | サブメニューラベルに変更はありますか？ |
|---|---|---|
| **プールライセンス > スループット容量ライセンス > スループット容量** | **プールライセンス > スループット容量** | いいえ |
| **プール型ライセンス > スループット容量ライセンス > CPXライセンス** | **プール型ライセンス > CPXライセンス** | いいえ |

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

| 以前の画面ナビゲーション | 変更された画面ナビゲーション | サブメニューラベルに変更はありますか？ |
|---|---|---|
| プール型ライセンス > スループット容量ライセンス > CICO | プール型ライセンス > CICO | いいえ |
| プール型ライセンス > スループット容量ライセンス > FIPSインスタンス | プール型ライセンス > FIPSインスタンス | いいえ |
| プール型ライセンス > セルフマネージド > ライセンス有効期限情報 | プール型ライセンス > セルフマネージド有効期限情報 | はい |
| プール型ライセンス > セルフマネージド > スループット容量ライセンス > セルフマネージドプール | プール型ライセンス > セルフマネージドスループット | はい |
| プールライセンス > 自己管理 > 自己管理VCPU | プールライセンス > 自己管理VCPU | いいえ |

### ゲートウェイ > HDX Insight

| 以前の画面ナビゲーション | 変更された画面ナビゲーション | サブメニューラベルに変更はありますか？ |
|---|---|---|
| HDX Insight > ライセンス > SSL VPNライセンス | HDX Insight > ライセンス | はい |

### 設定

サブメニューのラベルまたは名前の変更を除き、**設定**の下にその他の変更はありません。

| 以前の画面ナビゲーション | 変更された画面ナビゲーション | サブメニューラベルに変更はありますか？ |
|---|---|---|
| 設定 > データストレージ管理 | 画面ナビゲーションに変更はありません。 | サブメニューラベルは「**設定 > データストレージ**」に変更されました。 |

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

# 折りたたみ可能なメニュー

アイコンをクリックすると、メニュー全体を折りたたんだり展開したりできます。

## 展開されたメニュー

ペイン内のアイコン「**>>**」をクリックして、メニュー全体を展開します。

展開されたメニュー(/en-us/netscaler-application-delivery-management-software/media/expanded-menu.png)

## 折りたたまれたメニュー

ペイン内の「**Collapse <<**」をクリックして、メニュー全体を折りたたみます。

折りたたまれたメニュー(/en-us/netscaler-application-delivery-management-software/media/collapsed-menu.png)

# サイドバーの切り替え

サイドバーの表示を切り替えることで、画面スペースを最適化できます。パンくずリストの切り替えボタンをクリックして、サイドバーを非表示または表示します。

## サイドバーを表示

サイドバーを表示(/en-us/netscaler-application-delivery-management-software/media/show-sidebar.png)

## サイドバーを非表示

このオプションは、サイドバーを非表示にすることで画面スペースを最適化します。 サイドバーを非表示(/en-us/netscaler-application-delivery-management-software/media/hide-sidebar.png)

# ホーム画面に設定

NetScaler Console GUIには、ページとして表示されるサブメニュー名の横にアイコンがあります。ホーム画面アイコンを使用すると、ランディングページを設定できます。このアイコンは、特定のページにいる場合にのみ表示されます。ページをホーム画面から削除するには、アイコンをもう一度クリックするだけです。 ホーム画面に設定(/en-us/netscaler-application-delivery-management-software/media/set-as-home-screen.png)

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

# お気に入りの項目をピン留め

**ピン留め**機能を使用すると、お気に入りの項目にすばやくアクセスできます。メニューまたはサブメニューをピン留めするには、その上にカーソルを合わせ、名前の横に表示されるピンアイコンをクリックします。 ピン留めされたメニューアイコン(/en-us/netscaler-application-delivery-management-software/media/pinned-menu-icon.png)

ピン留めされたメニューは、サイドバーの**PINNED**の下に表示され、簡単にアクセスできます。 ピン留めされたメニュー(/en-us/netscaler-application-delivery-management-software/media/pinned-menu.png)

# サービスに移行

**サービスに移行**オプションは、**ヘルプセンター**のサブメニューとして利用できるようになりました。以前は、ナビゲーションペインのオプションとして利用できました。これにより、適切なメニュー項目の下で利用可能なオプションが合理化されます。

サービスに移行(/en-us/netscaler-application-delivery-management-software/media/migrate-to-service.png)

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

# 展開

NetScaler Console を使用してアプリケーションとネットワークインフラストラクチャを管理および監視する前に、まずハイパーバイザーまたはKubernetesクラスターのいずれかにインストールする必要があります。NetScaler Console をハイパーバイザーに展開する場合、シングルサーバーとして、または高可用性モードで展開できます。高可用性モードは Kubernetes クラスターには適用されません。NetScaler Insight Center を使用している場合は、NetScaler Console に移行して、分析機能に加えて、管理、監視、オーケストレーション、およびアプリケーション管理機能を利用できます。

- **シングルサーバー展開**: ハイパーバイザーに展開されたスタンドアロンの NetScaler Console の場合、データベースはサーバーと統合されており、単一のサーバーがすべてのトラフィックを処理します。NetScaler Console は、Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、および Linux KVM で展開できます。参照:
  - シトリックス ハイパーバイザー上のネットスケーラー コンソール
  - マイクロソフト ハイパーV 上のネットスケーラー コンソール
  - Azure 上の NetScaler コンソール
  - VMware ESXi 上の NetScaler コンソール
  - Linux KVM サーバー上の NetScaler Console
  - Nutanix ハイパーバイザー (Acropolis) 上の NetScaler Console
  - Kubernetes クラスター上の NetScaler Console
- **高可用性 (HA) 展開**: 2つの NetScaler Console サーバーの HA 展開は、中断のない運用を提供します。HA セットアップでは、両方の NetScaler Console ノードは、同じソフトウェアバージョンとビルドを使用して同じサブネットにアクティブ/パッシブモードで展開され、同じ構成である必要があります。HA 展開では、NetScaler Console プライマリノードにフローティング IP アドレスを構成する機能により、個別の NetScaler ロードバランサーが不要になります。参照: 高可用性展開での構成。

  **注:**

  高可用性は、Kubernetes クラスターに展開された NetScaler Console には適用されません。

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

- **軽量展開**: NetScaler Console を プールまたはフレックスライセンス のみに使用する予定がある場合は、より低い仕様で展開できます。詳細については、前提条件 を参照してください。
- **NetScaler Insight Center から NetScaler Console への移行**: 既存の構成、設定、またはデータを失うことなく、NetScaler Insight Center の展開を NetScaler Console に移行できます。NetScaler Console を使用すると、NetScaler によって生成されたさまざまな分析を表示できるだけでなく、単一の統合コンソールからグローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングすることもできます。参照: NetScaler Insight Center から NetScaler Console への移行
- **NetScaler ConsoleをDirectorと統合する**: Directorは、ネットワーク分析とパフォーマンス管理のためにNetScaler Consoleと統合されます。参照: NetScaler ConsoleをDirectorと統合する

# NetScaler Consoleのインストール要件

NetScaler Consoleは、Microsoft HyperV、 VMware ESXi、Linux KVM、およびCitrix Hypervisor™ プラットフォーム用の仮想アプライアンスとしてダウンロードおよびインストールできます。NetScaler Consoleをインストールする前に、 ソフトウェア要件、ブラウザ要件、ポート 情報、ライセンス情報、およびこれらすべてのプラットフォームにおける制限事項を理解しておく必要があります。

NetScaler Consoleをインストールするための特定のプラットフォーム要件と詳細な手順については、以下のトピックを参照してください。

- Citrix Hypervisor 環境における NetScaler Console
- Microsoft HyperV 環境における NetScaler Console
- VMware ESXiを使用するNetScaler Console
- Linux KVMサーバーを使用するNetScaler Console

## NetScaler Consoleの一般要件

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| ストレージ容量 | Citrix は、NetScaler Console の展開にソリッドステートドライブ (SSD) テクノロジーを使用することを推奨しています。 |

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

| コンポーネント | 要件 |
| --- | --- |
| | 必要なデフォルトのストレージ容量は 120 GB です。実際のストレージ要件は、NetScaler Console のサイジング見積もりによって異なります。 |
| | NetScaler Console のストレージ要件が 120 GB を超える場合は、追加のディスクを接続する必要があります。 |
| | Citrix は、初期展開時にストレージを見積もり、追加のディスクを接続することを推奨しています。追加できるディスクは 1 つだけです。 |
| | 詳細については、「NetScaler Console に追加ディスクを接続する方法」を参照してください。 |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 ギガビーピーエス |

## プールまたはフレックスライセンス専用の軽量 NetScaler® Console

NetScaler Console は、プールまたはフレックスライセンス のみに、以下の低い仕様で使用できます。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 8 GB |
| 仮想CPU | 4 |
| ストレージ | 120 GB |

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

**注記:**

Citrix は、NetScaler Console VHD をローカルストレージにホストすることを推奨します。SAN のストレージデバイスにホストされている場合、NetScaler Console は期待どおりに動作しない可能性があります。したがって、SAN への NetScaler Console の展開はサポートされていません。

# Citrix Hypervisor 上で動作する NetScaler Console

Citrix Hypervisor (旧称 XenServer) に NetScaler Console をインストールするには、まず、NetScaler Console の .xva イメージファイルをローカルコンピューターにダウンロードする必要があります。NetScaler Console のインストールを実行するには、Citrix XenCenter を使用する必要があります。

**注:**

NetScaler Console は XenMotion をサポートしていません。

## 前提条件

NetScaler Console をインストールする前に、以下の要件が満たされていることを確認してください。

- Citrix Hypervisor バージョン 7.1 以降が、最小要件を満たすハードウェアにインストールされていること。
- XenCenter が、最小要件を満たす管理ワークステーションにインストールされていること。Citrix Hypervisor に NetScaler Console をインストールするには、XenCenter を使用する必要があります。
- NetScaler Console の .XVA イメージファイルをダウンロード済みであること。

## XenCenter® システム要件

XenCenter は Windows クライアントアプリケーションです。Citrix Hypervisor™ ホストと同じマシンでは実行できません。以下の表に、最小システム要件を示します。

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

| コンポーネント | 要件 |
| --- | --- |
| オペレーティングシステム | Windows 7、Windows Server 2003、または Windows 10 のいずれか |
| .NET フレームワーク | バージョン 2.0 以降 |
| CPU | 750 MHz (MHz)、推奨: 1 ギガヘルツ (GHz) 以上 |
| RAM | 1 GB、推奨: 2 GB |
| NIC | 100 メガビット/秒 (Mbps) 以上の NIC |

## NetScaler® Application Delivery Management のインストール

1. XVA イメージファイルを Citrix Hypervisor にインポートし、**Console** タブから初期ネットワーク構成オプションを設定します。

   

2. 必要な IP アドレスを指定したら、構成設定を保存します。
3. プロンプトが表示されたら、nsrecover/nsroot 資格情報を使用してログオンします。

   

   **注**

   ログイン後、初期ネットワーク設定を更新したい場合は、`networkconfig` と入力し、設定を更新して保存します。

4. シェルプロンプトでコマンド `/mps/deployment_type.py` を入力して、展開スクリプトを実行します。

   

5. 展開タイプとして **NetScaler Console Server** を選択します。何も選択しない場合、デフォルトでサーバーとして展開されます。

   

6. NetScaler Console をスタンドアロン展開として展開するには、**Yes** と入力します。
7. NetScaler Console サーバーを再起動するには、**Yes** と入力します。

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

**注**

NetScaler Console をインストールした後、初期設定は後で更新できます。

### 検証

サーバーのインストール後、WebブラウザにNetScaler ConsoleサーバーのIPアドレスを入力すると、GUIにアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報は nsroot/nsroot です。

ブラウザにNetScaler Console設定ユーティリティが表示されます。

## Microsoft Hyper-V 上の NetScaler コンソール

Microsoft Hyper-V に NetScaler Console をインストールするには、まず NetScaler Console イメージファイルをローカルコンピューターにダウンロードする必要があります。また、システムにハードウェア仮想化拡張機能が搭載されていることを確認し、CPU仮想化拡張機能が利用可能であることを確認してください。

### 前提条件

NetScaler Console 仮想アプライアンスをインストールする前に、以下の要件が満たされていることを確認してください。

- Microsoft Hyper-V バージョン 6.2 以降が、最小要件を満たすハードウェアにインストールされていること。
- 最小システム要件を満たす管理ワークステーションに Microsoft Hyper-V Manager がインストールされていること。
- NetScaler Console イメージファイルがダウンロード済みであること。

### Microsoft Hyper-V のシステム要件

Microsoft Hyper-V は Windows クライアントアプリケーションです。次の表に、最小システム要件を示します。

| コンポーネント | 要件 |
| --- | --- |
| オペレーティングシステム | ウィンドウズ サーバー 2012 R2 |
| .NET フレームワーク | バージョン 2.0 以降 |

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

| コンポーネント | 要件 |
| --- | --- |
| CPU | 750 MHz (MHz)、推奨: 1ギガヘルツ (GHz) 以上 |
| RAM | 1 GB、推奨: 2 GB |
| NIC | 100メガビット/秒 (Mbps) 以上のNIC |

## NetScaler® Application Delivery Managementのインストール

インストールできるNetScaler Consoleサーバーの数は、Hyper-Vサーバーで利用可能なメモリによって異なります。

**NetScaler Consoleをインストールするには:**

1. ワークステーションでHyper-Vマネージャー クライアントを起動します。
2. **アクション**メニューで、**仮想マシンのインポート**をクリックします。

   
3. Hyper-Vイメージをインポートし、次の操作を行います。
   a. 仮想マシンのインポートダイアログボックスの**フォルダーの場所**セクションで、NetScaler Console Hyper-Vイメージを保存したフォルダーを参照し、そのフォルダーを選択して**次へ**をクリックします。
   b. 仮想マシンの選択セクションで、適切な仮想マシン名を選択します。
   c. 「**インポートの種類を選択**」セクションで、「仮想マシンをコピーする（新しい一意のIDを作成する）」オプションを選択し、「次へ」をクリックします。
   d. 「**保存先の選択**」セクションで、仮想マシンファイルを保存するフォルダーを指定できます。

      **注**

      デフォルトでは、ウィザードは仮想マシンファイルをローカルホストのデフォルトのHyper-Vフォルダーにインポートします。

      
   e. 「**ストレージフォルダーの選択**」セクションで、仮想ハードディスクを保存する場所を選択し、「**次へ**」をクリックします。

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

f. 概要ペインで仮想マシンの詳細を確認し、「**完了**」をクリックします。



NetScaler Console Hyper-Vイメージが右ペインに表示されます。

4. NetScaler Console Hyper-Vイメージを右クリックし、「**設定**」をクリックします。
5. 表示されるダイアログボックスの左ペインで、「**ハードウェア**」\>「**VM_Bus ネットワークアダプター**」に移動し、右ペインの「ネットワーク」リストから適切なネットワークを選択します。



6. 「**適用**」をクリックし、「**OK**」をクリックします。
7. NetScaler Console Hyper-Vイメージを右クリックし、「**接続**」をクリックします。
8. コンソールウィンドウで、「**開始**」ボタンをクリックします。
9. 初期ネットワーク構成オプションを設定します。



10. 必要なIPアドレスを指定した後、構成設定を保存します。
11. プロンプトが表示されたら、nsrecover/nsrootの資格情報を使用してログオンします。



**注**

ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`と入力して構成を更新し、構成を保存します。

12. シェルプロンプトでコマンドを入力して、展開スクリプトを実行します。

```
deployment_type.py
```



13. 展開タイプとして**NetScaler Console Server**を選択します。オプションを選択しない場合、デフォルトではサーバーとして展開されます。



14. NetScaler Consoleをスタンドアロン展開として展開するには、**Yes**と入力します。
15. NetScaler Consoleサーバーを再起動するには、**Yes**と入力します。

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

**注**

NetScaler Consoleをインストールした後、初期構成設定は後で更新できます。

### 検証

サーバーがインストールされた後、ブラウザのアドレスバーにNetScaler ConsoleサーバーのIPアドレスを入力してGUIにアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報はnsroot/nsrootです。

ブラウザにNetScaler Console設定ユーティリティが表示されます。

## VMware ESXi 上の NetScaler コンソール

このドキュメントでは、VMware vSphereクライアントを使用して、VMware ESXiにNetScaler Console仮想アプライアンスをインストールする方法について説明します。

### 前提条件

仮想アプライアンスのインストールを開始する前に、次の要件を確認してください。

- サポートされているVMware ESXiバージョンをインストールします。サポートされているバージョンの一覧については、サポートされているハイパーバイザーを参照してください。
- 最小システム要件を満たす管理ワークステーションにVMware Clientをインストールします。
- NetScaler Consoleのセットアップファイルをダウンロードします。

注

- VMotionは、**NetScaler Console 13.0 Build 47.22以降**でのみサポートされています。vSphereの高可用性およびvSphere DRSセットアップを含む、ESXiハイパーバイザーに展開されたNetScaler Consoleサーバーの移行をスケジュールおよび自動化できます。
- NetScaler Console用VMware Toolsは、ソフトウェアビルドの一部として提供され、個別にアップグレードまたは変更することはできません。

### NetScaler Consoleをインストールするには

VMware ESXiにNetScaler Console仮想アプライアンスをインストールするには、次の手順に従います。

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

**注**

手順とスクリーンショットは、VMware ESXiバージョン6.0に基づいています。GUIは、他のESXiバージョンでは異なる場合があります。VMXNET3アダプターを備えたVMware ESXiバージョン7.0.1cビルド番号17325551は、**NetScaler Console 13.0 71.40以降**でサポートされています。バージョン固有の手順については、VMwareのドキュメントを参照してください。

1. ワークステーションでVMware vSphereクライアントを起動します。
2. 「**IPアドレス/名前**」テキストボックスに、接続するVMware ESXiサーバーのIPアドレスを入力します。
3. 「**ユーザー名**」と「**パスワード**」テキストボックスに管理者資格情報を入力し、「**ログイン**」をクリックします。
4. 「**ファイル**」メニューで、「**OVFテンプレートの展開**」をクリックします。
5. 「**OVFテンプレートの展開**」ダイアログボックスの「**ファイルまたはURLから展開**」で、.ovfファイルを選択し、「**次へ**」をクリックします。

   **注**

   「選択したホストではオペレーティングシステム識別子がサポートされていません。VMwareサーバーがFreeBSDオペレーティングシステムをサポートしているかどうかを確認してください。」という警告メッセージが表示された場合は、「**はい**」をクリックします。

6. 「**OVFテンプレートの詳細**」ページで、「**次へ**」をクリックします。
7. NetScaler Console仮想アプライアンスの名前を入力し、「**次へ**」をクリックします。
8. ディスクフォーマットを、シンプロビジョニング形式またはシックプロビジョニング形式のいずれかを選択して指定します。

   **注**

   **シックプロビジョニング形式**を選択することをお勧めします。

9. 「**完了**」をクリックしてインストールプロセスを開始します。

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

10. これで、NetScaler Console仮想アプライアンスを起動する準備ができました。
11. ナビゲーションペインで、インストールした仮想アプライアンスを選択します。「**インベントリ**」メニューから「**仮想マシン**」を右クリックし、「**仮想ハードウェアのアップグレード**」をクリックします。「**仮想マシンの確認**」ダイアログボックスで、「**はい**」をクリックします。

    「初期設定」(/en-us/netscaler-application-delivery-management-software/media/mas-install-esxi-3.png)
12. 「**Inventory**」メニューで「**Virtual Machine**」をクリックし、次に「**Edit Settings**」をクリックします。
13. 「**Virtual Machine Properties**」ダイアログボックスの「**Hardware**」タブで「**Memory**」をクリックし、右側のペインで「**Memory Size**」を32 GBに指定します。
14. 「**CPUs**」をクリックし、右側のペインでCPUを8に指定します。「**OK**」をクリックします。
15. 必要に応じて追加のディスクを追加します。

    「初期設定」(/en-us/netscaler-application-delivery-management-software/media/step15-vmware.png)
16. ナビゲーションペインで、インストールした仮想アプライアンスを選択します。「**Inventory**」メニューから「**Virtual Machine**」をクリックし、「**Power**」をクリックし、次に「**Power On**」をクリックします。
17. 「**Console**」タブをクリックして、NetScaler Consoleの初期ネットワーク構成オプションを表示します。

    「初期設定」(/en-us/netscaler-application-delivery-management-software/media/admha-initialconfig.png)
18. 必要なIPアドレスを指定したら、構成設定を保存します。
19. プロンプトが表示されたら、nsrecover/nsrootの資格情報を使用してログオンします。

    「初期設定」(/en-us/netscaler-application-delivery-management-software/media/nmas-deployment-changes.png)

    **注**

    ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`と入力して構成を更新し、構成を保存します。
20. シェルプロンプトでコマンドを入力して、展開スクリプトを実行します。

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

```
deployment_type.py
```

初期設定(/en-us/netscaler-application-delivery-management-software/media/ha-deploymenttype.png)

21. デプロイタイプを**NetScaler Console Server**として選択します。オプションを選択しない場合、デフォルトでサーバーとして展開されます。

    初期設定(/en-us/netscaler-application-delivery-management-software/media/ha-deploymentconfig.png)

22. NetScaler Consoleをスタンドアロン展開としてデプロイするには、「**Yes**」と入力します。
23. NetScaler Consoleサーバーを再起動するには、「**Yes**」と入力します。

**注**

NetScaler Consoleをインストールした後、後で初期設定を更新できます。

### 検証

サーバーのインストール後、ブラウザにNetScaler ConsoleサーバーのIPアドレスを入力してGUIにアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報はnsroot/nsrootです。

ブラウザにNetScaler Console構成ユーティリティが表示されます。

**注**

VMware ESXiでのNetScaler Consoleの一般的なインストール時間は約10分ですが、一部のシステムではさらに時間がかかる場合があります。

## VMware ESXi 上でのNetScaler® エージェントの展開を自動化

NetScaler Console を使用すると、VMware ESXi 上でのNetScaler エージェントの展開を自動化できます。

管理者として、次のアクションを自動化できます。

- NetScaler エージェントを構成する

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

- NetScaler エージェントを登録し、エージェントのデフォルトパスワードを変更します。

## NetScaler エージェントを構成する

エージェントの構成を自動化するには、.ovf ファイルに次のパラメータの値を追加します。

1. `IPAddress`
2. `Netmask`
3. `Gateway`
4. `Nameserver`
5. `Hostname`

**注:**

.ovf ファイルはエージェントイメージファイルに含まれています。NetScaler エージェントファイルをダウンロードするには、`<https://www.citrix.com/downloads/citrix-application-management/>` にアクセスしてください。エージェントイメージファイルの命名パターンは次のとおりです。**MASAGENT-ESX-releasenumber-buildnumber.zip**

## NetScaler エージェントを登録し、デフォルトパスワードを変更する

**注記:**

登録とデフォルトパスワードの変更を行う前に、NetScaler エージェントの構成で指定されているパラメータを追加したことを確認してください。

NetScaler エージェントの登録とデフォルトパスワードの変更を自動化するには、同じ .ovf ファイルで次のパラメータの値を追加します。

1. `NetScaler Console Server IP`
2. `NetScaler Console Username`
3. `NetScaler Console Password`
4. `Agent New Password`

## 前提条件

仮想アプライアンスのインストールを開始する前に、次のことを確認してください。

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

- 最小システム要件を満たす管理ワークステーションに VMware vSphere 8.x をインストールします。
- NetScaler Console セットアップファイルをダウンロードします。

## NetScaler エージェントを構成および登録する方法

1. .OVF ファイルをダウンロードして編集する
2. VMware ESXi に NetScaler Console 仮想アプライアンスをインストールする
3. 確認する

### ステップ1：.OVFファイルをダウンロードして編集する

1. **MASAGENT-ESX-releasenumber-buildnumber.zip**からファイルを目的の場所に抽出します。以下のファイルが抽出されます。
   - .ovfファイル
   - .vmdkファイル
   - .ovaファイル
   - .mfファイル
2. 任意のエディターで.ovfファイルを開き、次の`<ProductSection>..</ProductSection>`サンプルコードを追加します。`</VirtualHardwareSection>`タグの後に

```
<ProductSection>

<Info>Information about the installed software</Info>

<Product>Application Delivery management</Product>

<Vendor>Citrix</Vendor>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ip">

<Label>IPAddress</Label>

</Property>
```

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

```
<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.netmask">

<Label>Netmask</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.gateway">

<Label>Gateway</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.nameserver">

<Label>Nameserver</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.hostname">

<Label>Hostname</Label>

</Property>
```

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

```
<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ServerIP">

<Label>NetScaler Console Server IP</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ServerUname">

<Label>NetScaler Console Username</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

ovf:type="string" ovf:key="eth0.ServerPassword">

<Label>NetScaler Console Password</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

ovf:type="string" ovf:key="eth0.NewPassword">

<Label>Agent New Password</Label>

</Property>
```

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

```
</ProductSection>
```

3. 設定したいパラメーターについては、ovf:value="VALUE"に対応する値を追加します。

   - NetScalerエージェントを設定するには、以下のパラメーターに値を追加します。
     - `IPAddress`
     - `Netmask`
     - `Gateway`
     - `Nameserver`
     - `Hostname`
   - NetScalerエージェントを登録し、デフォルトのパスワードを変更するには、以下のパラメーターに値を追加します。
     - `NetScaler Console Server IP`
     - `NetScaler Console Username`
     - `NetScaler Console Password`
     - `Agent New Password`

   **注:**

   - エージェントを登録してデフォルトパスワードを変更する前に、NetScalerエージェントを設定する必要があります。
   - .ovfファイルでデフォルトパスワードを登録して変更しない場合は、VMの展開後にこれらのアクションを手動で実行してください。

4. パラメータとその値を追加したら、.ovfファイルを保存します。

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

## ステップ2：VMware ESXiにNetScaler Console仮想アプライアンスをインストールする

1. **VMWare vSphere Client**にログインし、管理者資格情報を入力します。**ログイン**をクリックします。



2. ESXiサーバーを選択し、右クリックして**OVFテンプレートの展開**を選択します。



3. **OVFテンプレートの展開**ページで:

   a. **OVFテンプレートの選択**: 「**ローカルファイル**」を選択し、編集した.ovfファイルと.vmdkファイルを保存した場所に移動します。ファイルを選択し、「**開く**」をクリックしてアップロードします。「**次へ**」をクリックします。



   b. **名前とフォルダーの選択**: 仮想アプライアンスの名前を追加し、仮想マシンを展開するESXi上の場所を選択します。「**次へ**」をクリックします。



   c. **コンピューティングリソースの選択**: テンプレートの展開後に実行するリソースを選択します。「**次へ**」をクリックします。



   d. **詳細の確認**: OVFテンプレートの詳細を確認します。「**次へ**」をクリックします。



   e. **ストレージの選択**: OVFテンプレートを保存するデータストアを選択します。「**次へ**」をクリックします。



   f. **ネットワークの選択**: デフォルト設定で続行します。「**次へ**」をクリックします。



   g. **テンプレートのカスタマイズ**: OVFテンプレートのすべてのプロパティを確認します。OVFファイルのダウンロードと編集セクションの.ovfファイルに追加したすべてのパラメーターと値が表示されます。



   h. **完了準備**: 設定を保存して展開プロセスを開始するには、「**完了**」をクリックします。



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

デプロイが完了するまで待ちます。**OVFテンプレートの展開**操作のステータスが100%完了すると、エージェントがデプロイされます。

**重要:**

設定を編集する前に、仮想アプライアンスの電源を入れないでください。

4. インストールした新しい仮想アプライアンスをクリックし、**Configure > Settings > vApp Options > Edit**に移動します。
5. **vAppオプションの編集**ウィンドウで、**OVFの詳細 > OVF環境トランスポート**に移動し、**VMware Tools**を選択します。**OK**をクリックします。
6. 仮想マシンを右クリックし、**パワーオン**をクリックします。または、仮想マシンの**サマリー**タブを選択し、**パワーオン**をクリックすることもできます。
7. **サマリー**タブで、**Webコンソールの起動**を選択します。 **コンソールの起動**ウィンドウで、**Webコンソール**を選択します。**起動**をクリックします。
8. コンソールに、NetScalerエージェントがNetScaler Consoleサーバーに登録された後、登録成功メッセージが表示されます。NetScalerエージェントがデプロイされ、デフォルトパスワードが変更されたことを確認するには、NetScalerエージェント のユーザー名と新しいパスワードでログインします。

## ステップ 3: 確認

NetScaler エージェントが展開されていることを確認するには:

1. NetScaler エージェントが展開されたら、ブラウザで NetScaler Console サーバーの IP アドレスを入力して NetScaler Console GUI にアクセスします。
2. 資格情報を使用してサーバーにログインします。
3. **Infrastructure > Instances > Agents** に移動します。 新しく展開されたエージェントが ESX プラットフォームに表示されます。

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

# KubernetesクラスターのNetScaler Console

KubernetesクラスターにNetScaler Console仮想アプライアンスをインストールする前に、前提条件のセクションをお読みください。

## 前提条件

NetScaler Consoleをインストールする前に、以下の前提条件が満たされていることを確認してください。

### Kubernetesクラスター

- Kubernetesクラスターは、以下のバージョン以降である必要があります。
  - サーバーバージョン v1.20
  - クライアントバージョン v1.20

  バージョンを確認するには、コマンド `kubectl version` を入力します。
- クラスターにインストールされているHelmアプリケーションは、クライアントバージョンv3.4.0以降である必要があります。

  バージョンを確認するには、コマンド `helm version` を使用します。
- KubernetesクラスターのCNI (Container Network Interface) は、Calicoバージョンv3.21.1以降である必要があります。
- クラスター内のすべての従属ノードには、NFSクライアントがインストールされている必要があります。これは、NetScaler Consoleアプリケーションが、ネットワークファイルサーバーにマウントされたボリュームにデータと構成を永続化するためです。Ubuntuベースの従属ノードにNFSクライアントをインストールするには、次のコマンドを入力します。

`apt-get update` `apt install nfs-common`

- NetScaler Consoleアプリケーションには、クラスター全体で32 GBのメモリと8つのvCPU、およびNFS上に120 GBのスペースが必要です。

### NFS共有

NetScaler Consoleアプリケーションは、構成、証明書、イメージなどのデータを保存するために永続ボリュームを必要とします。この目的のために、NetScaler ConsoleはNFSマウントを必要とします。アプリケーションは、共有ネットワークマウントから2つのフォルダーを必要とします。

- 証明書、イメージなどのファイルを保存するためのもの
- データベース用のもの

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

注

SSDを備えたNFSを使用することをお勧めします。

これら2つのフォルダーは異なっていても同じでも構いません。両方のフォルダーに777の権限が必要です。最初のフォルダーには最低10 GBの容量が必要です。2番目のフォルダーのサイズは、データベースに永続化する必要があるデータの量によって異なります。最小サイズは100 GBです。 本番環境では、本番グレードのNFSソリューションを使用することをお勧めします。

## NetScalerアプライアンス

NetScalerアプライアンスはイングレスデバイスとして必要です。NetScalerは、必要なアプリケーションサービスをKubernetesの外部で利用可能にします。 クラスター。NetScalerアプライアンスはKubernetesクラスターの外部にあり、ワーカーノードはNetScalerから到達可能である必要があります。次の手順を実行します。

- NetScalerでSNIPを構成します。NetScalerはこのSNIPを使用してKubernetesクラスターのワーカーノードに到達します。
- 必要なアプリケーションサービスをKubernetesクラスターの外部で利用可能にするために、仮想サーバーIPアドレスとして使用する空いているIPアドレスを特定します。

### KubernetesクラスターへのNetScaler Consoleのインストール

KubernetesクラスターにNetScaler Consoleアプライアンスをインストールするには、次の手順に従います。

1. NetScalerサイトにアクセスし、Kubernetes用NetScaler Console Helm Chartのファイルをダウンロードします。
2. ダウンロードしたHelm Chartのtarballを、Kubernetesクラスターのメインノードの/varディレクトリに抽出します。
3. `/var/citrixadm`ディレクトリの下にある`values.yaml`ファイルを開きます。
4. ファイル内の`dbpasswd`フィールドにデータベースのパスワードを入力します。
5. 次の値を変更します。NetScaler Consoleアプリケーションは、これらの値を使用してNetScalerアプライアンスを構成し、サービスが外部に公開されるようにします。
   - `ingressIP`: アプリケーションにアクセスするためにNetScalerで構成された仮想IP。
   - `applicationID`: NetScalerアプライアンス上の他の構成からイングレス構成を区別するための一意のID。

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

- `ingressADCIP`: NetScaler Consoleアプリケーションのイングレスとして使用されるNetScaler IPアドレス (NSIP)。
- `ingressADCUsername`: NetScalerアプライアンスにアクセスするためのユーザー名。このユーザーは書き込み権限を持っている必要があります。
- `ingressADCPassword`: ユーザー名のパスワード。



6. **storage**セクションで次の値を変更します。これらの値は、NetScaler Consoleアプリケーションに必要なファイルを保存するために必要な永続性を指定します。

   - `nfsServer`: NFSサーバーのホスト名またはIPアドレス
   - `path`: アプリケーションファイルを保存するフォルダーのマウントパス。
   - `size`: 少なくとも10 GB。

   注

   この値の単位はGiです。例: 10Gi、20Gi。

7. `pg-datastore` の下の **storage** セクションに移動し、次の値を変更します。これらの値は、データベースの作成に使用される永続性を指定します。

   - `nsfServer`: NFS サーバーのホスト名または IP アドレス。
   - `size`: データストアに使用されるフォルダーのマウントパス。
   - `path`: 100 GB 以上。

   注

   この値の単位は Gi です。例: 100Gi、200Gi。

8. メインノードの /var/citrix ディレクトリに移動し、NetScaler Console アプリケーションをインストールするために、次のコマンドを実行します。 `helm install -n citrixadm --namespace <name> ./citrixadm`

   注

   この helm コマンドは、helm バージョン 3.x ではサポートされていません。

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

このコマンドは、クラスターに必要なポッドもインストールします。名前空間引数はオプションです。名前空間が指定されていない場合、Helm は NetScaler Console をデフォルトの名前空間にインストールします。管理を容易にするために、NetScaler Console を別の名前空間にインストールしてください。

9. ブラウザを開いて `http://< virtual server IP address >` と入力し、`nsroot/nsroot` を資格情報として使用して NetScaler Console にログインします。セキュアアクセスには `https://< virtual server IP address >` と入力します。

注

展開中、NetScaler Console アプリケーションはデータストアにテーブルを作成しますが、これには時間がかかる場合があります。Kubernetes が NetScaler Console アプリケーションのさまざまなポッドに割り当てるリソースに応じて、サービスが起動するまでに 5 〜 15 分かかることがあります。

# Linux KVMサーバー上のNetScaler コンソール

NetScaler Consoleをプロビジョニングできる仮想化プラットフォームには、Linux-KVMが含まれます。

Linux-KVMにNetScaler Consoleをインストールする前に、システムにハードウェア仮想化拡張機能があること、およびCPU仮想化拡張機能が利用可能であることを確認してください。ハイパーバイザーで`virsh`（仮想マシンを管理するためのコマンドラインツール）が利用可能であることを確認してください。

管理者資格情報を使用してCitrix.comウェブサイトにログオンし、最新のNetScaler Consoleセットアップファイルにアクセスして、コンピューターにダウンロードします。その後、Linux-KVMプラットフォームにNetScaler Consoleをインストールし、ネットワーク用に構成します。

## 前提条件

NetScaler Console仮想アプライアンスをインストールする前に、Linux-KVMバージョン3.6.11-4以降が、最小要件を満たすハードウェアにインストールされていることを確認してください。

### ハードウェア要件

| コンポーネント | 要件 |
| --- | --- |
| CPU | Intel VT-Xプロセッサに含まれるハードウェア仮想化機能を備えた64ビットx86プロセッサ。 |

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

| コンポーネント | 要件 |
| --- | --- |
| | Linux-KVMをホストするために、少なくとも2つのCPUコアを提供します。**注** CPUがLinuxホストをサポートしているかどうかをテストするには、ホストLinuxシェルプロンプトで次のコマンドを入力します: `*. egrep'\^flags.* ( vmx \| svm ) '/proc/cpuinfo*`。拡張機能のBIOS設定が無効になっている場合は、BIOSで有効にする必要があります。プロセッサ速度に関する特定の推奨事項はありませんが、速度が速いほどNetScaler Consoleのパフォーマンスが向上します。 |
| メモリ (RAM) | ホストLinuxカーネル用に最低4 GB。VMが必要とする追加メモリを追加します。 |
| ハードディスク | ホストLinuxカーネルとVMの要件に必要なスペースを計算します。単一のNetScaler Console VMには120 GBのディスクスペースが必要です。 |

**注記**

指定されたメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮し、OpenStackプラットフォームにNetScaler Consoleを展開するためのものです。OpenStackのハードウェア要件は、その上で実行される仮想マシンの数によって異なります。

### ソフトウェア要件

3.6.11-4カーネルの64ビットバージョン以降など、より新しいカーネルを推奨します。

### ネットワーク要件

NetScaler Consoleは、virtIO準仮想化ネットワークインターフェイスを1つのみサポートしています。NetScaler ConsoleとLinux-KVMが通信できるように、このインターフェイスをLinux-KVMホストの管理ネットワークに接続してください。

## NetScaler Consoleセットアップファイルのダウンロード

`www.citrix.com`からNetScaler Consoleセットアップファイルをダウンロードするには：

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

1. Webブラウザを開き、アドレスバーにwww.citrix.comと入力します。
2. **サインイン**オプションにカーソルを合わせ、**マイアカウント**をクリックし、Citrixの資格情報を入力してから、もう一度**サインイン**をクリックします。
3. **ダウンロード**セクションに移動します。
4. **ダウンロード**リストから、**NetScaler® Application Delivery Management**を選択します。
5. **NetScaler Application Delivery Management**ページで、リリースを選択します。たとえば、**Release 13.0**を選択します。
6. **製品ソフトウェア**をクリックして展開し、最新のビルドをクリックします。たとえば、**NetScaler MAS Release (Feature Phase) 13.0 Build 36.27**を選択します。

   選択したビルドページが表示されます。
7. 「**ダウンロードにジャンプ**」リストで、「**KVM 用 NetScaler MAS イメージ、13.0 ビルド xx.xx**」を選択します。
8. 「**ファイルのダウンロード**」をクリックし、EULA に同意して、圧縮されたイメージファイルをローカルマシンの任意のフォルダーにダウンロードします。

## Linux-KVM への NetScaler Application Delivery Management のインストール

1. SSH を使用して KVM ホストにログオンします。
2. CLI プロンプトで、いずれかのファイル転送プログラムを使用して、イメージをサーバー上のフォルダーにコピーします。
3. ダウンロードしたイメージを保存したディレクトリに移動します。
4. コマンドラインで以下を実行します。

   a. ディレクトリ内のファイルを一覧表示し、イメージファイルの存在を確認します。

   b. tar コマンドを使用して NetScaler Application Delivery Management イメージファイルを解凍します。解凍されたパッケージには、次のコンポーネントが含まれています。

      i. NetScaler Console の属性を指定するドメイン XML ファイル

      ii. ドメインディスクイメージのチェックサムを指定するテキストファイル

      iii. ドメインディスクイメージ

```
tar -xvfz MAS-KVM.tgz

MAS-KVM.xml
```

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

```
MAS-KVM.qcow2

checksum.txt
```

ドメインディスクイメージ (/en-us/netscaler-application-delivery-management-software/media/netscaler-mas-linux-kvm-1.png)

iv. バックアップオプションとして、MAS-KVM.xml のコピーを MAS1-KVM.xml として作成します。vi エディターを使用して MAS1-KVM.xml ファイルを開きます。

v. 次のネットワーク属性について MAS1-KVM.xml を編集します。

   i. `name` - 名前を指定します。

   ii. `mac` - MACアドレスを指定します。

   iii. `source file` - 絶対ディスクイメージソースパスを指定します。ファイルパスは絶対パスである必要があります。

   > **注**
   >
   > ドメイン名とMACアドレスは一意である必要があります。

   iv. `mode` - モードを指定します。

   v. `model type` - virtIOに設定します。

   vi. `source dev` - インターフェイスを指定します。

```
<name> MAS1-KVM</name>

<mac address='52:54:00:29:74:b3'/>

<source file='/var/ MAS-KVM.qcow2'/>

<source dev='eth0' mode='bridge'/>

<model type='virtio'/>
```

vi. 次のコマンドを使用して、MAS1-KVM.xmlファイルでVM属性を定義します: `virsh define \<FileName\>.xml`

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

```
virsh define MAS-KVM.xml

Domain MAS defined from MAS-KVM.xml
```

vii. 次のコマンドを入力して、NetScaler Consoleを起動します: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS

Domain MAS started
```

viii. 次のコマンドを使用して、NetScaler Console仮想マシンに接続できます: `virsh console \<DomainName\>`

```
virsh console MAS

Connected to domain MAS

Escape character is ^]
```

## ネットスケーラー アプリケーション デリバリー マネジメント を構成する

**注**

一部のLinux KVMホストでは、複数のCPUを持つFreeBSDゲストが適切に再起動しない場合があります。NetScaler Console仮想アプライアンスが再起動されると、NetScaler ConsoleのCLIとGUIが応答しなくなります。詳細については、`<https://bugs.launchpad.net/qemu/+bug/1329956>`を参照してください。

NetScaler Console仮想アプライアンスの再起動時にNetScaler ConsoleのCLIとGUIが応答しなくなるのを避けるには、KVMホスト上のすべての仮想マシンをシャットダウンし、KVMホストで次の操作を実行します。

1. 次のコマンドを使用してkvm_intelモジュールを削除します。 `rmmod kvm\_intel`

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

2. **APICv**を無効にし、次のコマンドを使用してkvm_intelモジュールを再ロードします。
   `modprobe kvm\_intel enable\_apicv=N`
3. KVMホスト上の仮想マシンを起動します。

NetScaler Consoleをインストールした後、サービスが利用可能になるまで約10分間待ち、その後NetScaler Consoleにログオンします。

1. コマンドラインで、デフォルトのシステム管理者資格情報を使用してシステムにログオンします。
   - ユーザー名: `nsroot`
   - パスワード: `nsroot`

   **注**

   初めてログオンした後、管理者パスワードを変更します。その後、ネットワークで機能するようにMASを設定します。パスワードはNetScaler Consoleのユーザーインターフェイスから変更できます。NetScaler Consoleのホームページから、**Settings > User Administration > Users**に移動します。ユーザーを選択して**Edit**をクリックし、Passwordフィールドでパスワードを更新します。
2. プロンプトで、次のように入力します。*shell*
3. **networkconfig**と入力してNetScaler Consoleの初期ネットワーク構成メニューに入ります。管理IPアドレスを設定します。
4. NetScaler Consoleの初期ネットワーク構成を完了するには、プロンプトに従います。コンソールには、NetScaler Consoleの次のパラメータを設定するためのNetScaler Console初期ネットワーク構成オプションが表示されます。ホスト名はデフォルトで入力されています。
   a. 「**2**」を入力してNetScaler ConsoleのIPv4アドレスを更新します - NetScaler Consoleにアクセスする管理IPアドレス
   b. 「**3**」を入力してネットマスクを更新します - 管理IPアドレスに関連付けられたサブネットマスク
   c. 「**4**」を入力してゲートウェイIPv4アドレスを更新します - NetScaler Consoleの管理IPアドレスのサブネットのデフォルトゲートウェイIPアドレス
   d. 「**7**」を入力して保存して終了します - 設定変更を保存してシステムを終了します。

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

5. シェルプロンプトでコマンドを入力して展開スクリプトを実行します:
   `deployment_type.py`
6. 表示される展開画面で、展開タイプとして「**NetScaler Console server**」を選択します。

   
7. NetScaler Consoleをスタンドアロン展開として展開するには、「**Yes**」と入力します。
8. NetScaler Consoleサーバーを再起動するには、「**Yes**」と入力します。
9. NetScaler Consoleサーバーが再起動したら、コマンドラインまたはGUIからデフォルトの管理者資格情報nsroot/nsrootを使用してNetScaler Consoleにログオンします。

   後で、ブラウザのアドレスバーにNetScaler ConsoleサーバーのIPアドレスを入力してNetScaler Consoleにアクセスできます。サーバーにログオンするためのデフォルトの管理者資格情報は*nsroot/nsroot*です。

# NutanixハイパーバイザーでのNetScaler Console

**注:**

この機能は、リリース14.1-38.xx以降で利用可能です。

KVMソフトウェアイメージを使用して、Nutanixハイパーバイザー上にNetScaler® Consoleサーバーを構成できます。開始する前に、NetScaler Console用のVMを作成するようにNutanix Prismを構成していることを確認してください。

## ハードウェア要件

| コンポーネント | 要件 |
|---|---|
| CPU | Intel VT-Xプロセッサに含まれるハードウェア仮想化機能を備えた64ビットx86プロセッサ。Linux-KVMをホストするために、少なくとも8つのCPUコアを提供します。 |
| メモリ (RAM) | ホストLinuxカーネル用に最低4 GB。VMが必要とする追加メモリを追加します。 |

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

| コンポーネント | 要件 |
| --- | --- |
| ハードディスク | ホストLinuxカーネルとVMの要件に必要な領域を計算します。単一のNetScaler Console VMには120 GBのディスク領域が必要です。 |

## NetScaler Consoleセットアップファイルをダウンロードする

NetScaler Consoleセットアップファイルをダウンロードするには:

1. www.citrix.com/downloadsページにログオンします。
2. 製品リストから**NetScaler Console**を選択します。
3. **Release 14.1**の下で、14.1-38.x以降のビルドを選択します。

   選択したビルドページが表示されます。
4. **Jump to Download**リストで、**Citrix ADM image for KVM, 14.1 Build xx.xx**を選択します。
5. **Download File**をクリックし、EULAに同意して、圧縮イメージファイルをローカルマシンの任意のフォルダーにダウンロードします。

## NutanixハイパーバイザーでNetScaler Consoleを構成する

1. `.tgz`ファイルを解凍します。
2. Nutanix Prismにログオンします。
3. **Settings**に移動し、**Image Configuration**を選択します。

   a. イメージ名を指定します。

   b. イメージタイプとして**DISK**を選択します。

   c. ストレージコンテナを選択します。

   d. **Image Source**で、を選択し、`.qcow2`拡張子のファイルをアップロードします。

   e. **Save**をクリックします。

   アップロードして保存すると、イメージとそのステータスが表示されます。
4. VM に移動し、**VM の作成**をクリックします。
5. **VM の作成**ページで、**CD ROM ドライブ**を削除します。
6. 新しいディスクを追加します。

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

a. **タイプ**リストから**DISK**を選択します。

b. **操作**リストから**イメージサービスからクローン**を選択します。

c. **バスタイプ**リストから**SCSI**を選択します。

d. リストから NetScaler Console イメージを選択します。

e. **追加**をクリックします。

ディスクが追加されました。

7. VM に次の NIC 詳細を追加します。

「NICの追加」(/en-us/netscaler-application-delivery-management-software/media/nutanix-hypervisor-setting-7.png)

8. **保存**をクリックします。
9. コンピューティングの詳細を指定します。NetScaler ConsoleとNetScalerエージェントにはデフォルト値を使用します。

「コンピューティングの詳細」(/en-us/netscaler-application-delivery-management-software/media/nutanix-hypervisor-setting-4.png)

10. **保存**をクリックします。

VMが一覧表示され、電源オフと表示されたら、VMを起動するためにシリアルポートを追加する必要があります。

11. そのアカウントに設定したユーザー名とパスワードを使用して、コントローラーVM (CVM) にSSH接続します。CVMのIPアドレスのリストは、Prism Elementコンソールの「ハードウェア」セクションで確認できます。
12. **ACLI**と入力します。
13. 次のコマンドを使用してシリアルポートを作成します。`vmname`にVPXアプライアンスの名前を入力します。

```
vm.serial_port_create <vmname> type=kServer index=0
```

## ネットワーク構成

1. VMの電源をオンにします。
2. VNCコンソールを起動します。

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

「VNCコンソール」(/en-us/netscaler-application-delivery-management-software/media/nutanix-hypervisor-setting-5.png)

3. VMが起動したら、デフォルトの資格情報 (**nsrecover**/**nsroot**) を使用してログインします。
4. プロンプトで、次のように入力します: *shell*
5. **networkconfig** と入力して、NetScaler Console の初期ネットワーク構成メニューに入ります。管理 IP アドレスを構成します。
6. NetScaler Console の初期ネットワーク構成を完了するには、プロンプトに従います。コンソールには、次のパラメータを設定するための NetScaler Console の初期ネットワーク構成オプションが表示されます。ホスト名はデフォルトで入力されています。

   a. NetScaler Console IPv4 アドレス（NetScaler Console にアクセスするための管理 IP アドレス）を更新するには、**2** と入力します。

   b. ネットマスク（管理 IP アドレスに関連付けられたサブネットマスク）を更新するには、**3** と入力します。

   c. ゲートウェイ IPv4 アドレス（NetScaler Console の管理 IP アドレスのサブネットのデフォルトゲートウェイ IP アドレス）を更新するには、**4** と入力します。

   d. 保存して終了するには、**7** と入力します。設定の変更を保存し、システムを終了します。

   ブラウザのアドレスバーに NetScaler Console サーバの IP アドレスを入力すると、NetScaler Console にアクセスできます。サーバにログオンするためのデフォルトの管理者資格情報は *nsroot/nsroot* です。

# Red Hat OpenShift Virtualization 上の NetScaler コンソール

**注:**

Red Hat® OpenShift® Virtualization (RHOCPV) への NetScaler Console のインストールは、NetScaler Console リリース 14.1-72.xx 以降でサポートされています。

NetScaler® Console を Red Hat® OpenShift® Virtualization (RHOCPV) に仮想マシンとして展開できます。これにより、OpenShiftベースの環境でNetScalerインスタンスを管理できます。

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

## ハードウェア要件

| コンポーネント | 最小要件 |
| --- | --- |
| CPU | 最小 8 vCPU |
| メモリ (RAM) | 最小 32 GiB |
| ハードディスク | 最小 120 GiB (ブートディスク) |

**注:**

ハードウェア要件は、RHOCPV に展開される NetScaler Console 仮想マシンに適用されます。これらの値は、展開時に使用される推奨される汎用 (U シリーズ – 2xlarge) インスタンスタイプに基づいています。RHOCPV クラスターノードが、これらの要件に基づいて NetScaler Console 仮想マシンを実行するのに十分な容量を持っていることを確認してください。

## 前提条件

### プラットフォーム要件

- RHOCPV (OpenShift Virtualization) クラスターが展開されていること
- OpenShift Web コンソールまたは CLI (oc) へのアクセス
- KubeVirt が有効になっていること

**注:**

RHOCPV に展開された NetScaler の場合、サポートされる最小バージョンは 14.1–66.64 です。詳細については、Red Hat OpenShift® Virtualization (RHOCPV) 上の NetScaler VPX インスタンス を参照してください。

## 展開アーキテクチャ

- NetScaler Console は RHOCPV 上で仮想マシンとして実行されます
- NetScaler Agent は RHOCPV 上に展開できます

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

# Red Hat OpenShift Virtualization への NetScaler Console のインストール

RHOCPV に NetScaler Console をインストールするには、次の手順を実行します。

### ステップ 1 - 環境を準備する

1. RHOCPV クラスターが稼働していることを確認してください。
2. 仮想マシンを作成するための管理者アクセス権があることを確認してください。
3. 仮想マシンを作成および管理するために、仮想化オペレーターが有効になっていることを確認してください。

### ステップ2 - NetScaler Consoleセットアップファイルをダウンロードする

NetScaler Consoleセットアップファイルをダウンロードするには：

1. `<https://www.citrix.com/downloads>` ページにログオンします。
2. 製品リストから **NetScaler Console** を選択します。
3. **Release 14.1** の下で、14.1-72.x 以降のビルドを選択します。選択したビルドページが表示されます。
4. **Jump to Download** リストで、**NetScaler Console/NetScaler Console Agent image for KVM, 14.1 Build 72.57** を選択します。
5. **Download File** をクリックし、EULA に同意して、圧縮イメージファイルをローカルマシンの任意のフォルダーにダウンロードします。

### ステップ3 - イメージをRHOCPVブータブルボリュームにアップロードする

1. Red Hat OpenShiftコンソールにログインします。
2. ダッシュボードで、**Virtualization > Bootable Volumes** に移動します。
3. 右上隅にある **Add volume** をクリックし、**with form** を選択して、クラスターにブータブルボリュームを追加します。
4. **Upload PVC image** フィールドで、`.qcow2` 拡張子のNetScaler Console/Agentイメージファイルをアップロードします。
5. **Volume name** を指定し、利用可能な **Storage** を選択します。
6. **Volume metadata Preference** フィールドを **legacy** として指定します。
7. 「**保存**」をクリックします。

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

RHOCPV ブート可能ボリュームにイメージをアップロードします(/en-us/netscaler-application-delivery-management-software/media/rhov-add-volume.png)

### ステップ 4 - 仮想マシンを作成する

インスタンスタイプから仮想マシンを作成するには：

1. **仮想化 > 仮想マシン** に移動し、「**作成**」をクリックします。
2. **インスタンスタイプ** タブを選択します。
3. ステップ 3 で作成したブート可能ボリュームを選択します。

   ブート可能ボリュームを選択します(/en-us/netscaler-application-delivery-management-software/media/rhov-create-virtual-machine.png)
4. NetScaler Console モデルの仮想マシンのハードウェア仕様に一致するインスタンスタイプを選択します。詳細については、ハードウェア要件 を参照してください。
5. 仮想マシンの名前を入力します。
6. 「**仮想マシンのカスタマイズ**」をクリックします。
7. 存在する場合はデフォルトディスク (ここ `cloudinitdesk`) をデタッチし、120 GB のブート可能ディスクを保持します。

   120 GB のブート可能ディスクを保持します(/en-us/netscaler-application-delivery-management-software/media/rhov-customize-virtual-machine.png)
8. **ネットワーク** セクションで、インターフェースモデルとして `virtio` を選択し、リストから必要なネットワークを選択します。

   ネットワークを選択します(/en-us/netscaler-application-delivery-management-software/media/rhov-edit-network-interface.png)
9. **仮想マシンを作成**をクリックします。

### ステップ 5. 仮想マシンを起動する

仮想マシンを起動し、実行状態に達していることを確認します。

### ステップ 6. NetScaler Console にアクセスする

次の URL を使用して NetScaler Console にアクセスします。

```
https://<console-ip-address>
```

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

# Azure クラウド上の NetScaler コンソール

14.1-43.x以降、NetScaler Consoleは、Azure Government Marketplaceを通じてAzure上に仮想マシン (VM) として展開できる、より多くの展開オプションを提供します。NetScaler Consoleサービスは、クラウド展開がエアギャップされており、インターネット接続がない顧客にとっては実行可能なオプションではありません。Azure上にVMとして展開されたNetScaler Consoleを使用すると、Azure展開内でNetScaler Consoleを使用してNetScaler VPXインスタンスを効率的に管理および監視できます。

**注:**

Azure Cloud上のNetScaler Consoleは、Azure Government Marketplaceでのみ利用可能です。

## 前提条件

設定する前に、Azure Cloudとリソースグループへのアクセス権があることを確認してください。

**注:**

NetScaler Consoleをプロビジョニングする前に、リソースグループ、ネットワークセキュリティグループ、仮想ネットワーク、およびその他の必要なエンティティを作成することをお勧めします。

## NetScaler Consoleの設定

Azure クラウドで:

1. Marketplaceに移動し、NetScaler Consoleを検索して、**選択**をクリックします。

   イメージを選択すると、**仮想マシンの作成**ワークフローにリダイレクトされます。

2. 以下を指定します:

   a. **リソースグループ** - リストからリソースグループを選択します。

   b. **仮想マシン名** - 任意の名前。

   c. **リージョン** - リストからリージョンを選択します。

   d. **イメージ** - Marketplaceから選択したため、自動的に入力されます。

   e. リストからVMサイズを選択します (8vCPU、32GB RAMを推奨)。

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

f. **認証タイプ** - SSH公開鍵を選択します。

> **注:**
>
> パスワードオプションはサポートされていません。

g. **ユーザー名** - 名前を`nsroot`に変更します。NetScaler Consoleにアクセスするためのデフォルトのユーザー名は`nsroot`です。

h. **SSH公開鍵のソース** - 既存のキーペアを使用するか、新しいキーペアを作成できます。

i. **パブリック受信ポート** - **なし**を選択します。

j. **確認 + 作成**をクリックします。

VMの概要が表示されます。すべてを検証し、**作成**をクリックします。

k. VMの展開状況は進行中と表示されます。展開が完了したら、**リソースに移動**をクリックします。

VMに関する情報が表示され、**ネットワーク**の下でVMのパブリックIPとプライベートIPを確認できます。ブラウザからパブリックIPを使用してログインできます (`nsroot` / `nsroot`)。

> **注:**
>
> プライベートIPアドレスを使用する場合は、同じAzureクラウドネットワークでAzure Virtual Desktopが実行されていることを確認し、プライベートIPアドレスを介してNetScaler Consoleにアクセスできるようにします。

l. SSHを使用して、ユーザー名`nsrecover`とパスワード`nsroot`で仮想マシンにログインし、NetScaler Consoleプロセスが稼働していることを確認します。

m. バックエンドプロセスが稼働したら、`nsroot`パスワードを使用してNetScaler Console GUIにログインできます。初回ログイン時に、システムはデフォルトパスワードの変更を促します。

## Azure Cloud上のネットスケーラー コンソール HAペア

Azureでは、NetScaler Consoleの高可用性は、Azure Load Balancer (ALB) を使用して実現されます。ALBは、プライマリノードとセカンダリノードの両方にヘルスプローブを送信してインスタンスを監視します。プライマリインスタンスは`200 OK`で応答しますが、セカンダリインスタンスは応答しません。これらの応答に基づいて、ALBはプライマリインスタンスにのみトラフィックを

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

送信します。フェイルオーバーが発生した場合、新しいプライマリは`200 OK`で応答を開始し、ALBは自動的にそこにトラフィックを送信します。

### 前提条件

以下を確認してください:

- Azure Cloudとリソースグループへのアクセス権があること。

  **注:**

  NetScaler Consoleをプロビジョニングする前に、リソースグループ、ネットワークセキュリティグループ、仮想ネットワーク、およびその他の必要なエンティティを作成することをお勧めします。

- 2つのスタンドアロンAzure Cloud上のNetScaler Consoleインスタンスを作成すること。
- 通信に必要なポートが開いていること。詳細については、システム要件を参照してください。

### NetScaler Console HAペアの構成

2つのスタンドアロンNetScaler Consoleインスタンスを構成した後:

1. いずれかのNetScaler Console GUIにログインします。
2. **Settings > High Availability Settings** に移動します。

   **注:**

   - HAペアを構成するには、他のNetScaler ConsoleのプライベートIPアドレスを指定する必要があります。
   - フローティングIPは、Azure VNet (Virtual Network) から利用可能な任意のIPにすることができます。

3. **NetScaler Console高可用性 (HA) の構成**をクリックし、セカンダリノードの詳細、フローティングIPアドレスを指定して、**構成**をクリックします。

   HAペア構成(/en-us/netscaler-application-delivery-management-software/media/console-azure-ha1.png)

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

4. 確認ウィンドウで、**はい**をクリックします。NetScaler Consoleインスタンスが再起動し、HAペアを形成します。
5. HAペアの構成が完了したら、プライマリNetScaler Consoleにログインし、**設定 > HA展開**に移動して、プライマリノードとセカンダリノードを検証します。

   HAペアの検証(/en-us/netscaler-application-delivery-management-software/media/console-azure-ha2.png)

次のステップは、Azure CloudでフローティングIPアドレスをAzureロードバランサーのフロントエンドIPとして構成することです。Azure Cloudポータルで、ロードバランサーを検索し、結果から**ロードバランサー**を選択して、**作成**をクリックします。

1. **基本**で、Console VMが構成されているのと同じリソースグループとリージョンにAzure Load Balancer (ALB) を作成します。
   a. **インスタンスの詳細**で、SKU: **Standard**、タイプ: **Internal**、ティア: **Regional**を選択します。
2. **フロントエンドIP構成**で、Console HAペア用に構成されたフローティングIPを持つフロントエンドIPを追加します。
3. **バックエンドプール**で、2つのConsoleインスタンスのIPアドレスを追加します。
4. **負荷分散ルール**: プロトコル、ポート、バックエンドポート、ヘルスプローブ、およびフローティングIPが有効になっている以下のルールを構成します。

| ルール名 | プロトコル | ポート | バックエンドポート | フローティングIP |
|---|---|---|---|---|
| ルール-80 | TCP | 80 | 80 | はい |
| ルール-443 | TCP | 443 | 443 | はい |
| ルール-5454 | TCP | 5454 | 5454 | はい |
| ルール-22 | TCP | 22 | 22 | はい |
| ルール-8443 | TCP | 8443 | 8443 | はい |
| ルール-7443 | TCP | 7443 | 7443 | はい |
| ルール-27000 | TCP | 27000 | 27000 | はい |
| ルール-7279 | TCP | 7279 | 7279 | はい |

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

| ルール名 | プロトコル | ポート | バックエンドポート | フローティングIP |
|---|---|---|---|---|
| ルール-5563 | TCP | 5563 | 5563 | はい |
| ルール-4739 | UDP | 4739 | 4739 | はい |
| ルール-5140 | UDP | 5140 | 5140 | はい |
| ルール-162 | UDP | 162 | 162 | はい |
| ルール-514 | UDP | 514 | 514 | はい |
| ルール-5557 | UDP | 5557 | 5557 | はい |
| ルール-5558 | UDP | 5558 | 5558 | はい |

5. **ヘルスプローブ**: ステップ4に記載されている必要なすべてのポートでHTTPヘルスチェックを作成します。このヘルスプローブにより、プライマリコンソールはアクティブとして、セカンダリコンソールはパッシブとして有効になります。例:

   a. ポート: 443

   b. URL: `/mas_health`

   c. 予期される応答コード: 200

   ロードバランサーの作成の詳細については、Azureドキュメントのロードバランサーの作成を参照してください。

   ロードバランサーを設定した後、ALBのフロントエンドIPアドレスを使用してNetScaler Consoleにアクセスできます。

   **注:**

   フロントエンドIPアドレスを介してNetScaler Consoleにアクセスするには、同じAzureネットワークでAzure Virtual Desktopが実行されていることを確認してください。

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

# Amazon Web Services (AWS) 上の NetScaler コンソール

**14.1-47.x**以降、**AWS GovCloud**でAWS MarketplaceのAMIを使用してNetScaler Consoleを展開できます。

## 前提条件

Amazon GUIを使用してAWS Virtual Private Cloud (VPC) 内でNetScaler Console AMIを起動するには、以下が必要です。

- AWSアカウント
- AWS 仮想プライベートクラウド (VPC)
- AWSでセキュリティグループを作成する際に、22、80、443などの必要なポートが開いていることを確認する。詳細については、システム要件を参照してください。

## NetScaler Consoleの構成

1. AWSの認証情報を使用してAWS Marketplaceにログオンします。
2. AMIを検索し、**AMIs**を選択します。
3. 検索ボックスに「NetScaler Console」と入力し、NetScaler Consoleを選択し、**Launch instance from AMI**をクリックします。
4. **Instance Type**で、リストから8 vCPUおよび32 GBメモリのオプションを選択します。

   **注:**

   デフォルトでは、NetScaler Console AMIは500 GBです。

5. **Key Pair (login)**で、既存のキーペアを選択するか、新しいキーペアを作成します。
6. 「**ネットワーク設定**」の下で「**編集**」をクリックし、次の操作を行います。

   a. リストからVPCを選択します。

   b. 新しいサブネットを選択または作成します。

   c. パブリックIPアドレスを使用してNetScaler Consoleを起動するには、「**パブリックIPの自動割り当て**」を有効にします。

   d. セキュリティグループを選択または作成します。

「

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

**注:**

」.

ポート22、443、80などの必要なポートが開いていることを確認してください。詳細については、「システム要件」を参照してください。

e. 「**インスタンスの起動**」をクリックします。インスタンスIDが作成されます。

7. インスタンスIDをクリックします。

「**ステータスチェック**」が「合格」（緑色のチェックマーク）と表示されるまで待つ必要がある場合があります。

8. セキュリティチェックが完了したら、インスタンスIDをクリックして詳細を表示します。

IPアドレスを使用してNetScaler Console GUIを起動します。プライベートIPアドレスを使用する場合は、AWSにVDIがあることを確認してください。

次の表は、SSH、GUI、およびシリアルコンソール（AWSからアクセスできるコンソール）を介したAWSログインプロセスについて説明しています。

| | SSH | | シリアルコンソール | | GUI | |

| | **エヌエスルート** | **エヌエスリカバリー** | **エヌエスルート** | **ンスリカバー** | **ンスルート** | **カスタムユーザー** |
|---|---|---|---|---|---|---|
| **パスワード** | 許可 (デフォルトパスワードは `nsroot`) | 許可 (デフォルトパスワードは `nsroot`) | 許可されていません | 許可 (デフォルトパスワードは `nsroot`) | 許可 (デフォルトパスワードは `nsroot`) | 許可 (ユーザー定義パスワード) |
| **公開キー** | 許可 | 該当なし | 該当なし | 該当なし | 該当なし | 該当なし |

# 高可用性展開を構成する

高可用性 (HA) とは、サービスの中断なしに常にユーザーが利用できるシステムを指します。高可用性セットアップは、システムのダウンタイム、ネットワークまたはアプリケーションの障害時に不可欠であり、あらゆる企業にとって重要な要件です。同じ構成のアクティブ/パッシブモードで2つのNetScaler Consoleノードを高可用性展開することで、中断のない運用が提供されます。

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

# 展開シナリオ

シナリオ(/en-us/netscaler-application-delivery-management-software/media/deploymentscenario-console.png)

**注**

単一のNetScaler Console HA展開で検証済みの最大ストレージ制限は3 TBです。詳細については、展開ガイドを参照してください。

**重要**

**HTTPSを使用してNetScaler Console 12.1ビルド48.18以降のバージョンにアクセスするには：**
高可用性モードでNetScaler Consoleを負荷分散するようにNetScalerインスタンスを構成している場合は、まずNetScalerインスタンスを削除します。次に、高可用性モードでNetScaler Consoleにアクセスするためのフローティング IPアドレスを構成します。
NetScaler Consoleにおける高可用性展開の利点は次のとおりです。

- プライマリノードとセカンダリノード間のハートビートを監視するための改善されたメカニズム。
- 論理的な双方向レプリケーションではなく、データベースの物理ストリーミングレプリケーションを提供します。
- 個別のNetScalerロードバランサーの必要性を排除するために、プライマリノードにフローティングIPアドレスを構成する機能。
- フローティングIPアドレスを使用してNetScaler Consoleユーザーインターフェイスに簡単にアクセスできます。
- NetScaler Consoleユーザーインターフェイスはプライマリノードでのみ提供されます。プライマリノードを使用することで、セカンダリノードにアクセスして変更を加えるリスクを排除できます。
- フローティングIPアドレスを設定することでフェイルオーバー状況に対応し、インスタンスの再設定は不要になります。
- スプリットブレイン状況を検出して処理する組み込み機能を提供します。

次の表は、高可用性展開で使用される用語について説明しています。

| 用語 | 説明 |
| --- | --- |
| プライマリノード | 高可用性展開に登録された最初のノード。 |

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

| 用語 | 説明 |
| --- | --- |
| セカンダリノード | 高可用性展開に登録された2番目のノード。 |
| ハートビート | 高可用性設定において、プライマリノードとセカンダリノード間でメッセージを交換するために使用されるメカニズム。これらのメッセージは、各ノード上のアプリケーションのステータスと健全性を判断します。 |
| フローティングIPアドレス | フローティングIPは、同じサブネット内の1つのノードから別のノードに瞬時に移動できるIPアドレスです。内部的には、プライマリノードのネットワークインターフェース上のエイリアスとして設定されます。フェイルオーバーが発生した場合、フローティングIPアドレスは古いプライマリから新しいプライマリにシームレスに移動します。単一のIPアドレスを使用してクライアントが高可用性ノードと通信できるため、高可用性設定で役立ちます。 |

**注:**

ポートとプロトコルの詳細については、ポートを参照してください。

## 高可用性アーキテクチャのコンポーネント

次の図は、高可用性モードで展開された2つのNetScaler Consoleノードのアーキテクチャを示しています。

HAアーキテクチャ(/en-us/netscaler-application-delivery-management-software/media/haarchitecture-console.png)

高可用性展開では、一方のNetScaler Consoleノードがプライマリノード (MAS 1) として構成され、もう一方がセカンダリノード (MAS 2) として構成されます。何らかの理由でプライマリノードがダウンした場合、セカンダリノードが新しいプライマリノードとして引き継ぎます。

## 監視ツール

監視ツールは、フェイルオーバー状況の監視、アラート、および処理に使用される内部プロセスです。このツールは、高可用性環境の各ノードでアクティブに実行されています。サブシステムの

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

起動、両ノードでのデータベースの初期化、フェイルオーバー時のプライマリノードまたはセカンダリノードの決定などを担当します。

## プライマリノード

プライマリノードは接続を受け入れ、インスタンスを管理します。AppFlow、SNMP、LogStream、syslogなどのすべてのプロセスはプライマリノードによって管理されます。NetScaler Consoleのユーザーインターフェイスアクセスはプライマリノードで利用できます。フローティングIPアドレスはプライマリノードで構成されます。

## セカンダリノード

セカンダリノードは、プライマリノードから送信されるハートビートメッセージをリッスンします。セカンダリノード上のデータベースは読み取りレプリカモードのみです。セカンダリノードではどのプロセスもアクティブではなく、NetScaler Consoleのユーザーインターフェイスはセカンダリノードではアクセスできません。

## 物理ストリーミングレプリケーション

プライマリノードとセカンダリノードは、ハートビートメカニズムを介して同期します。データベースの物理ストリーミングレプリケーションにより、セカンダリノードは読み取りレプリカモードで起動します。セカンダリノードは、プライマリノードから受信したハートビートメッセージをリッスンします。セカンダリノードが180秒間ハートビートを受信しない場合、プライマリノードはダウンしていると見なされます。その後、セカンダリノードがプライマリノードとして引き継ぎます。

## ハートビートメッセージ

ハートビートメッセージは、プライマリノードとセカンダリノード間で送受信されるユーザーデータグラムパケット (UDP) です。NetScaler Consoleのすべてのサブシステムとデータベースを監視し、ノードの状態、健全性、プロセスなどに関する情報を交換します。この情報は、高可用性ノード間で毎秒共有されます。フェイルオーバーまたは高可用性状態の切断が発生した場合、管理者にはアラートとして通知が送信されます。

## フローティングIPアドレス

高可用性セットアップでは、フローティングIPアドレスはプライマリノードに関連付けられています。これは、クライアントがプライマリノードのNetScaler Consoleに接続するために使用できる、プライマリノードIPアドレスに与えられたエイリアスです。フローティングIPアドレスはプライマリノードに構成されているため、フェイルオーバー時にインスタンスの再構成は必要ありません。インスタンスは、新しいプライマリに到達するために同じIPアドレスに再接続します。

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

## 注意すべき重要な点

- 高可用性セットアップでは、両方のNetScaler Consoleノードがアクティブ-パッシブモードで展開されます。これらは、同じソフトウェアバージョンとビルドを使用し、同じ構成を持つ同じサブネット上にある必要があります。
- フローティングIPアドレス:
  - フローティングIPアドレスはプライマリノードに構成されます。
  - フェイルオーバーが発生した場合、インスタンスを再構成する必要はありません。
  - ユーザーインターフェイスから高可用性ノードにアクセスするには、プライマリノードIPまたはフローティングIPアドレスのいずれかを使用できます。

    **注:**

    ユーザーインターフェイスにアクセスするには、フローティングIPアドレスを使用することをお勧めします。

- データベース:
  - 高可用性セットアップでは、すべての構成ファイルが1分間隔でプライマリノードからセカンダリノードに自動的に同期されます。
  - データベースの同期は、データベースの物理レプリケーションによって即座に行われます。
  - セカンダリノード上のデータベースは読み取りレプリカモードです。
- NetScaler Consoleのアップグレード:
  - 内部プロセスにより、NetScaler Consoleは以前のバージョンから暗黙的にアップグレードされます。

    **注記：**

    アップグレードが成功した後、フローティングIPアドレスを設定する必要があります。

- UDPデフォルトポート5005は、ハートビートの送信とメッセージの受信のために、両方のノードで利用可能です。

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

- MACアドレス ハイパーバイザーの「MACアドレス変更」オプションの設定は、仮想マシンが受信するトラフィックに影響します。フェイルオーバー後、フローティングIPアドレスが新しいプライマリノードにシームレスに移動するように、仮想スイッチでMACアドレス変更を有効にしてください。 例えば、VMware ESXi上でNetScaler Consoleを高可用性で展開する場合、MACアドレスの変更を受け入れるようにしてください。ESXiは現在、アクティブなMACアドレスを初期MACアドレス以外のものに変更する要求を許可しています。

  **注記：**

  ESXIバージョン6.7に展開されたNetScaler Consoleの場合、**MACアドレス変更**オプションを**拒否**に設定することもできます。フェイルオーバー後、**MACアドレス変更**の設定に関わらず、トラフィックは新しいプライマリノードにシームレスに流れます。したがって、MACアドレスの変更を受け入れることは必須ではありません。

  NetScaler ConsoleがESXIバージョン6.7より低いバージョンに展開されている場合、**MACアドレス変更**オプションが**許可**に設定されていることを確認してください。

## 前提条件

NetScaler Consoleノードの高可用性を設定する前に、以下の前提条件に注意してください。

- NetScaler Consoleの高可用性展開は、NetScaler Consoleバージョン12.0ビルド51.24以降でサポートされています。
- NetScalerサイトからNetScaler Consoleイメージファイル (.xva) をダウンロードします: `<https://www.citrix.com/downloads/>`

スケジューリング動作とネットワーク遅延を改善するために、CPU優先度 (仮想マシンプロパティで) を最高レベルに設定することをお勧めします。

次の表に、仮想コンピューティングリソースの最小要件を示します。

| コンポーネント | 要件 |
| --- | --- |
| RAM | **32 GB** |
| 仮想CPU | **8 CPU** |
| ストレージ容量 | NetScaler Consoleの展開には、ソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。デフォルト値は120 |

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

| コンポーネント | 要件 |
| --- | --- |
| | GBです。実際のストレージ要件は、NetScaler Consoleのサイジング見積もりによって異なります。NetScaler Consoleのストレージ要件が120 GBを超える場合は、追加のディスクを接続する必要があります。**注:** 追加できるディスクは1つだけです。初期展開時にストレージを見積もり、追加のディスクを接続することをお勧めします。詳細については、「NetScaler Consoleに追加ディスクを接続する方法」を参照してください。 |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 Gbpsまたは100 Mbps |
| **ハイパーバイザー** | **バージョン** |
| シトリックス ハイパーバイザー | 6.2および6.5 |
| ヴイエムウェア ESXi | 5.5 および 6.0 |
| マイクロソフト Hyper-V | 2012 R2 |
| リナックス KVM | Ubuntu および Fedora |

## NetScaler Console を高可用性モードでセットアップするには

バージョン 14.1 ビルド 17.x 以降、プライマリノードの NetScaler Console GUI から直接高可用性セットアップを展開できます。

1. 最初のサーバー (プライマリノード) を登録します。
2. 2番目のサーバー (セカンダリノード) を登録します。
3. プライマリノードの GUI で高可用性セットアップを展開します。

## 最初のサーバー (プライマリノード) を登録する

プライマリノードを登録するには:

1. NetScaler サイトからダウンロードした .xva イメージファイルを使用し、それをハイパーバイザーにインポートします。

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

> **注:**
>
> .xva イメージファイルのインポートと起動には数分かかる場合があります。画面下部にステータスが表示されます。

XVAファイル(/en-us/netscaler-application-delivery-management-software/media/importvm.png)

2. インポートが成功したら、右クリックして**開始**をクリックします。

   ファイルの開始(/en-us/netscaler-application-delivery-management-software/media/startvm.png)

3. **コンソール**タブから、NetScaler Consoleを初期ネットワーク構成で設定します。

   ネットワーク構成(/en-us/netscaler-application-delivery-management-software/media/admha-initialconfig.png)

4. 初期ネットワーク構成が完了すると、システムはログインを促します。次の資格情報を使用してログオンします – *nsrecover/nsroot*。

> **注:**
>
> ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`と入力し、構成を更新して保存します。

## 2番目のサーバー（セカンダリノード）を登録する

1. NetScalerサイトからダウンロードした**.xva**イメージファイルを使用して、ハイパーバイザーにインポートします。
2. **コンソール**タブから、次の画像に表示されているように、NetScaler Consoleを初期ネットワーク構成で設定します。
3. 初期ネットワーク構成が完了すると、システムはログインを促します。次の資格情報を使用してログオンします – *nsrecover/nsroot*。

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

**注:**

- ログオン後、初期ネットワーク構成を更新する場合は、`networkconfig`と入力し、構成を更新して保存します。
- 設定に問題がある場合、システムはエラーメッセージを表示します。
- システムが再起動し、設定が有効になるまでに数分かかります。

## プライマリノードGUIから高可用性セットアップを展開する

プライマリノードとセカンダリノードの両方を登録した後、プライマリノードGUIにログインして高可用性ペアをセットアップします。

注:

- ノードを高可用性ペアに展開する前に、初期ネットワーク構成後、セカンダリノードが再起動を完了していることを確認してください。

プライマリノードから高可用性ペアを展開するには、次の手順に従います。

1. プライマリノードGUIにログインします。
2. **設定 > 管理 > 高可用性設定 > NetScaler Console高可用性 (HA) の構成** に移動します。
3. **Configure NetScaler Console High Availability (HA) ページ**で、セカンダリノードの次の詳細を入力します。
   - ピアノードIPアドレス
   - ピアノードパスワード
   - フローティングIPアドレス
4. 「Configure」をクリックします。
5. **Confirm** ページで、**Yes** をクリックします。

   HAペアを構成する(/en-us/netscaler-application-delivery-management-software/media/configure-ha-pair.png)

   プライマリノードとセカンダリノードの両方が再起動され、高可用性ペアが形成されます。これには通常、約10分かかります。

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

注:

- これで、**フローティングIPアドレス**の使用を開始できます。
- ノードの高可用性展開には、フローティングIPアドレスが必須です。
- 高可用性展開が完了したら、フローティングIPアドレスを使用してNetScaler Consoleのユーザーインターフェイスにアクセスします。

6. **Settings > Deployment**に移動して、展開を検証します。

注:

セカンダリノードが起動するまでに約10分かかる場合があります。それまでは、セカンダリノードのステータスは**Down**と表示されます。

詳細については、よくある質問を参照してください。

## 高可用性を無効にする

NetScaler Consoleの高可用性ペアで高可用性を無効にし、ノードをスタンドアロンのNetScaler Consoleサーバーに変換できます。

**注:**

プライマリノードから高可用性を無効にします。

**高可用性を無効にするには:**

1. Webブラウザで、NetScaler Consoleサーバーのプライマリノードの IPアドレスを入力します。
2. **ユーザー名**フィールドと**パスワード**フィールドに、管理者資格情報を入力します。
3. **システム**タブで、**展開**に移動し、**HAを解除**をクリックします。

   ダイアログボックスが表示されます。**はい**をクリックして、高可用性展開を解除します。

## 高可用性を再展開する

高可用性をスタンドアロン展開に無効にした後、再度高可用性モードに再展開できます。高可用性の再展開は、高可用性の初回展開と同様です。詳細については、「プライマリノードGUIから高可用性セットアップを展開する」を参照してください。

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

**注：**

NetScaler® Consoleの高可用性を無効にした後、スタンドアロンライセンスサーバーとして1つのコンソールノードのみを使用してください。2番目のノードは再プロビジョニングする必要があります。

## 高可用性フェイルオーバーシナリオ

次のいずれかの条件が発生した場合にフェイルオーバーが発生します。

- **ノード障害**：プライマリノードがダウンし、プライマリノードから180秒間ハートビートが検出されない場合。
- **アプリケーションヘルス障害**：プライマリノードは稼働中ですが、NetScaler Consoleのプロセスの1つがダウンしている場合。

## データベース同期ログメッセージを表示する

NetScaler Console HAペアでは、設定ファイルはプライマリノードからセカンダリノードに自動的に同期され、データベースの物理ストリーミングレプリケーションが行われます。

ただし、ストリーミングレプリケーションエラーが発生した場合は、**データベースの同期**ボタンが表示されます。**データベースの同期**ボタンをクリックして、データベース同期プロセスを開始できます。

データベース同期の進行状況を表示するには、**ログの表示**をクリックします。**データベース同期ログ**メッセージが表示され、同期の進行状況の詳細をリアルタイムで確認できます。

## スプリットブレインシナリオ

ネットワークリンクのダウンタイムにより両方のノード間で通信がない場合、次のようになります。

- プライマリノードはプライマリとして動作し続けます
- セカンダリノードはハートビートの受信に失敗したため、プライマリとして引き継ぎます
- 両方のノードは個別のデータベースインスタンスを実行します

例えば、企業では2つのNetScaler Consoleノードがプライマリとセカンダリとして展開されています。ネットワークリンクのダウンタイムの可能性があるため、2つのNetScaler Consoleノード間の

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

通信は完全に途絶えます。180秒以上ハートビートの交換がないため、両方のノードは自身をプライマリノードと見なします。両方のノードはアクティブノードとして機能し、独自のデータベースインスタンスを実行します。

NetScaler Console 12.1以降のリリースでは、ネットワークリンクとハートビートが復元された後、このスプリットブレイン状況は適切に処理されます。高可用性同期は自動的に復元されます。回復時間は、ノード間のデータの量とリンクの速度によって異なります。

**注:**

スプリットブレイン状態の間、古いプライマリノードで発生した変更は、高可用性に再結合されると新しいプライマリによってリセットされます。スプリットブレイン中に新しいプライマリノードで発生した変更はそのまま維持されます。

## ライセンス

NetScaler Consoleサーバーには、VIP、CICO、およびプールされた容量ライセンスを含めることができます。ライセンスがNetScaler Consoleサーバーに発行されると、ライセンスはサーバーホストIDにバインドされます。別のNetScaler Consoleサーバーにライセンスを割り当てることは制限されています。

NetScaler Consoleの高可用性ペアをライセンスサーバーとして構成すると、プライマリに適用されたライセンスファイルはセカンダリに同期されます。

**注：**

- リリース12.1-50.x以降では、NetScaler Consoleライセンスはプライマリノードからセカンダリノードへ自動的に同期されます。

## 異なるレイヤー3サブネット間での高可用性 (HA over L3) の構成

リリース14.1-66.x以降、NetScaler Consoleは異なるレイヤー3 (L3) サブネット間での高可用性 (HA) デプロイメントをサポートしています。

この機能強化により、以下の機能が提供されます。

- プライマリおよびセカンダリのNetScaler Consoleノードは、異なるL3サブネットまたはデータセンターにデプロイできます。

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

- フローティングIPアドレス (VIP) は、外部ロードバランサーによって構成および所有されます。
- ロードバランサーは、クライアントトラフィックをアクティブなNetScaler Consoleノードに転送します。
- ノード間のHA同期は変更されません。

一般的なHAの概念、ノードの役割、および同期動作については、HAドキュメントを参照してください。

NetScaler Consoleは、外部ロードバランサーを使用してフローティングIPアドレスを管理し、L2の依存関係を排除することで、異なるサブネット間でのHAデプロイメントをサポートします。

以前は、フローティングIPアドレスがHAペアによって内部的に所有および管理されていたため、NetScaler Consoleではプライマリノードとセカンダリノードが同じサブネットに存在する必要がありました。これにより、レイヤー2の依存関係が生じ、セグメント化されたネットワークや地理的に離れたネットワーク間でのデプロイメントが制限されていました。このため、HAデプロイメントはレイヤー2環境に限定され、お客様は以下のことができませんでした。

- 異なるサブネット間でのHAのデプロイ。
- データセンター間でのノードの分散。
- ルーティングされたエンタープライズネットワークアーキテクチャとの整合。

### 高レベルアーキテクチャ

- フローティングIPアドレス (VIP) は、外部ロードバランサーで構成されます。
- NetScaler Console はこのデプロイで VIP の所有権を取得しません。
- ロードバランサーは、ヘルスチェックに基づいてアクティブノードにトラフィックを転送します。
- HA同期は、L3接続を介してノード間で直接継続されます。
- NetScaler Console 内のARPベースのVIP引き継ぎは使用されません。

**注:**

推奨されるロードバランサーはNetScalerですが、サードパーティのロードバランサーもサポートされています。

L3越しのHA(/en-us/netscaler-application-delivery-management-software/media/ha-over-l3-architecture.png)

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

## 展開と構成

### 前提条件

- 外部のレイヤー3対応ロードバランサーが展開され、以下から到達可能であること:
  - クライアント
  - 両方のNetScaler Consoleノード
- プライマリノードとセカンダリノード間のネットワーク接続。

### ワークフロー

1. 2つのNetScaler Consoleノード（プライマリとセカンダリ）を別々のL3サブネットまたはデータセンターに展開します。
2. 外部ロードバランサーを展開して構成します。
3. ロードバランサー（フロントエンド）にフローティングIPアドレス（VIP）を作成し、両方のNetScaler Consoleノードをバックエンドターゲットとして追加します。
4. 次のプロトコルとポートを使用して、VIPのロードバランシングルールを作成します。

| LB仮想サーバー | プロトコル | ポート |
|---|---|---|
| HTTP | TCP | 80 |
| HTTPS | TCP | 443 |
| DBとHA | TCP | 5454 |
| NTP | UDP | 123 |
| SNMP | UDP | 162 |
| SYSLOG | UDP | 514 |
| ライセンス | TCP | 27000 |
| ベンダーデーモン | TCP | 7279 |

5. ロードバランサーがアクティブノードにのみトラフィックを転送するように、すべてのバックエンドターゲットでヘルスモニターを設定します。

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

| モニター / 目的 | プロトコル / ポート |
| --- | --- |
| HAとDB | TCP / 5454 |
| SNMP | UDP / 162 |
| システムログ | UDP / 514 |
| NTP | UDP / 123 |

6. NetScaler Console HAペアを設定し、フローティングIPアドレスが外部で構成されていることを指定します。

### NetScaler ConsoleでHAを構成する

1. プライマリとして構成するノードでNetScaler Console GUIにサインインします。
2. **>** に移動します。
3. **NetScaler Console High Availability (HA) の構成**を選択し、セカンダリノードの詳細を入力します。
4. 外部ロードバランサーで構成されたVIPを入力し、**フローティングIPアドレスは外部で構成されています**を選択して、**保存**をクリックします。

   **注記:**

   外部ロードバランサーでフローティングIPアドレス (VIP) を構成します。NetScaler Consoleは、異なるサブネットのHAモデルではこのVIPを所有または管理しません。

5. NetScaler Consoleインスタンスが再起動し、HAペアを形成します。
6. HAが構成されたら、プライマリノードにサインインし、**設定 > HA展開**に移動して、プライマリとセカンダリのステータスを検証します。

### NetScalerを外部ロードバランサーとして構成する

クライアントトラフィックがアクティブなNetScaler Consoleノードにのみ送信されるように、外部ロードバランサーでフローティングIPアドレス (VIP) と転送ルールを構成します。正確な手順は

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

ロードバランサーベンダーによって異なります。以下の要件は広く適用され、NetScalerまたはサードパーティのロードバランサーで実装できます。

1. クライアントがNetScaler Consoleにアクセスするために使用する、同じ仮想IPアドレス (フロントエンド) を持つすべての仮想サーバーを作成します。
2. 各仮想サーバーのサービスグループを作成し、両方のNetScaler Consoleノードをサービスグループメンバーとしてバインドします。
3. サービスグループをそれぞれの仮想サーバーにバインドします。
4. アクティブノードを確実に示すモニターを作成し、それらをステップ2で構成したサービスグループにバインドします。

**注記:**

ロードバランサーと両方のNetScaler Consoleノード間で、システム要件で定義されているすべての必要なポートが開いていることを確認してください。

### NetScalerロードバランシング構成スクリプトの例

ロードバランシング仮想サーバーを追加する

```
add lb vserver ADM-LB HTTP <EXTERNAL_VIP> 80 -persistenceType NONE
-cltTimeout 180



add lb vserver ADM-LB-HTTPS SSL <EXTERNAL_VIP> 443 -persistenceType NONE
-cltTimeout 180



add lb vserver ADM-LB-SNMP UDP <EXTERNAL_VIP> 162 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-SYSLOG UDP <EXTERNAL_VIP> 514 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-DB_HA TCP <EXTERNAL_VIP> 5454 -persistenceType NONE
```

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

```
-cltTimeout 9000



add lb vserver ADM-LB-LICENSE TCP <EXTERNAL_VIP> 27000 -persistenceType
NONE -cltTimeout 9000



add lb vserver ADM-LB-NTP UDP <EXTERNAL_VIP> 123 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-VENDOR-DEMON TCP <EXTERNAL_VIP> 7279
-persistenceType NONE -cltTimeout 9000
```

サービスグループを追加する

```
add serviceGroup ADM-SVCG-HTTP HTTP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-HTTPS SSL -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES

-cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO



add serviceGroup ADM-SVCG-SNMP UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-SYSLOG UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO
```

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

```
add serviceGroup ADM-SVCG-DB_HA TCP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-NTP UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-LICENSE TCP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-VENDOR-DEMON TCP -maxClient 0 -maxReq 0 -cip
DISABLED -usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA
NO -TCPB NO -CMP NO
```

ロードバランシング仮想サーバーをサービスグループにバインドする

```
bind lb vserver ADM-LB ADM-SVCG-HTTP



bind lb vserver ADM-LB-HTTPS ADM-SVCG-HTTPS



bind lb vserver ADM-LB-SNMP ADM-SVCG-SNMP



bind lb vserver ADM-LB-SYSLOG ADM-SVCG-SYSLOG



bind lb vserver ADM-LB-DB_HA ADM-SVCG-DB_HA
```

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

```
bind lb vserver ADM-LB-NTP ADM-SVCG-NTP

bind lb vserver ADM-LB-LICENSE ADM-SVCG-LICENSE

bind lb vserver ADM-LB-VENDOR-DEMON ADM-SVCG-VENDOR-DEMON
```

サービスグループをNetScaler Consoleノードにバインドする

```
bind serviceGroup ADM-SVCG-HTTP <PRIMARY_IP> 80

bind serviceGroup ADM-SVCG-HTTP <SECONDARY_IP> 80

bind serviceGroup ADM-SVCG-HTTPS <PRIMARY_IP> 443

bind serviceGroup ADM-SVCG-HTTPS <SECONDARY_IP> 443

bind serviceGroup ADM-SVCG-SNMP <PRIMARY_IP> 162

bind serviceGroup ADM-SVCG-SNMP <SECONDARY_IP> 162
```

ロードバランシングモニターを追加する

```
add lb monitor monitor-snmp UDP-ECV -send "Udp data" -destPort 162
```

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

```
add lb monitor monitor-syslog UDP-ECV -send "Udp data" -LRTM DISABLED
-destPort 514


add lb monitor monitor-db TCP-ECV -LRTM DISABLED -destPort 5454


add lb monitor monitor-ntp UDP-ECV -send "Udp data" -LRTM DISABLED
-destPort 123
```

モニターとメンバーをサービスグループにバインドする

```
bind serviceGroup ADM-SVCG-SNMP -monitorName monitor-snmp


bind serviceGroup ADM-SVCG-SYSLOG <PRIMARY_IP> 514


bind serviceGroup ADM-SVCG-SYSLOG <SECONDARY_IP> 514


bind serviceGroup ADM-SVCG-SYSLOG -monitorName monitor-syslog


bind serviceGroup ADM-SVCG-DB_HA <PRIMARY_IP> 5454


bind serviceGroup ADM-SVCG-DB_HA <SECONDARY_IP> 5454


bind serviceGroup ADM-SVCG-DB_HA -monitorName monitor-db
```

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

```
bind serviceGroup ADM-SVCG-NTP <PRIMARY_IP> 123

bind serviceGroup ADM-SVCG-NTP <SECONDARY_IP> 123

bind serviceGroup ADM-SVCG-NTP -monitorName monitor-ntp

bind serviceGroup ADM-SVCG-LICENSE <PRIMARY_IP> 27000

bind serviceGroup ADM-SVCG-LICENSE <SECONDARY_IP> 27000

bind serviceGroup ADM-SVCG-VENDOR-DEMON <PRIMARY_IP> 7279

bind serviceGroup ADM-SVCG-VENDOR-DEMON <SECONDARY_IP> 7279
```

モードを有効にしてサービスグループを更新する

```
enable ns mode USIP

enable ns mode MBF

set serviceGroup ADM-SVCG-SYSLOG -usip YES

set serviceGroup ADM-SVCG-SNMP -usip YES
```

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

### 利点

- **柔軟で回復力のある展開**: 異なるサブネットまたはデータセンター間でHAを有効にし、障害分離と可用性を向上させます。
- **最新のネットワークアーキテクチャとの整合性**: レイヤー2の制約なしに、ルーティングされた（L3）およびセグメント化されたエンタープライズ環境をサポートします。
- **既存のインフラストラクチャを活用**: NetScaler ADCまたはサードパーティのロードバランサーと統合し、スケーラブルで柔軟なトラフィック管理を実現します。

## 高可用性のためのディザスターリカバリを構成する

災害とは、自然災害または人為的な出来事によって引き起こされる事業機能の突然の中断です。災害はデータセンターの運用に影響を与え、その後、災害現場で失われたリソースとデータは完全に再構築および復元される必要があります。データセンターにおけるデータの損失やダウンタイムは致命的であり、事業継続性を崩壊させます。

NetScaler Consoleのディザスターリカバリ（DR）機能は、高可用性モードで展開されたNetScaler Consoleの完全なシステムバックアップおよびリカバリ機能を提供します。リカバリ時には、証明書、構成ファイル、およびデータベースの完全なバックアップがリカバリサイトで利用可能です。

次の表は、NetScaler Consoleでディザスターリカバリを構成する際に使用される用語について説明しています。

| 用語 | 説明 |
| --- | --- |
| プライマリサイト（データセンターA） | プライマリサイトには、高可用性モードで展開されたNetScaler Consoleノードがあります。 |
| リカバリサイト（データセンターB） | リカバリサイトには、スタンドアロンモードで展開されたディザスターリカバリノードがあります。このノードは読み取り専用モードであり、プライマリサイトがダウンするまで動作しません。 |
| ディザスターリカバリノード | リカバリノードは、リカバリサイトに展開されたスタンドアロンノードです。プライマリサイトで災害が発生し、機能しなくなった場合に、このノードが（新しいプライマリとして）動作可能になります。 |

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

**注**

プライマリサイトとDRサイトは、ポート5454と22を介して相互に通信し、これらのポートはデフォルトで有効になっています。

ポートとプロトコルの詳細については、ポートを参照してください。

## 基本認証を有効にする

基本認証は、一時的に有効にする必要があります。

- エージェントとディザスタリカバリノードの初期登録を完了する。
- NetScaler GUIからライセンスアクティベーションシステム (LAS) のチェックアウトを開始する。

**注**

基本認証は、初期登録にのみ必要です。

### 基本認証を構成する

1. **設定 > 管理 > システム構成 > システム、タイムゾーン、許可されたURL、およびエージェント設定** に移動します。
2. **Basic Settings** をクリックします。
3. **Enable Allow Basic Authentication** を選択します。
4. **OK** をクリックします。

**注**

DRサイトが正常に構成される前に基本認証オプションを有効にしてください。そうしないと、次のエラーが表示されます。

`Not valid username/password or incorrect host IP, or the host is unable to respond to the request.`.

## ディザスタリカバリワークフロー

次の図は、ディザスターリカバリーのワークフロー、ディザスター発生前の初期設定、およびディザスター発生後のワークフローを示しています。

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

### ディザスター発生前の初期設定



この図は、ディザスター発生前のディザスターリカバリー設定を示しています。

プライマリサイトには、高可用性モードで展開されたNetScaler Consoleノードがあります。詳細については、「高可用性展開」を参照してください。

リカバリーサイトには、スタンドアロンのNetScaler Consoleディザスターリカバリーノードがリモートに展開されています。ディザスターリカバリーノードは読み取り専用モードで、プライマリノードからデータを受信してデータバックアップを作成します。リカバリーサイトのNetScalerインスタンスも検出されますが、トラフィックは流れていません。バックアッププロセス中、すべてのデータ、ファイル、および構成は、プライマリノードからディザスターリカバリーノードにレプリケートされます。

## 前提条件

ディザスターリカバリーノードを設定する前に、次の前提条件に注意してください。

- ディザスターリカバリー設定を有効にするには、プライマリサイトに高可用性モードで構成されたNetScaler Consoleノードが必要です。
- NetScaler Console HAペア（プライマリサイト）とスタンドアロンノード（DRサイト）は、同じソフトウェアバージョン、ビルド、および構成である必要があります。

スケジューリング動作とネットワーク遅延を改善するために、CPU優先度（仮想マシンプロパティ内）を最高レベルに設定することをお勧めします。

次の表に、ディザスターリカバリーノードを構成するための最小要件を示します。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| ストレージ容量 | NetScaler Consoleの展開には、ソリッドステートドライブ（SSD）テクノロジーの使用を推奨します。デフォルト値は120 GBです。実際のストレージ要件は、NetScaler Consoleのサイジング見積もりによって異なります。NetScaler Consoleのストレージ要件が120 GBを超える場合は、追加のディスクを接続する必要があります。**注** 追加できるディスクは1つだ |

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

| コンポーネント | 要件 |
| --- | --- |
| | けです。初期展開時にストレージを見積もり、追加のディスクを接続することをお勧めします。詳細については、「NetScaler Consoleにディスクを追加する方法」を参照してください。 |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 Gbpsまたは100 Mbps |
| **ハイパーバイザー** | **バージョン** |
| シトリックス ハイパーバイザー | 6.2および6.5 |
| ヴイエムウェア ESXi | 5.5および6.0 |
| マイクロソフト ハイパーV | 2012 R2 |
| リナックス ケーブイエム | Ubuntu および Fedora |

## 初めてのディザスタリカバリ設定

- NetScaler Console を高可用性モードで展開する
- NetScaler Console ディザスタリカバリノードを展開して登録する
- ユーザーインターフェイスからディザスタリカバリ設定を有効/無効にする

### NetScaler Console を高可用性モードで展開する

ディザスタリカバリ設定を行うには、NetScaler Console が高可用性モードで展開されていることを確認してください。NetScaler Console の高可用性展開の詳細については、「高可用性展開」を参照してください。

**注**

- 高可用性モードで展開された NetScaler Console は、NetScaler Console リリースバージョン 13.1 にアップグレードする必要があります。
- プライマリノードにディザスタリカバリノードを登録するには、**フローティング IP アドレスが必須です**。

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

### DR コンソールを使用して NetScaler Console ディザスタリカバリノードを展開および登録する

NetScaler Console ディザスタリカバリノードを登録するには:

1. NetScalerサイトから`.xva`イメージファイルをダウンロードし、ハイパーバイザーにインポートします。
2. **Console**タブから、NetScaler Consoleを初期ネットワーク構成で設定します。

   **注**

   災害復旧ノードは別のサブネットに配置できます。

   
3. 初期ネットワーク構成が完了すると、システムはログインを促します。次の資格情報を使用してログインします – `nsrecover` / `nsroot`。

   **重要**

   登録中にDRノードの資格情報 (`nsrecover` / `nsroot`) を変更しないでください。DRノードを正常に登録した後で、DRノードの資格情報を変更できます。
4. 災害復旧ノードを展開するには、「**/mps/deployment_type.py**」と入力してEnterキーを押します。NetScaler Console展開構成メニューが表示されます。

   
5. 災害復旧ノードを登録するには、**2**を選択します。

   
6. コンソールは、高可用性ノードのフローティングIPアドレスとパスワードを要求します。
7. フローティングIPアドレスとパスワードを入力して、災害復旧ノードをプライマリノードに登録します。

   

   災害復旧ノードが正常に登録されました。

   登録成功(/en-us/netscaler-application-delivery-management-software/media/agentdeploy.png)

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

**注**

- 災害復旧ノードにはGUIがありません。
- 登録が成功すると、サーバーにログオンするためのデフォルトの管理者資格情報は `nsroot` / `nsroot` です。

8. DRノードのパスワードを変更する場合は、次のスクリプトを実行します。

```
/mps/change_freebsd_password.sh <username> <password>
```

**例：**

```
/mps/change_freebsd_password.sh nsroot new_password
```

### NetScaler Console GUIを使用して災害復旧ノードを展開する

DRコンソールを使用して災害復旧ノードが正常に登録されたら、NetScaler Console GUIからDRノードを展開します。この手順により、NetScaler Consoleプライマリサイトから災害復旧設定が有効になります。

1. **システム > システム管理 > ディザスタリカバリ設定** に移動します。
2. **Disaster Recovery**ページで、**Deploy DR Node**を選択します。
3. 確認ダイアログボックスが表示されます。続行するには**Yes**をクリックします。

**注**

システムバックアップにかかる時間は、データサイズとWANリンク速度によって異なります。

NetScaler Console GUIでDRノードを正常に展開した後、DRノードのデータベースの状態、メモリ、CPU、およびディスク使用量を監視できます。

災害復旧設定を無効にするには、「**DRノードの削除**」を選択します。確認ダイアログボックスが表示されます。続行するには「**はい**」をクリックします。

DRノードを再度有効にするには、高可用性ペアのDRノードを再構成します。

1. ハイパーバイザーまたはSSHコンソールを使用してDRノードにログオンします。

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

2. (#deploy-and-register-the-pageadm-product-name-short-disaster-recovery-node-using-dr-console)で利用可能な手順に従って、DRノードを構成します。
3. NetScaler Console GUIを使用して災害復旧ノードを展開する。

詳細については、FAQを参照してください。

**重要**

- プライマリサイトで災害が発生したことを検出するのは管理者の責任です。
- プライマリサイトがダウンした後、災害復旧ワークフローは管理者によって手動で開始されます。
- 管理者は、リカバリサイトの災害復旧ノードでリカバリススクリプトを実行して、プロセスを手動で開始する必要があります。
- プライマリサイトでHAペアをアップグレードする場合、DRサイトのスタンドアロンノードも手動でアップグレードする必要があります。

## 災害後のワークフロー

災害後にプライマリサイトがダウンした場合、災害復旧ワークフローは次のように開始する必要があります。

1. 管理者は、プライマリサイトで災害が発生し、動作していないことを特定します。
2. 管理者はリカバリプロセスを開始します。
3. 管理者は、要件に基づいて、ディザスタリカバリノード（リカバリサイト）で次のいずれかのリカバリスクリプトを手動で実行する必要があります。

   - DRノードでSNMP、Syslog、およびAnalyticsを設定します。

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
     ```

   - DRノードをライセンスサーバーとしても設定します。

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -reconfig-ls
     <IP-address-of-the-primary-site>
     ```

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

4. 内部的には、NetScalerインスタンスは、新しいプライマリサイトとなったディザスタリカバリノードにデータを送信するように自動的に再構成されます。

   次の図は、プライマリサイトが災害に見舞われた後のディザスタリカバリワークフローを示しています。

   ディザスタリカバリワークフロー(/en-us/netscaler-application-delivery-management-software/media/drpostdisaster.png)

   **注:**

   DRサイトでスクリプトを起動すると、DRサイトが新しいプライマリサイトになります。DRユーザーインターフェイスにもアクセスできます。

## ディザスタリカバリ後

災害が発生し、管理者がリカバリスクリプトを起動すると、DRサイトが新しいプライマリサイトになります。

後で設定を元のサイトに戻したい場合は、「元のプライマリサイトへの設定の復元」を参照してください。

**重要**

- NetScaler Console 12.1.49.x以前のリリースをインストールしている場合、Citrixに連絡して、NetScaler Console（DRサイト）で元のライセンスを再ホストするための30日間の猶予期間が与えられます。
- 12.1.50.x以降のリリースでは、NetScaler ConsoleライセンスはDRサイトに自動的に同期されます（ライセンスについてCitrixに連絡する必要はありません）。
- インスタンスにプールライセンスを適用している場合、バージョン**11.1 65.x以降**、**12.1 58.x以降**、**13.0 47.x以降**のNetScalerインスタンス、およびNetScaler SDX **13.0 76.x以降**は、DRサイトでの自動ライセンスサーバー更新をサポートしています。その他のすべてのバージョンでは、インスタンスをDRサイトに手動で再構成する必要があります。

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

## 設定を元のプライマリサイトに戻す

災害後、設定されたディザスタリカバリ (DR) ノードが新しいプライマリサイトとなり、クライアントトラフィックはこのノードを経由します。

詳細については、「災害後のワークフロー」を参照してください。

元のプライマリサイトが災害から復旧し、すべての操作をプライマリサイトに移行することを決定した場合、元のプライマリサイトをDRノードの設定と一致するように再構成します。

開始する前に、プライマリサイトとDRサイトの両方がアクティブであることを確認してください。

DRサイトから元のプライマリサイトに変更を戻すには、次の手順を実行します。

1. 元のプライマリサイトにログインし、次のコマンドを実行します。

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
   ```

   このコマンドは、Syslog、SNMP、およびAnalyticsのみをプライマリサイトに構成します。

   プライマリサイトをNetScalerインスタンスのプールライセンスサーバーとして構成する場合は、次のコマンドを実行します。

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
   ```

   `-O` コマンドはDRサイトのIPアドレスを取得し、プライマリサイトをプールライセンスサーバーとして再構成します。

2. DRサイトを再構成します。「ディザスタリカバリセットアップの展開」を参照してください。

DRサイトから元のプライマリサイトへの設定の復元が正常に完了すると、クライアントトラフィックはNetScaler Consoleプライマリノードを経由します。

## スタンドアロンノードのディザスタリカバリを構成する

スタンドアロンモードで展開されたNetScaler Consoleのディザスタリカバリも構成できます。

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

次の表は、NetScaler Consoleでディザスタリカバリを構成する際に使用される用語について説明しています。

| 用語 | 説明 |
| --- | --- |
| プライマリサイト (データセンターA) | プライマリサイトには、スタンドアロンモードで展開されたNetScaler Consoleノードがあります。 |
| リカバリサイト (データセンターB) | リカバリサイトには、スタンドアロンモードで展開されたディザスタリカバリノードがあります。このノードは読み取り専用モードであり、プライマリサイトがダウンするまで動作しません。 |
| ディザスタリカバリノード | リカバリノードは、リカバリサイトに展開されたスタンドアロンノードです。プライマリサイトで障害が発生し、機能しなくなった場合に、このノードが動作可能になります（新しいプライマリとして）。 |

**注**

プライマリサイトとDRサイトは、ポート5454と22を介して相互に通信し、これらのポートはデフォルトで有効になっています。

ポートとプロトコルの詳細については、ポートを参照してください。

### ディザスタリカバリのワークフロー

プライマリサイトには、スタンドアロンモードで展開されたNetScaler Consoleノードがあります。

リカバリサイトには、リモートで展開されたディザスタリカバリノードがあります。ディザスタリカバリノードは読み取り専用モードで、プライマリノードからデータを受信してデータバックアップを作成します。リカバリサイトのNetScalerインスタンスも検出されますが、それらを介してトラフィックは流れません。バックアッププロセス中に、すべてのデータ、ファイル、および構成がプライマリノードからディザスタリカバリノードにレプリケートされます。

### 前提条件

ディザスタリカバリノードをセットアップする前に、以下の前提条件に注意してください。

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

- ディザスタリカバリ設定を有効にするには、プライマリサイトでNetScaler Consoleがスタンドアロンモードで構成されている必要があります。
- スタンドアロンのNetScaler Console（プライマリサイト内）とディザスタリカバリノード（DRサイト内）は、同じソフトウェアバージョン、ビルド、および構成である必要があります。

スケジューリング動作とネットワーク遅延を改善するために、CPU優先度（仮想マシンプロパティ内）を最高レベルに設定することをお勧めします。

次の表に、ディザスタリカバリノードを構成するための最小要件を示します。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| ストレージ容量 | NetScaler Consoleの展開には、ソリッドステートドライブ (SSD) テクノロジーの使用を推奨します。デフォルト値は120 GBです。実際のストレージ要件は、NetScaler Consoleのサイジング見積もりによって異なります。NetScaler Consoleのストレージ要件が120 GBを超える場合は、追加のディスクを接続する必要があります。**注** 追加できるディスクは1つだけです。初期展開時にストレージを見積もり、追加のディスクを接続することをお勧めします。詳細については、「NetScaler Consoleにディスクを追加する方法」を参照してください。 |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 Gbpsまたは100 Mbps |
| **ハイパーバイザー** | **バージョン** |
| シトリックス ハイパーバイザー | 6.2および6.5 |
| ヴイエムウェア イーエスエックスアイ | 5.5および6.0 |
| マイクロソフト ハイパーV | 2012 R2 |

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

| コンポーネント | 要件 |
| --- | --- |
| リナックス ケーブイエム | UbuntuおよびFedora |

## 初回ディザスターリカバリ設定

- NetScaler Consoleを展開する
- NetScaler Consoleディザスターリカバリノードを展開して登録する
- ユーザーインターフェイスからディザスターリカバリ設定を有効/無効にする

### NetScaler Consoleを展開する

ディザスターリカバリ設定を行うには、NetScaler Consoleがスタンドアロンモードで展開されていることを確認してください。詳細については、「シングルサーバー展開」を参照してください。

### DRコンソールを使用してNetScaler Consoleディザスターリカバリノードを展開して登録する

NetScaler Consoleディザスターリカバリノードを登録するには：

1. NetScalerサイトから`.xva`イメージファイルをダウンロードし、ハイパーバイザーにインポートします。
2. **Console**タブから、NetScaler Consoleを初期ネットワーク構成で設定します。

   **注**

   ディザスターリカバリノードは別のサブネットに配置できます。

   
3. 初期ネットワーク構成が完了すると、システムはログインを促します。次の資格情報を使用してログオンします – `nsrecover` / `nsroot`。

   **重要**

   登録中にDRノードの資格情報 (`nsrecover` / `nsroot`) を変更しないでください。DRノードを正常に登録した後で、DRノードの資格情報を変更できます。
4. ディザスタリカバリノードを展開するには、**/mps/deployment_type.py** と入力してEnterキーを押します。NetScaler Consoleの展開設定メニューが表示されます。

   設定メニュー(/en-us/netscaler-application-delivery-management-software/media/drstep4.png)

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

5. ディザスタリカバリノードを登録するには、**2** を選択します。

   ノードの登録(/en-us/netscaler-application-delivery-management-software/media/drstep5.png)

6. コンソールは、スタンドアロンノードのIPアドレスとパスワードを要求します。
7. ディザスタリカバリノードを登録するには、スタンドアロンノードのIPアドレスとパスワードを入力します。

   ディザスタリカバリノードが正常に登録されました。

   登録成功(/en-us/netscaler-application-delivery-management-software/media/agentdeploy.png)

   **注**

   - ディザスタリカバリノードにはGUIがありません。
   - 登録が正常に完了すると、サーバーにログオンするためのデフォルトの管理者資格情報は `nsroot` / `nsroot` になります。

8. DRノードのパスワードを変更する場合は、次のスクリプトを実行します。

   ```
   /mps/change_freebsd_password.sh <username> <password>
   ```

   **例：**

   ```
   /mps/change_freebsd_password.sh nsroot new_password
   ```

### NetScaler Console GUIを使用してディザスタリカバリノードを展開する

災害復旧ノードがDRコンソールを使用して正常に登録された後、NetScaler Console GUIからDRノードを展開します。この手順により、NetScaler Consoleプライマリサイトから災害復旧設定が有効になります。

1. **システム > システム管理 > 災害復旧設定** に移動します。
2. **Disaster Recovery**ページで、**Deploy DR Node**を選択します。
3. 確認ダイアログボックスが表示されます。続行するには**Yes**をクリックします。

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

**注**

システムバックアップにかかる時間は、データサイズとWANリンク速度によって異なります。

NetScaler Console GUIでDRノードを正常に展開した後、DRノードのデータベースの状態、メモリ、CPU、およびディスク使用量を監視できます。

災害復旧設定を無効にするには、**Remove DR Node**を選択します。確認ダイアログボックスが表示されます。続行するには**Yes**をクリックします。

DRノードを再度有効にするには、高可用性ペアのDRノードを再構成します。

1. ハイパーバイザーまたはSSHコンソールを使用してDRノードにログオンします。
2. DRコンソールを使用してNetScaler Console災害復旧ノードを展開および登録するで利用可能な手順に従って、DRノードを構成します。
3. NetScaler Console GUIを使用して災害復旧ノードを展開する。

詳細については、FAQを参照してください。

**重要**

- プライマリサイトで災害が発生したことを検出するのは、管理者の責任です。
- 災害復旧ワークフローは、プライマリサイトがダウンした後、管理者が手動で開始します。
- 管理者は、リカバリサイトの災害復旧ノードでリカバリスクリプトを実行して、プロセスを手動で開始する必要があります。
- プライマリサイトのスタンドアロンノードをアップグレードする場合、DRサイトのスタンドアロンノードも手動でアップグレードする必要があります。

### 災害後のワークフロー

災害後にプライマリサイトがダウンした場合、災害復旧ワークフローは次のように開始する必要があります。

1. 管理者は、プライマリサイトが災害に見舞われ、動作不能になっていることを確認します。
2. 管理者はリカバリプロセスを開始します。

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

3. 管理者は、要件に基づいて、災害復旧ノード（リカバリサイト）で次のいずれかのリカバリスクリプトを手動で実行する必要があります。

   - DRノードでSNMP、Syslog、およびAnalyticsを設定します。

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
     ```

   - DRノードをライセンスサーバーとしても設定します。

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -reconfig-ls
     <IP-address-of-the-primary-site>
     ```

4. 内部的には、NetScalerインスタンスは、新しいプライマリサイトとなった災害復旧ノードにデータを送信するように自動的に再構成されます。

   **注:**

   DRサイトでスクリプトを開始すると、DRサイトが新しいプライマリサイトになります。DRユーザーインターフェイスにもアクセスできます。

### 災害復旧後

災害が発生し、管理者がリカバリスクリプトを開始すると、DRサイトが新しいプライマリサイトになります。

後で設定を元のサイトに戻したい場合は、「元のプライマリサイトに設定を戻す」(#revert-configurations-to-the-original-primary-site)を参照してください。

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

**重要**

- NetScaler Console 12.1.49.x以前のリリースをインストールしている場合、Citrixに連絡して、NetScaler Console（DRサイト）で元のライセンスを再ホストするための30日間の猶予期間が与えられます。
- 12.1.50.x以降のリリースでは、NetScaler ConsoleライセンスはDRサイトに自動的に同期されます (ライセンスについてCitrixに連絡する必要はありません)。
- インスタンスにプールライセンスを適用している場合、バージョン**11.1 65.x以降**、**12.1 58.x以降**、**13.0 47.x以降**のNetScalerインスタンス、およびNetScaler SDX **13.0 76.x以降**は、DRサイトでの自動ライセンスサーバー更新をサポートしています。その他のすべてのバージョンでは、インスタンスをDRサイトに手動で再構成する必要があります。

### 元のプライマリサイトに設定を戻す

災害後、設定された災害復旧 (DR) ノードが新しいプライマリサイトとなり、クライアントトラフィックはこのノードを経由します。

災害後のセットアップ(/en-us/netscaler-application-delivery-management-software/media/disaster-recovery-node-active-console.png)

詳細については、「災害後のワークフロー」(#workflow-after-the-disaster)を参照してください。

元のプライマリサイトが災害から復旧し、すべての操作をプライマリサイトに移行することを決定した場合、元のプライマリサイトをDRノードの設定と一致するように再構成します。

開始する前に、プライマリサイトとDRサイトの両方がアクティブであることを確認してください。

DRサイトから元のプライマリサイトに変更を戻すには、次の手順を実行します。

1. 元のプライマリサイトにログインし、次のコマンドを実行します。

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
   ```

   このコマンドは、Syslog、SNMP、およびAnalyticsのみをプライマリサイトに構成します。

   プライマリサイトをNetScalerインスタンスのプールライセンスサーバーとして構成する場合は、次のコマンドを実行します。

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

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
password> -L <primary-node-password>  -O yes &
```

`-O` コマンドは、DRサイトのIPアドレスを取得し、プライマリサイトをプールされたライセンスサーバーとして再構成します。

2. DRサイトを再構成します。「」を参照してください(#first-time-disaster-recovery-setup)。

DRサイトから元のプライマリサイトに設定を正常に復元した後、クライアントトラフィックはNetScaler Consoleプライマリノードを介して流れます。

# マルチサイト展開のためのオンプレミスエージェントの構成

NetScaler Console の以前のバージョンでは、リモートデータセンターに展開された NetScaler インスタンスは、プライマリデータセンターで実行されている NetScaler Console から管理および監視できました。NetScaler インスタンスはデータをプライマリ NetScaler Console に直接送信していたため、WAN 帯域幅が消費されていました。また、分析データの処理には、プライマリ NetScaler Console の CPU およびメモリリソースが使用されていました。

データセンターは世界中に配置できます。エージェントは次のシナリオで重要な役割を果たします。

- WAN 帯域幅の消費を削減するために、リモートデータセンターにエージェントをインストールする。
- データ処理のためにプライマリ NetScaler Console に直接トラフィックを送信するインスタンスの数を制限する。

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

**注**

- リモートデータセンターのインスタンスにエージェントをインストールすることをお勧めしますが、必須ではありません。必要に応じて、ユーザーは NetScaler インスタンスをプライマリ NetScaler Console に直接追加できます。
- 1つ以上のリモートデータセンターにエージェントをインストールしている場合、エージェントとプライマリサイト間の通信はフローティングIPアドレスを介して行われます。詳細については、ポートを参照してください。
- 1つ以上のリモートデータセンターにエージェントをインストールし、プールされたライセンスをインスタンスに適用できます。このシナリオでは、プライマリサイトと1つ以上のリモートデータセンター間の通信はフローティングIPアドレスを介して行われます。
- NetScaler Console オンプレミスエージェントは、プールされたライセンスをサポートしていません。

NetScaler Console 12.1 以降では、インスタンスをエージェントで構成して、別のデータセンターにあるプライマリ NetScaler Console と通信できます。

エージェントは、プライマリ NetScaler Console と、異なるデータセンターにわたって検出されたインスタンスとの間の仲介役として機能します。エージェントをインストールする利点は次のとおりです。

- インスタンスはエージェントに構成され、未処理のデータはプライマリ NetScaler Console ではなくエージェントに直接送信されます。エージェントは最初のレベルのデータ処理を行い、処理されたデータを圧縮形式でプライマリ NetScaler Console に送信して保存します。
- エージェントとインスタンスは同じデータセンターに併置されているため、データ処理が高速になります。
- エージェントをクラスタリングすることで、エージェントのフェイルオーバー時に NetScaler インスタンスの再配布が可能になります。サイト内の1つのエージェントが故障した場合、NetScaler インスタンスからのトラフィックは、同じサイト内の別の利用可能なエージェントに切り替えられます。

  **注**

  サイトごとにインストールされるエージェントの数は、処理されるトラフィックによって異なります。

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

## アーキテクチャ

次の図は、2つのデータセンターにあるNetScalerインスタンスと、マルチサイトエージェントベースのアーキテクチャを使用したNetScaler Consoleの高可用性展開を示しています。



プライマリサイトには、高可用性構成で展開されたNetScaler Consoleノードがあります。プライマリサイトのNetScalerインスタンスは、NetScaler Consoleに直接登録されます。

セカンダリサイトでは、エージェントが展開され、プライマリサイトのNetScaler Consoleサーバーに登録されます。これらのエージェントはクラスターで動作し、エージェントのフェイルオーバーが発生した場合に継続的なトラフィックフローを処理します。セカンダリサイトのNetScalerインスタンスは、そのサイト内にあるエージェントを介してプライマリNetScaler Consoleサーバーに登録されます。インスタンスは、プライマリNetScaler Consoleではなく、エージェントに直接データを送信します。エージェントはインスタンスから受信したデータを処理し、圧縮された形式でプライマリNetScaler Consoleに送信します。エージェントはセキュアなチャネルを介してNetScaler Consoleサーバーと通信し、チャネルを介して送信されるデータは帯域幅効率のために圧縮されます。

## 基本認証を有効にする

基本認証は、次の目的で一時的に有効にする必要があります。

- エージェントとディザスタリカバリノードの初期登録を完了します。
- NetScaler GUIからライセンスアクティベーションシステム (LAS) のチェックアウトを開始します。

**注:**

基本認証は、初期登録にのみ必要です。

### 基本認証を構成する

1. **設定 > 管理 > システム設定 > システム、タイムゾーン、許可されたURL、およびエージェント設定** に移動します。
2. 「**基本設定**」をクリックします。
3. 「**基本認証を許可するを有効にする**」を選択します。
4. 「**OK**」をクリックします。

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

# はじめに

- データセンターにエージェントをインストールします
  - エージェントを登録します
  - エージェントをサイトにアタッチします
- NetScalerインスタンスを追加します
  - 新しいインスタンスを追加します
  - 既存のインスタンスを更新します

## データセンターにエージェントをインストールします

プライマリNetScaler Consoleと別のデータセンターにある管理対象のNetScalerインスタンス間の通信を有効にするために、エージェントをインストールして構成できます。

エンタープライズデータセンターの次のハイパーバイザーにエージェントをインストールできます。

- シトリックス ハイパーバイザー™
- ヴイエムウェア ESXi
- マイクロソフト ハイパーV
- Linux KVM サーバー

**注**

マルチサイト展開用のオンプレミスエージェントは、NetScaler Console の高可用性展開でのみサポートされます。

エージェントのインストールを開始する前に、ハイパーバイザーが各エージェントに提供する必要がある仮想コンピューティングリソースが確保されていることを確認してください。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| ストレージ容量 | 30 GB |

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

| コンポーネント | 要件 |
| --- | --- |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 ギガビット/秒 |

### ポート

通信のために、エージェントとNetScaler Consoleオンプレミスサーバーの間で以下のポートを開放する必要があります。

| タイプ | ポート | 詳細 | 通信方向 |
| --- | --- | --- | --- |
| TCP | 8443, 7443, 443 | エージェントとNetScaler Consoleオンプレミスサーバー間の送受信通信用。 | NetScalerエージェントからNetScaler Console |

エージェントとNetScalerインスタンスの間で、以下のポートを開放する必要があります。

| タイプ | ポート | 詳細 | 通信方向 |
| --- | --- | --- | --- |
| TCP | 80 | エージェントとNetScalerインスタンス間のNITRO通信用。 | NetScaler ConsoleからNetScalerへ、およびNetScalerからNetScaler Consoleへ |
| TCP | 22 | エージェントとNetScalerインスタンス間のSSH通信用。高可用性モードで展開されたNetScaler Consoleサーバー間の同期用。 | NetScaler ConsoleからNetScalerへ、およびNetScalerエージェントからNetScalerへ |
| UDP | 4739 | エージェントとNetScalerインスタンス間のAppFlow通信用。 | NetScaler から NetScaler Console へ |
| ICMP | 予約ポートなし | NetScaler ConsoleとNetScalerインスタンス間、または高可用 | |

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

| タイプ | ポート | 詳細 | 通信方向 |
|---|---|---|---|
| | | 性モードで展開されたセカンダリNetScaler Consoleサーバー間のネットワーク到達性を検出するため。 | |
| UDP | 161, 162 | NetScalerインスタンスからエージェントへのSNMPイベントを受信するため。 | ポート161 - NetScaler ConsoleからNetScaler |
| | | | ポート 162 ー NetScaler から NetScaler Console |
| UDP | 514 | NetScalerインスタンスからエージェントへのsyslogメッセージを受信するため。 | NetScaler から NetScaler Console |
| TCP | 5557 | エージェントとNetScalerインスタンス間のLogstream通信のため。 | NetScaler から NetScaler Console |

### エージェントを登録する

1. NetScalerサイトからダウンロードしたエージェントイメージファイルを使用し、ハイパーバイザーにインポートします。エージェントイメージファイルの命名パターンは次のとおりです。**MASAGENT-\<HYPERVISOR\>-\<Version.no\>.** 例: **MASAGENT-XEN-13.0-xy.xva**
2. **Console**タブから、NetScaler Consoleの初期ネットワーク構成を設定します。
3. NetScaler Consoleのホスト名、IPv4アドレス、およびゲートウェイIPv4アドレスを入力します。オプション7を選択して、構成を保存して終了します。

   
4. 登録が成功すると、コンソールはログオンを促します。資格情報として *nsrecover/nsroot* を使用します。

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

5. エージェントを登録するには、**/mps/register_agent_onprem.py** と入力します。NetScaler エージェントの登録資格情報は、次の図に示すように表示されます。
6. NetScaler ConsoleのフローティングIPアドレスとユーザー資格情報を入力します。



登録が成功すると、エージェントは再起動してインストールプロセスを完了します。

エージェントが再起動したら、NetScaler Console GUIにアクセスし、メインメニューから**Infrastructure > Instances > Agents**ページに移動して、エージェントのステータスを確認します。新しく追加されたエージェントは**Up**状態と表示されます。

**注**

NetScaler Consoleはエージェントのバージョンを表示し、エージェントが最新バージョンであるかどうかも確認します。ダウンロードアイコンは、エージェントが最新バージョンではなく、アップグレードが必要であることを示します。エージェントのバージョンをNetScaler Consoleのバージョンにアップグレードすることをお勧めします。

### エージェントをサイトにアタッチする

1. エージェントを選択し、**Attach Site**をクリックします。
2. 「**サイトの添付**」ページで、リストからサイトを選択するか、プラス（+）ボタンを使用してサイトを作成します。
3. 「**保存**」をクリックします。

**注**

- デフォルトでは、新しく登録されたすべてのエージェントはデフォルトのデータセンターに追加されます。
- エージェントを正しいサイトに関連付けることが重要です。エージェントに障害が発生した場合、そのエージェントに割り当てられているNetScalerインスタンスは、同じサイト内の他の機能しているエージェントに自動的に切り替わります。

## エージェントのアクション

「**インフラストラクチャ > エージェント > アクションの選択**」で、エージェントにさまざまなアクションを適用できます。

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

「**アクションの選択**」では、次の機能を使用できます。

新しい証明書のインストール: セキュリティ要件を満たすために別のエージェント証明書が必要な場合は、追加できます。

デフォルトパスワードの変更: インフラストラクチャのセキュリティを確保するために、エージェントのデフォルトパスワードを変更します。

テクニカルサポートファイルの生成: 選択したNetScalerエージェントのテクニカルサポートファイルを生成します。このファイルをダウンロードして、調査とトラブルシューティングのためにCitrixテクニカルサポートに送信できます。

## NetScalerインスタンスの追加

インスタンスとは、NetScaler Consoleからエージェントを介して検出、管理、監視したいNetScalerアプライアンスまたは仮想アプライアンスのことです。NetScaler Consoleまたはエージェントに、次のNetScalerアプライアンスおよび仮想アプライアンスを追加できます。

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler ゲートウェイ
- Citrix SSL フォワードプロキシ

詳細については、「NetScaler Consoleにインスタンスを追加する」(/ja-jp/netscaler-application-delivery-management-software/current-release/configure/add-instances.html)を参照してください。

### 既存のインスタンスをエージェントにアタッチする

インスタンスがすでにプライマリNetScaler Consoleに追加されている場合は、エージェントを編集することでそのインスタンスをエージェントにアタッチできます。

1. **Infrastructure > Instances**に移動し、インスタンスタイプを選択します。例: NetScaler。
2. 既存のインスタンスを編集するには、**Edit**をクリックします。
3. エージェントを選択するにはクリックします。
4. **Agent**ページで、インスタンスを関連付けるエージェントを選択し、**OK**をクリックします。

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

**注**

インスタンスを関連付ける**Site**を必ず選択してください。

### イベントを検証するためにインスタンスのGUIにアクセスする

インスタンスが追加され、エージェントが構成されたら、インスタンスのGUIにアクセスしてトラップ宛先が構成されているかどうかを確認します。

NetScaler Consoleで、**Infrastructure > Instances** に移動します。**Instances** で、アクセスするインスタンスのタイプ（例：NetScaler VPX）を選択し、特定のインスタンスのIPアドレスをクリックします。

選択したインスタンスのGUIがポップアップウィンドウに表示されます。

デフォルトでは、エージェントはインスタンスのトラップ宛先として構成されています。確認するには、インスタンスのGUIにログオンし、トラップ宛先を確認します。

**重要**

リモートデータセンターのNetScalerインスタンスにエージェントを追加することは推奨されますが、必須ではありません。

インスタンスをプライマリMASに直接追加したい場合は、インスタンスの追加時に**エージェント**を選択しないでください。

## NetScalerエージェントのフェイルオーバー

エージェントのフェイルオーバーは、2つ以上の登録済みエージェントがあるサイトで発生する可能性があります。サイトでエージェントが非アクティブ（DOWN状態）になると、NetScaler Consoleは非アクティブなエージェントのNetScalerインスタンスを他のアクティブなエージェントに再配布します。

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

**重要**

- **エージェントフェイルオーバー**機能がアカウントで有効になっていることを確認してください。この機能を有効にするには、「NetScaler Console機能の有効化または無効化」を参照してください。
- エージェントがスクリプトを実行している場合は、そのスクリプトがサイト内のすべてのエージェントに存在することを確認してください。これにより、エージェントのフェイルオーバー後に変更されたエージェントがスクリプトを実行できます。

NetScaler Console GUIでサイトをエージェントにアタッチするには、「エージェントをサイトにアタッチする」を参照してください。

エージェントのフェイルオーバーを実現するには、NetScalerエージェントを1つずつ選択し、同じサイトにアタッチします。

たとえば、2つのエージェント10.106.1xx.2xと10.106.1xx.3xがバンガロールサイトにアタッチされ、稼働しています。いずれかのエージェントが非アクティブになると、NetScaler Consoleはそれを検出し、状態をダウンとして表示します。

NetScalerエージェントがサイトで非アクティブ（ダウン状態）になると、NetScaler Consoleはエージェントがアクティブ（アップ状態）になるまで5分間待機します。エージェントが非アクティブのままの場合、NetScaler Consoleは同じサイト内の利用可能なエージェント間でインスタンスを自動的に再配布します。

NetScaler Console は、サイト内のアクティブなエージェント間で負荷を分散するために、30 分ごとにインスタンスの再配布をトリガーします。

## エージェントの到達不能しきい値と通知を構成する

エージェントがダウンしているか、特定の期間到達できない場合、電子メール、Slack、PagerDuty、ServiceNow を介してエージェントのステータスに関する通知を受け取ることができます。**Infrastructure > Instances > Agents** で、**Settings** をクリックし、期間を 5 分から 60 分の間で指定し、通知を受け取りたい通知方法を選択します。

エージェントのしきい値通知(/en-us/netscaler-application-delivery-management-software/media/agent-threshold-notification.png)

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

# NetScaler® Console エージェントと NetScaler Console 間のセキュアな通信

NetScaler Console エージェントと NetScaler Console 間のセキュアな通信は、バージョン 14.1-34.x 以降で利用可能です。Console サーバーの SSL 証明書を検証することで、このセキュアな通信を有効にできます。以前は、NetScaler Console エージェントと NetScaler Console オンプレミスサーバー間の通信は、Console サーバーの SSL 証明書を検証していなかったため、潜在的なセキュリティ脆弱性につながっていました。

このセキュアな通信を有効にするには：

1. NetScaler Console に SSL 証明書が構成されていることを確認します。
2. NetScaler Console エージェントにログインします。
3. CA ルート証明書を **/mpsconfig/console_onprem_cacert** に配置します。これはサーバー証明書の検証に使用されます。CA ルート証明書の名前は **cacert.pem** である必要があります。
4. 次のコマンドを実行して、セキュアな通信を構成します。
   **Configure_secure_communication_with_server.py**
5. これにより、NetScaler Console サーバーの FQDN (完全修飾ドメイン名) または IP アドレスの入力が求められます。
6. スクリプトの実行を完了するには、FQDN または IP アドレスを入力します。

   セキュアな通信(/en-us/netscaler-application-delivery-management-software/media/secure-communication-mitm.png)
7. スクリプトは、提供された CA ルート証明書を使用して、FQDN または IP アドレスによって提示されたサーバー証明書を検証します。証明書の検証が成功すると、セキュアな通信が有効になります。
8. このスクリプトは、エージェントがNetScaler Consoleに登録される前でも後でも呼び出すことができます。

**注：**

これはVMベースのエージェントにのみ適用されます。

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

# KubernetesクラスターにNetScaler®エージェントをマイクロサービスとしてインストールする

NetScaler Consoleをオンプレミスで使用している場合、コンテナエージェントは、いくつかの特定の戦略的および技術的な理由で使用されます。重要な理由のいくつかを以下に示します。

- **クラウドネイティブワークロードのシームレスな管理** - コンテナエージェントを使用する主な理由は、NetScaler CPX（NetScalerのコンテナ化されたバージョン）を管理するためです。
- **ローカライズされた制御**: エージェントは、オンプレミスのConsoleとKubernetesクラスター内で実行されているNetScaler CPXインスタンス間のライセンスプロキシとして機能します。
- **簡素化された接続（マイクロサービスアーキテクチャ）** - NetScaler ConsoleとKubernetesクラスターが異なるネットワーク上にある場合、コンテナエージェントは安全な「クラスター内」ゲートウェイとして機能します。

**注:**

- オンプレミスエージェントを構成し、Kubernetesクラスターがホストされているネットワークにエージェントを登録することもできます。
- NetScaler Consoleリリース14.1ビルド60.x以降、NetScaler Consoleは、コンテナ化されたコンソールエージェントの使用をサポートしています。コンテナ化されたコンソールエージェントを使用することで、KubernetesまたはOpenShiftプラットフォーム上の管理対象インスタンスの接続と監視が合理化されます。

## はじめに

1. NetScaler Consoleで、**Infrastructure > Instances > Agents**に移動します。
2. **Select Action**リストから、**Download Agent Microservice**オプションを選択します。
3. **Download Agent Microservice**ページで、次のパラメータを指定します。
    - **Application ID** – Kubernetesクラスター内のエージェントのサービスを定義し、同じクラスター内の他のエージェントとこのエージェントを区別するための文字列ID。
    - **Password** – NetScaler CPXのパスワードを指定します。このパスワードを使用して、エージェントを介してNetScaler CPXをNetScaler Consoleにオンボードします。
    - **Confirm Password** – 確認のために同じパスワードを指定します。

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

**注記:**

- デフォルトのパスワード ( `nsroot` ) を使用してはいけません。

4. **Download Yaml File** をクリックします。

## KubernetesクラスターにNetScalerエージェントをインストールする

Kubernetesメインノードで次の手順を実行します。

1. ダウンロードしたYAMLファイルを保存します。
2. 次のコマンドを実行します。

```
kubectl create -f <yaml file>
```

例:

```
kubectl create -f onprem6540.yaml
```

エージェントが正常に作成されました。

- [ ] NetScaler Consoleで、**Infrastructure > Instances > Agents** に移動してエージェントのステータスを確認します。

- [ ] エージェントを設定した後、NetScaler CPXインスタンスを追加し、サービスグラフで分析を表示できます。詳細については、以下を参照してください。

- NetScaler NetScaler CPXインスタンスをNetScaler Consoleに追加する
- サービスグラフのセットアップ

# NetScaler Console オンプレミス展開用の NetScaler Console エージェント OpenShift オペレーターをインストールする

NetScaler Console オンプレミスを使用している場合、コンテナエージェントはいくつかの特定の戦略的および技術的な理由で使用されます。重要な理由のいくつかを以下に示します。

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

- **クラウドネイティブワークロードのシームレスな管理** - コンテナエージェントを使用する主な理由は、NetScaler CPX (NetScaler のコンテナ化されたバージョン) を管理するためです。
- **ローカライズされた制御** - エージェントは、NetScaler Console オンプレミスと Kubernetes クラスター内で実行されている NetScaler CPX インスタンスの間でライセンスプロキシとして機能します。
- **接続の簡素化 (マイクロサービスアーキテクチャ)** - NetScaler Console と Kubernetes クラスターが異なるネットワーク上にある場合、コンテナエージェントは安全な「インクラスター」ゲートウェイとして機能します。

**注:**

NetScaler Console エージェントは、NetScaler Console オンプレミス 14.1.60.x 以降の NetScaler Console オンプレミス展開でサポートされています。

オペレーターは、Kubernetes アプリケーションを効果的、自動化され、スケーラブルな方法で展開および管理できるオープンソースツールキットです。管理者として、**NetScaler® ADM Agent Operator** を使用して OpenShift クラスターにエージェントを展開できます。

**注:**

OpenShift クラスターで構成されたエージェントは、デフォルトでは自動的にアップグレードされません。

## 前提条件

展開する前に、以下を確認してください。

- ポッドの権限を制御するための特権セキュリティコンテキスト制約があること。エージェントの場合、サービスアカウントに特権セキュリティコンテキスト制約を取得するには、次のコマンドを実行します。

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- エージェントログインシークレットを作成するには、次のコマンドを実行します (`loginsecret`):

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

```
oc create secret generic admlogin --from-literal=username=nsroot --
from-literal=password=<NetScaler Console-agent-password> -n <namespace>
```

- NetScaler Console Server のシークレットを作成するには、次のコマンドを実行します (`accessSecret`) シークレット:

```
oc create secret generic testonprem--from-literal=username=nsroot --
from-literal=password=< NetScaler Console password> -n <namespace>
```

## エージェントオペレーターをインストールする

1. OpenShiftクラスターコンソールにログオンします。
2. **Operators > OperatorHub** に移動します。
3. 検索バーにエージェント名を入力し、**NetScaler ADM Agent Operator** を選択して、**Install** をクリックします。

   NetScalerエージェントオペレーター (/en-us/netscaler-application-delivery-management-software/media/netscaler-agent-operator.png)
4. **Install Operator** ページには、2つのオプションがあります。

   a. **クラスター上のすべての名前空間 (デフォルト)** - エージェントオペレーターがクラスターで利用可能なすべての名前空間をサブスクライブできるようにし、クラスター上の任意の名前空間からエージェントオペレーターのインスタンスを起動できるようにします。

   b. **クラスター上の特定の名前空間** - エージェントオペレーターがクラスター上の選択された名前空間をサブスクライブできるようにし、選択された名前空間からのみエージェントオペレーターのインスタンスを起動できるようにします。

      この例では、エージェントオペレーターは **Default** という名前空間に割り当てられています。**Update approval** の下にある **Automatic** を選択し、**Install** をクリックします。

      NetScalerエージェントオペレーター (/en-us/netscaler-application-delivery-management-software/media/netscaler-install-operator.png)

      エージェントオペレーターが正常にサブスクライブされるまで待ちます。

      使用準備ができたNetScalerオペレーター (/en-us/netscaler-application-delivery-management-software/media/netscaler-agent-ready-to-use.png)

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

5. **Workloads > Pods** に移動し、`netscaler-adm-agent-operator-controller` ポッドが稼働していることを確認します。
6. ポッドが稼働した後、**NetScaler ADM Agent Operator** にコンソールエージェントの2つのインスタンスが表示されるはずです。エージェントをデプロイするには、**NetScaler ADM Agent Operator On Prem** をクリックします。

   NetScaler Operatorが提供するAPI (/en-us/netscaler-application-delivery-management-software/media/netscaler-agent-provided-api.png)
7. パラメータを更新するには、**YAMLビュー**を選択し、**作成**をクリックします。

   **注:**

   OpenShiftクラスターごとにエージェントのインスタンスが1つだけであることを確認してください。

   次の3つのパラメータは必須です。

   - `accessSecret`: `testonprem`という名前のシークレットが作成されます。
   - `AdmURL`: NetScaler ConsoleのIPアドレス。
   - `loginsecret`: `admlogin`という名前のシークレットが作成されます。

   ☐
   ☐
8. **ワークロード > Pods**に移動し、エージェントポッドが稼働していることを確認します。

   ☐

## エージェントインスタンスを削除する

**オペレーター > インストール済みオペレーター**に移動して、クラスターからエージェントのインスタンスを削除できます。**NetScaler ADM Agent Operator**タブでインスタンスを選択し、リストから**AdmAgentOnPremsの削除**を選択します。

☐

## エージェントオペレーターをアンインストールする

クラスターからエージェントオペレーターポッドをアンインストールしたい場合は、**Operators > Installed Operators** に移動し、リストから **Uninstall Operator** を選択します。

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

NetScaler Operator ADMエージェントのオンプレミスアンインストール(/en-us/netscaler-application-delivery-management-software/media/netscaler-agent-uninstall.png)

# エージェントのアップグレード

**注:**

エージェントのバージョンが14.1-38.x以降であることを確認してください。

14.1–43.50以降、NetScaler Console GUIを介してNetScalerエージェント（14.1-38.x以降）をアップグレードできます。この機能強化により、各エージェントの手動アップグレードワークフローが不要になり、単一のワークフローですべてのエージェントをアップグレードしたり、後でアップグレードをスケジュールしたりできるようになります。

## アップグレードワークフロー

1. **Infrastructure > Instances > Agents** に移動します。
2. **Upgrade Schedules** をクリックします。

   スケジュールされたアップグレード (/en-us/netscaler-application-delivery-management-software/media/agent-upgrade-schedules.png)
3. **Upgrade Schedules** ページで、**Add** をクリックします。
4. **Add Agents** をクリックし、アップグレードするエージェントをリストから選択して、**Next** をクリックします。

   **注:**

   ビルド14.1-38.x以降を実行しているエージェントのみが表示されます。

   エージェントの追加 (/en-us/netscaler-application-delivery-management-software/media/upgrade-agents-add.png)
5. **Select Image** タブで、ローカルまたはアプライアンスからイメージ (.tgz) を選択します。イメージは、ローカルコンピューターまたはアプライアンスからアップロードできます。**Appliance** を選択すると、NetScaler Console GUIに `/var/mps/mas_agent_images` に存在するイメージが表示されます。リストからイメージを選択します。

   イメージの選択 (/en-us/netscaler-application-delivery-management-software/media/upgrade-agents-image-select.png)

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

6. 画像を選択した後、「**次へ**」をクリックします。
7. 「**アップグレードスケジュール**」で「**今すぐアップグレード**」を選択して、すぐにアップグレードします。

   アップグレードをスケジュールする場合は、「**後でスケジュール**」を選択し、タイムゾーン、日付、時刻（24時間形式）を選択して詳細を指定します。
8. アップグレードワークフローの通知を受け取りたい場合は、「**通知**」の下にある「**通知の設定**」をクリックし、カテゴリ`AgentMonitoring`を選択し、通知を受け取りたい通信オプション（メール、SMS、Slack、PagerDuty、ServiceNow）を選択します。
9. 「**完了**」をクリックします。

# NetScaler Consoleシングルサーバー展開を高可用性展開に移行する

NetScaler Consoleシングルサーバーを、2台のNetScaler Consoleサーバーによる高可用性展開にアップグレードできます。NetScaler Consoleサーバーの高可用性ペアはアクティブ/パッシブモードで動作し、両方のサーバーは同じ構成を持ちます。このタイプのアクティブ/パッシブ展開では、一方のNetScaler Consoleサーバーがプライマリノードとして、もう一方がセカンダリノードとして構成されます。何らかの理由でプライマリノードがダウンした場合、セカンダリノードが引き継ぎます。詳細については、「高可用性展開の構成」を参照してください。

NetScaler Consoleシングルサーバーを高可用性ペアに移行するには、次の手順を実行する必要があります。

1. 単一のNetScaler Consoleサーバーにログオンします。
2. **Settings > Administration** に移動し、**High Availability Settings** の下にある **Configure NetScaler® Console High Availability (HA)** をクリックします。
3. **Configure NetScaler Console High Availability (HA)** ページで、次の操作を行います。
   a. セカンダリNetScaler ConsoleサーバーのIPアドレスを入力します。
   b. セカンダリノードのパスワードを指定します。
   c. フローティングIPアドレスを指定します。
   d. **Configure** をクリックします。

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

4. 確認ウィンドウで、**Yes** をクリックします。NetScaler Consoleインスタンスが再起動し、HAペアを形成します。
5. HAペアの構成が完了したら、プライマリNetScaler Consoleにログインし、**Settings > HA Deployment** に移動してプライマリノードとセカンダリノードを検証します。



# NetScaler Insight CenterからNetScaler Consoleへの移行

既存の構成、設定、またはデータを失うことなく、NetScaler Insight Centerの展開をNetScaler Consoleに移行できるようになりました。NetScaler Consoleを使用すると、アプリケーションに関連付けられたNetScalerインスタンスによって生成されたさまざまな分析を表示できるだけでなく、単一の統合コンソールからグローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングすることもできます。

**注**

現在、移行はNetScaler® Insight Centerスタンドアロンインスタンスでのみサポートされています。

## 前提条件

NetScaler Insight Center仮想アプライアンスをNetScaler Consoleに移行する前に、以下の要件が満たされていることを確認してください。

- NetScaler Insight Center 11.1 Build 47.14以降がインストールされていること。
- NetScaler Console 12.0 build 57.24 .tgzイメージファイルをダウンロード済みであること。

  **注**

  NetScaler Console 12.0 build 57.24をインストールし、その後最新のNetScaler Console 13.1ビルドにアップグレードする必要があります。詳細については、「アップグレード」を参照してください。

- NetScaler Console 13.1の最新ビルドの.tgzイメージファイルをダウンロード済みであること。

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

## ハードウェア要件

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 CPU |
| ストレージ容量 | 120 GB |
| | **注記** パフォーマンス向上のため、**500 GB**の使用を推奨します。また、CitrixはNetScaler Consoleの展開にソリッドステートドライブ（SSD）テクノロジーを使用することを推奨しています。 |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 Gbpsまたは100 Mbps |
| ハイパーバイザー要件 | |
| シトリックス ハイパーバイザー | 6.2、6.5 |
| ヴイエムウェア イーエスエックス | 5.5、6.0 |
| マイクロソフト Hyper-V | 2012 R2 |
| リナックス - KVM | ウブントゥ、フェドラ |

## インストール手順

**NetScaler Insight CenterをNetScaler Consoleに移行するには**:

1. NetScaler Insight Centerのシェルプロンプトにログオンします。
2. NetScaler Console 12.0 ビルド 57.24 を */var/mps/mps_images* フォルダーにダウンロードします。
3. **tar -zxvf build-mas-12.0-57.24.tgz**コマンドを使用してTGZファイルを解凍します。

   ▢
4. **./installmas**コマンドを使用してNetScaler Consoleをインストールします。

   ▢

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

5. NetScaler Console 12.0 build 57.24をインストールした後、上記の手順を実行して最新のNetScaler Console 13.1 buildにアップグレードする必要があります。

移行後、NetScaler Insight Centerインベントリで検出されたすべてのNetScalerインスタンスは、NetScaler Consoleの**Infrastructure > Instances**セクションに表示されます。ただし、初回は検出されたアプライアンスでホストされている仮想サーバーを手動でポーリングする必要があります。

**注**

NetScaler Consoleでは、デフォルトでは、検出されたNetScalerインスタンス内に作成された2つの仮想サーバーを管理および監視するためのライセンス費用はかかりません。2つを超える仮想サーバーを監視および管理するには、必要なNetScaler Consoleライセンスをインストールしてください。詳細については、NetScaler Console Licensingを参照してください。

# NetScaler Console と Citrix Director を統合する

Director は、ネットワーク分析とパフォーマンス管理のために NetScaler Console と統合されます。

- ネットワーク分析は、NetScaler Console から HDX Insight レポートを取得し、ネットワークのアプリケーションおよびデスクトップビューを提供します。この機能により、Director は展開における ICA トラフィックの高度な分析ビューを提供します。
- パフォーマンス管理は、履歴保持とトレンドレポートを提供します。リアルタイム評価と比較したデータの履歴保持により、容量や健全性のトレンドを含むトレンドレポートを作成できます。

NetScaler Console を Director と統合すると、HDX Insight レポートは Director で以下の情報を提供します。

- ページの タブには、展開全体におけるアプリケーション、デスクトップ、およびユーザーの遅延と帯域幅の影響が表示されます。
- ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

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

# 前提条件

## HDX Insight から NetScaler Console への移行のハードウェア要件

| コンポーネント | 要件 |
| --- | --- |
| RAM | 32 GB |
| 仮想CPU | 8 |
| ストレージ容量 | 500 GB。NetScaler Consoleの展開には、ソリッドステートドライブ（SSD）テクノロジーの使用をお勧めします。 |
| 仮想ネットワークインターフェース | 1 |
| スループット | 1 Gbpsまたは100 Mbps |

### 最小要件

ネットワーク統合を構成する前に、HDX™ Insightsアクセス権を持つRBACユーザーを作成していることを確認してください。

### ソフトウェア要件

NetScaler Console仮想アプライアンスに移行する前に、以下の要件が満たされていることを確認してください。

- Directorバージョン1811がインストールされていること
- NetScaler HDX Insightバージョン10.1以降がインストールされていること
- HDX InsightおよびNetScaler ConsoleがCitrix VDAバージョン7.0以降をサポートしていること
- Citrix WorkspaceがCitrix Virtual Apps and Desktopsバージョン7.0以降でサポートされていること
- 正確なICA RTTメトリックを表示するために、Mac版Citrix Workspaceバージョン11.8以降、およびWindows版Citrix Workspaceバージョン14.0以降が利用可能であることを確認してください。
- NetScaler Console バージョン 11.0 以降がインストールされている必要があります。NetScaler Console のインストール方法の詳細については、「NetScaler Console の展開」を参照してください。

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

### 制限事項

- この機能の利用可否は、組織のライセンスと管理者権限によって異なります。
- ICAセッションのラウンドトリップタイム (RTT) は、Citrix Workspace for Windows 3.4 以降および Citrix Workspace for Mac 11.8 以降で正しくデータが表示されます。これらの Workspace の以前のバージョンでは、データが正しく表示されません。
- トレンドビューでは、バージョン 7 より前の VDA の HDX 接続ログオンデータは収集されません。以前の VDA の場合、グラフデータは 0 と表示されます。
- ストレージ容量が 500 GB 未満の外部ハードディスクがすでに存在する展開環境では、別のハードディスクを追加することはできません。

**注**

- Director の詳細および NetScaler Console を Director と統合する手順については、`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.html>` を参照してください。
- HDX Insight の詳細については、`<http://docs.citrix.com/ja-jp/xenapp-and-xendesktop/7-11/director/hdx-insight.html>` を参照してください。

## NetScaler Console に追加ディスクを接続する

NetScaler Console のストレージ要件は、NetScaler Console のサイジング見積もりに基づいて決定されます。デフォルトでは、NetScaler Console は 120 GB のストレージ容量を提供します。データを保存するために 120 GB を超える容量が必要な場合は、追加ディスクを接続できます。

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

**注記：**

- ストレージ要件を見積もり、サーバーに追加ディスクを接続します。
- NetScaler Console のシングルサーバー展開の場合、デフォルトディスクに加えて、サーバーに接続できるディスクは 1 台のみです。
- NetScaler Console の高可用性展開の場合、各ノードに追加ディスクを接続する必要があります。両方のディスクのサイズは同じである必要があります。
- 容量の小さい既存の外部ディスクがある場合は、新しいディスクを接続する前にそのディスクを削除する必要があります。
- NetScaler Console の展開には、ソリッドステートドライブ (SSD) テクノロジーを使用することをお勧めします。

このドキュメントでは、追加の新しいディスクの接続、パーティションの作成、および追加ディスクのサイズ変更に関する次のシナリオについて説明します。

1. スタンドアロン NetScaler Console に追加ディスクを接続する
2. ディスクパーティションツールを起動する
3. 新しい追加ディスクにパーティションを作成する
4. 既存の追加ディスクのパーティションのサイズを変更する
5. 追加ディスクのパーティションを削除する

## スタンドアロン NetScaler Console に追加ディスクを接続する

1. NetScaler Console仮想マシンをシャットダウンします。
2. ハイパーバイザーで、必要なディスクサイズの追加ディスクをNetScaler Console仮想マシンに接続します。

   新しく接続された大容量ディスクには、データベースデータとNetScaler Consoleログファイルが保存されます。既存の120ギガバイトのデフォルトディスクは、コアファイル、オペレーティングシステムログファイルなどの保存に使用されます。
3. NetScaler Console仮想マシンを起動します。

## ディスクパーティションツールを起動する

NetScaler Consoleは、新しいコマンドラインツールである**NetScaler Consoleディスクパーティションツール**を提供するようになりました。

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

1. このツールを使用して、新しく追加された追加ディスクにパーティションを作成できます。
2. このツールを使用して、既存の追加ディスクのサイズを変更することもできます。ただし、既存の外部ディスクは2テラバイトを超えてはなりません。

   **注：**

   - 既存のディスクを2テラバイトを超えてサイズ変更すると、データ損失が発生する可能性があります。これは、プラットフォームの既知の制限によるものです。
   - 2テラバイトを超えるストレージ容量を作成するには、既存のパーティションを削除し、この新しいツールを使用してパーティションを作成する必要があります。

3. この新しいツールを使用すると、ディスクに対して任意のパーティション操作を明示的に実行できます。このツールは、ディスクと関連データに対する明確な可視性と制御を提供します。

   **注：**

   このツールは、NetScaler Consoleサーバーに接続した追加ディスクでのみ使用できます。このツールを使用して、プライマリ（デフォルト）ディスクにパーティションを作成することはできません。

ディスクパーティションツールを起動するには：

1. PuTTYなどのSSHクライアントを使用して、NetScaler ConsoleへのSSH接続を開きます。
2. `nsrecover/nsroot`資格情報を使用して、NetScaler Consoleにログオンします。
3. シェルプロンプトに切り替えて、次のように入力します。

   ```
   /mps/DiskPartitionTool.py
   ```

   

   **注:**

   高可用性展開のNetScaler Consoleの場合、両方のノードでツールを起動し、それぞれの仮想マシンにディスクを接続した後で、パーティションを作成またはサイズ変更する必要があります。

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

## 新しい追加ディスクにパーティションを作成する

新しいセカンダリディスクが追加されるたびに、パーティションを作成するために **create** コマンドが使用されます。このコマンドは、既存のパーティションが「remove」コマンドを使用して削除された後、既存のセカンダリディスク上にパーティションを作成するためにも使用できます。

**注:**

ディスクパーティションツールでパーティションを作成する際に、2テラバイトのサイズ制限はありません。このツールは2テラバイトを超えるパーティションを作成できます。ディスクをパーティション分割すると、32 GBのサイズのスワップパーティションが自動的に追加されます。その後、プライマリパーティションはディスク上の残りのすべての領域を使用します。

コマンドが実行されると、GUIDパーティションテーブル（GPT）パーティションスキームが作成されます。また、残りの領域を使用するために32 GBのスワップパーティションとデータパーティションが作成されます。その後、プライマリパーティションに新しいファイルシステムが作成されます。

**注:**

このプロセスには数秒かかる場合があり、中断しないでください。

「作成コマンド3」(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-4.png)

作成コマンドが完了すると、新しいパーティションをマウントするために仮想マシンが自動的に再起動されます。

「作成コマンド3」(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-5.png)

再起動後、新しいパーティションは/var/mpsにマウントされます。

「新しいパーティション」(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-6.png)

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

追加されたスワップパーティションは、「作成」コマンドの出力にスワップ領域として表示されます。

「スワップパーティション」(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-7.png)

**注:**

パーティションが作成された後、ツールは仮想マシンを再起動します。

## 既存の追加ディスク内のパーティションのサイズを変更する

接続されている（セカンダリ）ディスクのサイズを変更するには、**resize**コマンドを使用できます。`master boot record (MBR`)またはGPTスキームを持つディスクのサイズを変更できます。ディスクのサイズは2テラバイト未満である必要があります。

**注:**

- `resize`コマンドは、既存のデータを失うことなく機能するように設計されています。ただし、サイズ変更を行う前に、このディスクの重要なデータを外部ストレージにバックアップすることをお勧めします。データバックアップは、サイズ変更操作中にディスクデータが破損する可能性がある場合に役立ちます。
- パーティションのサイズを変更する際は、ディスク容量を100 GBずつ増やすようにしてください。このような段階的な増加により、頻繁にサイズ変更を行う必要がなくなります。

「パーティションのサイズ変更」(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-8.png)

「`resize`」コマンドはすべての前提条件をチェックし、すべての前提条件が満たされ、サイズ変更に同意した後で処理を進めます。これには、ディスクにアクセスしているプロセス（NetScaler Consoleサブシステム、PostgreSQL DBプロセス、NetScaler Consoleモニタープロセスを含む）を停止します。プロセスが停止すると、ディスクはサイズ変更の準備のためにアンマウントされます。サイズ変更は、パーティションを拡張して利用可能なすべての領域を占有し、その後ファイルシステムを拡張することによって行われます。ディスクにスワップパーティションが存在する場合、サイズ変更後にディスクの最後に削除され、再作成されます。スワップパーティションについては、ドキュメントの**Create**コマンドセクションで説明されています。

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

**注:**

「ファイルシステムの拡張」プロセスには時間がかかる場合があるため、進行中にプロセスを中断しないように注意してください。パーティションのサイズを変更した後、ツールは仮想マシンを再起動します。

サイズ変更プロセスにおけるすべての中間ステップ（アプリケーションの停止、ディスクのサイズ変更、ファイルシステムの拡張）はコンソールに表示されます。プロセスが完了すると、次のメッセージが表示されます。

再起動後、`df` コマンドを使用してサイズの増加を確認できます。サイズを増やした前後の詳細は次のとおりです。

## 追加ディスクのパーティションを削除する

セカンダリディスク上の既存のパーティションは、最大2テラバイトまでサイズ変更できます。この問題は、パーティションに関する既知の制限によるものです。2テラバイトを超えるディスクが必要な場合は、新しいディスクを接続し、ディスクパーティションツールを使用してパーティションを作成します。または、`remove` コマンドを使用して既存のパーティションを削除し、その後パーティションを作成することもできます。

**注:**

既存のパーティションを削除すると、すべての既存データが削除されます。したがって、このコマンドを使用する前に、重要なデータはすべて外部ストレージにバックアップする必要があります。

「remove」コマンドを実行すると確認が求められ、確認されると、セカンダリディスクを使用しているすべてのプロセス（NetScaler Consoleサブシステム、PostgreSQLプロセス、NetScaler Consoleモニターなど）が停止します。スワップパーティションが存在し、そのパーティションでスワップが有効になっている場合、スワップは無効になります。

「y」と入力すると、コマンドはディスクをアンマウントし、ディスク上のすべてのパーティションを削除します。

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

**注:**

パーティションを削除した後、ツールは仮想マシンを再起動します。

## 仮想マシンを再起動する

パーティションが作成またはサイズ変更された場合、またはスワップファイルが作成された場合は、仮想マシンを再起動してください。変更は再起動後にのみ有効になります。この目的のために、ツールには**reboot**コマンドが用意されています。

確認を求められ、確認後、すべてのプロセス（NetScaler Consoleサブシステム、PostgreSQLプロセス、NetScaler Consoleモニターなど）が停止します。その後、仮想マシンが再起動されます。

## ディスクデータのバックアップファイルを作成する

**注:**

バックアップファイルを作成するにはディスク容量が必要です。バックアップコマンドを実行する前に、十分なディスク容量（50%以上）があることを確認してください。

パーティションのサイズ変更または削除を行う前に、NetScaler Consoleデータをバックアップするには：

1. NetScaler Consoleを停止します。

   ```
   /mps/masd stop
   ```

2. PostgreSQL を停止します。

   ```
   su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
   ```

3. NetScaler Console Monitor を停止します。

   ```
   /mps/scripts/stop_mas_monit.sh
   ```

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

4. tarball を作成します。

```
cd /var

tar cvfz /var/mps/mps_backup.tgz mps
```

**注:**

この操作には、バックアップするデータのサイズによって時間がかかります。

5. チェックサムを生成します。

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
```

6. tarball とチェックサムファイルをリモートサーバーにコピーします。
7. コピーした tarball の正確性を検証します。転送されたファイルのチェックサムを生成し、ソースのチェックサムと比較します。
8. NetScaler Console 仮想マシンから tarball を削除します。

```
cd /var/mps/

rm mps_backup.tgz  mps_backup_checksum
```

## 追加コマンド

前述のコマンドに加えて、ツールで以下のコマンドも使用できます。

**ヘルプコマンド:**

サポートされているコマンドを一覧表示するには、**help** または **?** と入力して Enter キーを押します。各コマンドの詳細なヘルプを表示するには、**help** または **?** の後にコマンド名を入力し、**Enter** キーを押します。

**情報コマンド:**

「**info**」コマンドは、セカンダリディスクが存在する場合、そのセカンダリディスクに関する情報を提供します。このコマンドは、デバイス名、パーティションスキーム、人間が判読できる形式のサイズ、およびディスクブロックの数を提供します。スキームはMBRまたはGPTのいずれかで

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

す。MBRスキームは、NetScaler Consoleの以前のバージョンを使用してディスクがパーティション分割されたことを意味します。MBR/GPTベースのパーティションはサイズ変更できますが、2テラバイトを超えることはできません。GPTパーティションスキームは、NetScaler Console 12.1以降を使用してディスクがパーティション分割されたことを意味します。

**注:**

GPTパーティションは、作成時に2テラバイトを超えることができます。ただし、より小さいサイズのディスクを作成した後で、ディスクを2テラバイトを超えるサイズにリサイズすることはできません。この問題は、プラットフォームの既知の制限事項です。

**Create_swapfile コマンド:**

NetScaler Consoleのプライマリディスク上のデフォルトのスワップパーティションは4 GBであるため、デフォルトのスワップ領域は4 GBです。NetScaler Consoleのデフォルトのメモリ構成（2 GB）の場合、このスワップ領域で十分です。ただし、より高いメモリ構成でNetScaler Consoleを実行する場合、ディスク上により多くのスワップ領域を割り当てる必要があります。

**注:**

スワップパーティションは通常、オペレーティングシステムのインストール中にハードディスクドライブ（HDD）上に作成される専用のパーティションです。このようなパーティションはスワップ領域とも呼ばれます。スワップパーティションは、追加のメインメモリをシミュレートする仮想メモリに使用されます。

NetScaler Consoleの以前のバージョンで追加されたセカンダリディスクには、デフォルトではスワップパーティションが作成されません。「create_swapfile」コマンドは、スワップパーティションを持たない古いNetScaler Consoleバージョンを使用して作成されたセカンダリディスクを対象としています。このコマンドは以下を確認します。

- セカンダリディスクの存在
- ディスクがマウントされていること
- ディスクのサイズ（少なくとも500 GB）
- スワップファイルの存在

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

`create_swapfile` コマンドは、メモリが16 GB以上の場合にのみ有用であり、メモリが少ない場合には有用ではありません。そのため、このコマンドはスワップファイルの作成に進む前にメモリも確認します。

すべての条件が満たされ、ユーザーが続行に同意した場合、セカンダリディスクに32 GBのスワップファイルが作成されます。スワップファイルの作成プロセスには数分かかります。進行中にプロセスを中断しないように注意してください。正常に完了すると、スワップファイルを有効にするために再起動が行われます。

再起動後、topコマンドを使用してスワップの増加を確認できます。

**終了コマンド:**

ツールを終了するには、exitと入力し、**Enter**キーを押します。

## 高可用性で展開されたNetScaler Consoleに追加ディスクをアタッチする

セカンダリディスクなしで高可用性セットアップにNetScaler Consoleサーバーのペアを構成しているとします。また、2つ以上のNetScalerインスタンスを追加し、すべてのプロセスが実行されていることを確認済みであるとします。このセットアップの仮想マシンにセカンダリディスクを追加したい場合があります。高可用性セットアップでは、このタスクで詳述されているように、両方のノードに追加ディスクを追加する必要があります。

1. セカンダリノードをシャットダウンします。
2. ハイパーバイザーを介してディスクを追加します。

   **注:**

   セカンダリノードのメインディスクを拡張しないようにしてください。

3. セカンダリノードを起動します。
4. セカンダリノードでパーティションツールを実行します。
5. ディスクが追加された後、セカンダリノードが再起動します。
6. セカンダリノードが再起動した後、シャットダウンします。
7. プライマリノードをシャットダウンします。

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

8. ハイパーバイザーを介してディスクを追加します。

   **注:**

   プライマリノードのメインディスクを拡張しないようにしてください。

9. プライマリノードを起動します。
10. プライマリノードでパーティションツールを実行します。
11. ディスクが追加された後、プライマリノードが再起動します。
12. プライマリノードが稼働状態になったら、セカンダリノードを起動します。
13. セカンダリノードが稼働しており、データベースが同期されていることを確認します。
14. すべてのデータがまだ存在することを確認します。

**両方のノードでRAMの容量を増やすには:**

1. Console_Secondaryをシャットダウンし、必要に応じてRAMサイズを増やします。ノードを再起動しないでください。
2. Console_Primaryをシャットダウンし、必要に応じてRAMサイズを増やします。

   両方のノードでRAMサイズを均等に増やすようにしてください。たとえば、プライマリノードのRAMサイズを16 GBに増やす場合は、セカンダリノードでも同様に増やしてください。
3. Console_Primaryを再起動します。
4. Console_Primaryが再起動したら、それがプライマリノードであるかどうかを確認します。
5. Console_Secondaryノードを起動します。再起動後、セカンダリとして起動していること、およびDB同期が機能していることを確認します。
6. すべてのデータがまだ存在することを確認します。

   **注:**

   セカンダリディスクを追加した後、プライマリノードが起動するまでに時間がかかります。また、両方のノードにセカンダリディスクを追加し、RAM容量を増やすプロセス全体では、両方のノードがしばらくの間ダウンしている必要があります。このメンテナンスアクティビティを計画する際には、このダウンタイムを考慮してください。

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

# NetScaler Console を介した NetScaler MPX™ ディスク暗号化

**注:**

- ディスク暗号化は、NetScaler MPX 9100 インスタンスでのみサポートされています。
- NetScaler MPX 9100 インスタンスのディスク暗号化は、スタンドアロンの NetScaler Console でのみ有効にできます。
- リリース 14.1-56.x 以降、ディスク暗号化は、May 20, 2025 以降に製造された NetScaler MPX 9100、16000、および MPX 15000-50G インスタンスでサポートされています。

ディスク暗号化は、ストレージディスクに保存されている機密データを保護するために不可欠です。これにより、物理ストレージデバイスが侵害された場合でも、データにアクセスできなくなることが保証されます。NetScaler MPX の場合、ディスク暗号化は、`/var/core`、`/var/crash`、`/var/log`、`/var/nslog`、`/flash/nsconfig`、`/var/nstrace`、および `/var/temp` のような重要なディレクトリに対して、追加のセキュリティ層を提供します。

ディスク暗号化の利点の一部を次に示します。

- **保存データの保護**: システムの電源がオフになっているときに、機密データへの不正アクセスを防止します。
- **コンプライアンス**: データセキュリティに関する規制およびコンプライアンス要件を満たすのに役立ちます。
- **物理的な盗難リスクの軽減**: 盗難または紛失したストレージデバイス上の機密データや専有データにアクセスできないようにします。
- **セキュアブートプロセス**: 起動時に認証された資格情報を要求し、許可されたユーザーのみがシステムにアクセスできるようにします。
- **重要なデータのセキュリティ強化**: ログ、構成、クラッシュデータを不正アクセスから保護します。

NetScaler MPX 9100 のディスク暗号化は、**May 20, 2025** 以降に出荷されたビルド 14.1-47.x でのみサポートされており、ビルド 14.1-47.x を実行している NetScaler Console を介して有効にできます。各 NetScaler MPX インスタンスのディスク暗号化には、Thales CipherTrust Manager であ

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

るハードウェアセキュリティモジュール (HSM) サーバーによって管理されるキーが必要です。NetScaler MPX インスタンスは、NetScaler Console を使用して HSM サーバーからキーを取得します。

NetScaler MPX 9100、16000、および MPX 15000-50G のディスク暗号化は、**May 20, 2025** より前に出荷されたビルド 14.1-56.x でのみサポートされており、ビルド 14.1-56.x を実行している NetScaler Console を介して有効にできます。この機能を有効にするには、「NetScaler Console を介したインスタンスディスク暗号化」を参照してください。

**注:**

NetScaler Consoleは、HSMサーバーとしてThales CipherTrust Managerをサポートしています。

暗号化を成功させるには、HSMサーバーにNetScaler MPXインスタンスのシリアル番号を追加する必要があります。NetScaler MPXインスタンスのシリアル番号を追加すると、NetScaler ConsoleはHSMサーバーからインスタンスのシリアル番号を使用してキーを取得します。

ディスク暗号化が完了した後：

- NetScaler MPXインスタンスのディスクが取り外された場合、データにはアクセスできません。
- NetScaler MPXインスタンスを再起動した場合、NetScaler ConsoleがHSMサーバーからそのシリアル番号を使用してNetScaler MPXインスタンスを認証した後にのみ、再起動は成功します。

# 前提条件

以下を確認してください。

- 9100の場合、NetScaler MPXインスタンスはビルド14.1-47.xを実行しており、ビルド14.1-47.xを実行しているNetScaler Consoleオンプレミスで管理されています。

  **注記：**

  ディスク暗号化はNetScaler Consoleサービスではサポートされていません。

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

- NetScaler Consoleがインスタンスをシリアル番号で認証した後、キーを共有するために、HSM（Thales CipherTrust Manager）サーバーにNetScaler MPXインスタンスのシリアル番号を追加していること。
- NetScaler MPXインスタンスがNetScaler Consoleを通じてバックアップされていること。詳細については、NetScalerインスタンスのバックアップと復元を参照してください。
- MPX 16000およびMPX 15000-50Gの場合、NetScaler Consoleオンプレミスはリリース14.1ビルド56.xであること。

## HSM（Thales CipherTrust Manager）サーバーにインスタンスのシリアル番号を追加する

NetScaler MPXインスタンスを暗号化する前に、HSMサーバーにNetScaler MPXインスタンスのシリアル番号を追加する必要があります。

1. Thales CipherTrust Managerサーバーにログオンします。
2. 左側のペインで、 を選択し、 をクリックします。
3. で、`serialnumber` という名前のラベルを追加し、 テキストボックスにインスタンスのシリアル番号を指定し、 ボタンをクリックしてキーの詳細を追加してから、 をクリックします。

   ディスク暗号化キーの追加(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-add-key.png)
4. キーの詳細ページで、このキーの「エクスポート可能」トグルを有効にする必要があります。

   エクスポート可能トグルの有効化(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-exportable-toggle.png)

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

**注：**

- サポートされるキーの最大サイズは511バイトです。たとえば、AES-128とAES-256はサポートされています。512～4096のRSAキーはサポートされていません。
- サポートされているキーサイズのみを使用することをお勧めします。サポートされていないキーサイズを設定すると、NetScaler®インスタンスは失敗します。
- 正しいシリアル番号を指定していることを確認してください。シリアル番号が一致しない場合、暗号化プロセスは開始されません。
- NetScaler Consoleからインスタンスのシリアル番号をコピーすることをお勧めします。NetScaler Console GUIで、 **> >** の順に移動し、NetScaler MPXインスタンスを選択して、 リストから をクリックします。

# NetScaler Consoleによるインスタンスディスク暗号化

ディスク暗号化を開始する前に、NetScaler Consoleを介してMPXインスタンスのバックアップを取得していることを確認してください。詳細については、「インスタンスバックアップの構成」を参照してください。

バックアップを取得した後：

1. **> >** の順に移動します。
2. 「**NetScaler MPX**」タブで、管理対象インスタンスの詳細を確認できます。暗号化するインスタンスには、「**Disk Encryption Status**」の下に「**Plain Text**」と表示されます。

   
3. 「**Select Action**」リストから、「**Disk Encryption Settings**」をクリックします。

   
4. 「**Select Action**」リストから「**Promote device**」をクリックします。

**注:**

特にMay 20, 2025より前に製造されたMPXアプライアンスの場合、ディスク暗号化機能をアクティブにするには、「**Promote device**」オプションの選択が必須です。MPXアプライアンスがディスク暗号化対応デバイスへの変換を完了するまで、約30分かかります。



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

5. 「**ディスク暗号化設定**」ページで:

   a. NetScaler Consoleがシリアル番号を使用して暗号化キーを取得できるHSMサーバーのIPアドレス、ユーザー名、パスワードを指定します。

   b. **Key Manager Proxy**を有効にします。ディスク暗号化プロセスを続行するには、このオプションを有効にする必要があります。

   > **注:**
   >
   > 暗号化が完了した後でも、**Key Manager Proxy**が常に有効になっていることを確認してください。このオプションを無効にすると、インスタンスのアップグレード後やインスタンスの強制再起動などのシナリオで、暗号化されたインスタンスが正常に再起動しなくなります。

   c. 「**Save**」をクリックします。

6. インスタンスを選択し、**Select Action**リストから**Encrypt File System**をクリックします。

   ファイルシステムを暗号化(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-encrypt-file-system.png)

   確認ウィンドウが表示されます。続行するには**Yes**をクリックします。

7. NetScaler Consoleに、暗号化が開始され、インスタンスが約30分間**Down**ステータスになることを示す確認メッセージが表示されます。

   インスタンスのステータス(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-progress.png)

   インスタンスの状態は**Encryption in progress**と表示されます。

   インスタンスの状態(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-progress-status.png)

## 暗号化後の検証

インスタンスの暗号化は約30分で完了します。暗号化が完了したら、次のようになります。

- SSHクライアントを使用してNetScaler MPXインスタンスにログオンし、次のコマンドを使用して暗号化が成功したかどうかを検証できます。

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

`show filesystemencryption`

| 暗号化前 | 暗号化後 |
| --- | --- |
| 暗号化前(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-status-before.png) | 暗号化後(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-status-after.png) |

- NetScaler MPXインスタンスを再起動し、次の例に示すように、暗号化後に再起動が完了したかどうかを検証できます。

- 次のコマンドを使用して、**Key Manager Proxy** が正常に構成され、NetScalerからアクセスできるかどうかを検証できます。

  `show keymanagerproxy`

**注:**

暗号化後、NetScaler Consoleは`mpx_disk_encryption_default_profile`を使用してNetScaler MPXインスタンスにアクセスします。
`mpx_disk_encryption_default_profile`にはデフォルトの資格情報(`nsroot`/`nsroot`)があります。

## 暗号化後にNetScaler MPXインスタンスを復元する

バックアップを取得する前にデフォルトのパスワード (nsroot) を変更した場合は、暗号化後にバックアップ中に使用されたプロファイルがNetScaler Consoleで利用可能であることを確認してください。

## NetScaler MPX™ HAペアの暗号化後の動作

プライマリノードとセカンダリノードの両方が同じ暗号化ステータスである必要があります。プライマリノードとセカンダリノードの暗号化ステータスに不一致がある場合、両ノード間の同期は無効になります。SSHクライアントを使用してプライマリNetScaler® MPXインスタンスにログ

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

オンし、次のコマンドを使用して両ノードが同じ暗号化ステータスを表示しているかどうかを検証します。

`sh ha node`

HAペアの暗号化ステータス(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-ha-pair-encrypt-status.png)

2つのノードの暗号化ステータスが異なる場合:

- ディスク暗号化の不一致がある場合、次の出力が表示されます。

  HAペアの暗号化の不一致(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-ha-pair-mismatch.png)
- ディスク暗号化の不一致エラーは、HA同期の有効化、HAプロパティの有効化、およびHA同期の強制実行に対して表示されます。
  - `set ha node -haprop enabled`

    HAプロパティエラー(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-ha-pair-prop-error.png)
  - `set ha node -hasync enabled`

    HA同期エラー(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-ha-pair-sync-error.png)
  - `force ha sync`

    HA強制同期エラー(/en-us/netscaler-application-delivery-management-software/media/disk-encryption-ha-force-sync-error.png)

# 暗号化後のNetScaler MPX™クラスターの動作

クラスターを正常に形成するには、すべてのノードが同じ暗号化ステータスである必要があります。いずれかのノードの暗号化ステータスに不一致がある場合：

- 不一致のノードのヘルスステータスは **NOT UP** と表示され、そのノードはトラフィックを処理しません。

  
- クラスター内の不一致ノードの同期は無効になります。

  

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

- ノードをクラスターに追加できません。結合コマンドの失敗メッセージが表示されます：

  

- クラスターコマンドの伝播は無効になります。

  

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

# NetScaler Console クラウドコネクト

NetScaler Console Cloud Connect は、NetScaler Console on-prem から Citrix Cloud™ を介して NetScaler Console サービスへの安全なアウトバウンド接続を確立し、NetScaler Console on-prem でクラウド提供機能を利用できるようにします。

Cloud Connect を構成して、NetScaler Console on-prem で次の機能を使用できます。

- **LASベースのライセンス (エンタイトルメント配信)** - NetScaler Console on-prem で Cloud Connect が有効になっており、展開が LAS互換バージョンで実行されている場合、LAS は自動的に有効になります。ライセンスエンタイトルメントは自動的に取得および更新されます。詳細については、「ライセンスアクティベーションサービス」を参照してください。
- **アセット配信** - アセット配信は、認証、承認、監査、VPN、および GUI コンポーネントの受信リクエストを保護するために定義された組み込み WAF プロファイルに対して、暗号化された署名更新と暗号化されたスキーマ更新を提供します。Cloud Connect が有効になっている場合、アセット配信はデフォルトで有効になり、必要に応じて管理者は無効にできます。詳細については、「VPN仮想サーバーおよび認証仮想サーバーのWeb App Firewall保護」を参照してください。
- **アップグレードアドバイザリ** - NetScaler Console on-prem でアップグレードアドバイザリを使用するには、Cloud Connect を有効にする必要があります。Cloud Connect を有効にすると、NetScaler Console は最新のビルド情報を取得し、管理対象の NetScaler インスタンスのビルドと比較して、NetScaler Console on-prem での NetScaler インスタンスの EOL、EOM、および古いビルドを実行しているインスタンスを特定するのに役立ちます。Cloud Connect が有効になっている場合、アップグレードアドバイザリはデフォルトで有効になります。必要に応じて、管理者は無効にできます。詳細については、「アップグレードアドバイザリ」を参照してください。
- **ServiceNow統合** - この統合は、Citrix ITSMコネクタを使用してNetScaler ConsoleとServiceNowインスタンス間で通信します。NetScaler ConsoleとServiceNowの統合では、トークンベースの認証にITSMアダプターサービスを使用します。詳細については、「NetScaler ConsoleとServiceNowインスタンスの統合」を参照してください。

## 前提条件

Cloud Connect を構成する前に、次の前提条件を満たしていることを確認してください。

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

- インターネット接続があるか、Citrix Cloud にアクセスできるように NetScaler Console on-prem でプロキシサーバーが構成されていることを確認してください。
- Cloud Connect 構成のために NetScaler Console にアクセスするために使用するラップトップまたはマシンは、初期設定時にインターネット接続が必要です。詳細については、「FAQ」を参照してください。
- NetScaler Console サービスアカウントが利用可能であることを確認してください。
  - ステップ 1: Citrix Cloud アカウントを作成するか、既存の Citrix Cloud アカウントを使用してサインインします。Citrix Cloud アカウントの作成方法の詳細については、「Citrix Cloud アカウントの作成」を参照してください。
  - ステップ 2: NetScaler Console サービスを管理して、NetScaler Console サービステナントを作成します。NetScaler Console サービスの管理方法の詳細については、「はじめに」を参照してください。
- 次のエンドポイント URL へのアクセスを許可していることを確認してください。

| サービス | 政府機関向けクラウドのURL | APAC、EU、および米国リージョンのURL | 日本向けURL | なぜ必要ですか？ |
|---|---|---|---|---|
| トラストサービス | `*.citrixnetworkapi.us` | - | - | NetScaler ConsoleオンプレミスとCitrix Cloudサービス間の信頼を確立するために使用されます。 |
| | `trust.citrixnetworkapi.us` | `trust.citrixnetworkapi.net` | `trust.citrixnetworkapi.jp` | |
| サービスURL | `*.agent.adm.cloud.us` | `*.agent.adm.cloud.com` | `*.agent.adm.citrixcloud.jp` | これらは、Cloud Connect操作に使用されるNetScaler Consoleサービスエンドポイントです。NetScaler |

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

| サービス | 政府機関向けクラウドのURL | APAC、EU、および米国リージョンのURL | 日本向けURL | なぜ必要ですか？ |
|---|---|---|---|---|
| | | | | Consoleオンプレミスは、クラウド提供機能のためにこれらのエンドポイントへのアウトバウンド通信を開始します。 |
| | `*.adm.cloud.us` | `*.adm.cloud.com` | `*.citrixnetworkapi.jp` | |
| | `adm.cloud.us` | `adm.cloud.com` | `*.adm.citrixcloud.jp` | |
| | - | `netscalermas.cloud.com` | `adm.citrixcloud.jp` | エンドポイント、POP名などの顧客詳細を取得するために使用されます。 |
| Citrix Cloud™ 接続 | `citrix.cloud.us` | `Citrix.cloud.com` | `citrix.citrixcloud.jp` | Cloud Connect のオンボーディング中の認証とテナント選択に必要です。 |
| | `accounts.cloud.us` | `Accounts.cloud.com` | `accounts.citrixcloud.jp` | |

- NetScaler Console on-prem GUI にアクセスするブラウザで、ポップアップブロッカーを無効にしてください。
- (Government Cloud にのみ適用) Government Cloud リージョンエンドポイントに接続するには、NetScaler Console on-prem で次の手順を実行します。
  - NetScaler Console on-prem のシェルで、次のコマンドを実行します。

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

```
cd /mps/python/util/



python consoleService.py --region gov
```

**注:**

これらのコマンドは、NetScaler Console プロセスを再起動します。

- (Japan Cloud ユーザーにのみ適用) Japan リージョンエンドポイントに接続するには、NetScaler Console on-prem で次の手順を実行します。
  - NetScaler Console on-prem のシェルで、次のコマンドを実行します。

```
cd /mps/python/util/



python consoleService.py --region japan
```

**注:**

このコマンドは、NetScaler Console プロセスを再起動します。

- 次のポートを設定します。

```
-  443 (NetScaler Console on-prem/proxy to Cloud)

-  80 (NetScaler Console on-prem to proxy)
```

- Cloud Connect の設定に使用する NetScaler Console GUI ホストのブラウザのポップアップブロッカーを無効にします。

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

# Cloud Connect を構成する

## ワークフロー 1 – 新規ユーザー (Citrix Cloud アカウントなし、NetScaler Console サービステナントなし)

1. Citrix Cloud アカウントを作成します。詳細については、「Citrix Cloud アカウントの作成」を参照してください。
2. Citrix Cloud アカウントにサインインし、**NetScaler Console サービス**タイルをクリックします。ログインに成功すると、NetScaler Console サービステナント作成手順のページにリダイレクトされます。
   a. ビジネスニーズに合った**地域**を選択し、**完了**をクリックします。
   b. **役割**を選択してセットアップを完了します。詳細については、はじめにを参照してください。
3. NetScaler Consoleオンプレミスにログインし、**Cloud**アイコン > **Get Started**をクリックします。



4. **NetScaler Consoleサービスに接続**をクリックします。



   a. Citrix Cloudアカウントにログインします。
   b. アカウント名を選択してログインを完了します。
   c. 「ログイン成功」のメッセージが表示されます。

Cloud Connectの設定が完了し、Cloud Connectは**接続済み**ステータスを表示します。**Cloud Connect**設定ページから、**ServiceNow**などの統合を有効にするためにさらに進むことができます。

## ワークフロー2 – Citrix Cloudアカウントは存在するが、NetScaler Consoleサービステナントは存在しない

1. Citrix Cloudアカウントにサインインし、**NetScaler Consoleサービス**タイルをクリックします。ログインに成功すると、ページはNetScaler Consoleサービステナント作成手順にリダイレクトされます。
   a. ビジネスニーズに合った**地域**を選択し、**完了**をクリックします。
   b. **役割**を選択してセットアップを完了します。詳細については、はじめにを参照してください。

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

2. NetScaler Consoleで、**Cloud**アイコン > **Get Started**をクリックします。



3. **NetScaler Consoleサービスに接続**をクリックします。



   a. Citrix Cloudアカウントにログインします。
   b. ログインを完了するには、アカウント名を選択します。
   c. 「ログイン成功」のメッセージが表示されます。

Cloud Connectの設定が完了し、Cloud Connectは**接続済み**ステータスを表示します。**Cloud Connect**設定ページから、**ServiceNow**などの統合を有効にすることができます。

### ワークフロー3 - Citrix CloudアカウントとNetScaler Consoleサービステナントが存在する場合

1. NetScaler Consoleで、**Cloud**アイコン > **開始**をクリックします。



2. **NetScaler Consoleサービスに接続**をクリックします。



   a. Citrix Cloudアカウントにログインします。
   b. ログインを完了するには、アカウント名を選択します。
   c. 「ログイン成功」のメッセージが表示されます。

Cloud Connect の設定が完了し、Cloud Connect は **Connected** ステータスを表示しています。**Cloud Connect** 設定ページから、**ServiceNow** などの統合を有効にすることができます。

## Cloud Connect のプロキシ構成サポート

Cloud Connect は、認証なしおよび認証済みの両方のプロキシサーバーをサポートしています。プロキシサーバーの構成はオプションです。

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

**注:**

- NetScaler Console リリース 14.1-66.x 以降、Cloud Connect は明示的なプロキシ展開における SSL インターセプトをサポートしています。信頼できる通信を確立するには、プロキシの CA 証明書をアップロードしてください。SSL インスペクションを使用したプロキシ対応構成の証明書管理については、「CA 証明書の管理」を参照してください。
- 基本認証タイプがサポートされています。
- 以下のプロキシ構成タイプがサポートされています。
  - 明示的フォワードプロキシ (非インターセプト)
  - 明示的 SSL インターセプトプロキシ
  - 透過的 SSL インターセプトプロキシ

  プロキシ構成タイプの詳細については、「プロキシ構成のサポート」を参照してください。
- Cloud Connect は一部のサービス操作で WebSocket 通信を必要とするため、プロキシが WebSocket 接続を許可するように構成されていることを確認してください。

1. Cloud Connect 構成ページで、 をクリックします。

   

2. プロキシを有効にし、IP/FQDN とポートを入力します。
3. 必要に応じて、`Username` と `Password` を追加します。

   NetScaler Console サービスに接続します (/en-us/netscaler-application-delivery-management-software/media/proxy-server-configuration-fields.png)

# Cloud Connect のステータスと更新動作

## Cloud Connect のステータス

Cloud Connect のステータスは、オンプレミスの NetScaler Console と Citrix Cloud 間の接続の現在の健全性を反映します。サポートされている状態は次のとおりです。

- **接続済み** – 接続は正常で、正常に動作しています。
- **切断済み** – 接続は意図的に切断されています。
- **保留中** – Cloud Connect は確立中です。

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

- **エラー** – Cloud Connect 接続で問題が検出されました。

### Cloud Connect ステータスの更新

Cloud Connect のステータスは 6 時間ごとに自動的に更新されます。管理者は、**Cloud Connect ステータスの更新**を使用して、即座にステータス更新をトリガーすることもできます。

更新アクションは、必要なクラウドサービス URL の到達可能性を検証します。

**注:**

NetScaler Console リリース 14.1-73.x 以降、更新は **接続の確認**と統合されています。

## Cloud Connect の診断

「**Check Connectivity**」診断ツールは、NetScaler ConsoleオンプレミスとNetScaler Console サービス間の接続の問題を管理者がトラブルシューティングするのに役立ちます。

「**Check Connectivity**」ツールは、次のチェックを実行します。

- 必要なすべてのCloud Connectサービスエンドポイントの到達可能性チェック。
- 該当する場合、設定されたプロキシ設定を介した接続の検証。
- **WebSocket接続の検証:** Cloud Connectがクラウドサービスとの永続的な接続を維持するために使用するWebSocket通信を検証します。NetScaler Consoleリリース14.1-72.x以前では、このチェックはRefreshアクションの一部として実行されていました。
- **ダミーファイルのアップロードとダウンロードの検証:** LASベースのライセンスなど、すべてのCloud Connect機能のエンドツーエンド通信を検証します。NetScaler Consoleリリース14.1-72.x以前では、このチェックはRefreshアクションの一部として実行されていました。

診断結果には、次の情報が含まれます。

- 各サービスURLは「到達可能」または「到達不能」として表示されます。
- 障害は、詳細なエラーメッセージとともにUIに直接表示されます。

ネットワークまたはプロキシの問題を解決した後、管理者は次のアクションを実行する必要があります。

- 「**Check Connectivity**」を再実行します。
- 「**Refresh Cloud Connect Status**」を使用して、全体的な接続状態を更新します。



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

Cloud Connectがまだ完全に確立または接続されていない場合でも、CCIDを入力することで「**Check Connectivity**」を実行できます。この手順は、Cloud Connectに接続する前にすべての前提条件が満たされていることを確認するのに役立ちます。

「**Check Connectivity**」をクリックして、CCIDを入力してCCIDへの接続を確認し、Cloud Connectが完全に確立される前でもすべての前提条件が満たされていることを確認します。

クラウドコネクト - CCID検索(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-search-ccid.png)

Cloud Connect のすべての前提条件を表示するには、「**前提条件の表示**」をクリックします。

Cloud Connect - 前提条件の表示(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-prerequisite-list.png)

### エラー処理とメッセージング

診断とプロキシ検証に基づいて、次のエラーが観測される可能性があります。

- **SSL証明書の検証に失敗しました** – プロキシCA証明書が見つからないか無効であることを示します。このエラーは、SSL傍受プロキシが使用され、プロキシCA証明書がコンソールにアップロードされていない場合に発生します。

  Cloud Connect - SSL証明書の検証失敗(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-ssl-certificate-failure.png)
- **必要なサービスURLに到達できません** – プロキシ構成が正しく機能していないか、必要なURLがネットワークで許可されていないことを示します。

  Cloud Connect - プロキシ構成の失敗(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-proxy-failure.png)

## Cloud Connect ステータスの通知

NetScaler Console は、Cloud Connect ステータスの変更について管理者に通知を生成します。これらの通知は、アップグレードアドバイザリ、アセット配信、テレメトリベースのサービス、統合など、Cloud Connect に依存する機能に影響を与える可能性のある Cloud Connect 接続の問題について管理者に警告します。

Cloud Connect 通知は、オンプレミスの NetScaler Console と Citrix Cloud 間の接続状態に変化があったときにトリガーされます。これには以下が含まれます。

- Cloud Connect が「接続済み」から「切断済み」または「エラー」に移行した場合

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

- Cloud Connect が「切断済み」または「エラー」から「接続済み」に戻った場合

**設定 > システムイベント** で Cloud Connect のステータスイベントを表示することもできます。

「Cloud Connect - システムイベント 1」(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-system-events-1.png)

「Cloud Connect - システムイベント 2」(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-system-events-2.png)

## 通知頻度

Cloud Connectが`Disconnected`または`Error`の状態のままである場合、6時間ごとに通知が送信されます。Cloud Connectの接続が復元されると、復旧を示す単一の通知が送信されます。

## 通知チャネル

Cloud Connectの通知は、標準のNetScaler Console通知フレームワークを通じて配信され、**システムイベント通知**を使用して構成できます。サポートされている通知チャネルは次のとおりです。

- メール
- スラック
- PagerDuty
- ServiceNow

## 通知の管理

Cloud Connectのステータス通知は、デフォルトで有効になっています。必要に応じて、メール通知を無効にできます。メール通知を無効にするには：

1. **設定 > 管理 > イベント通知とダイジェストの構成**に移動します。
2. **イベント通知 > システム通知の構成**で、**CloudConnectStatus**を検索します。
3. **CloudConnectStatus**システムイベントカテゴリを削除し、**保存**をクリックします。

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

# Cloud Connect を介して収集されるデータ

**重要:**

Cloud Connect は NetScaler テレメトリプログラムのチャネルではありません。テレメトリは自動有効化されたチャネルを使用して収集されます。テレメトリ関連の情報については、「NetScaler テレメトリプログラム」を参照してください。

NetScaler Console オンプレミスで Cloud Connect が有効になっており、LAS互換バージョンを使用している場合、LAS は自動的に有効になります。LAS 関連ワークフローの一部として収集される情報の詳細については、「License Activation Service」を参照してください。

# Cloud Connect 接続の問題のトラブルシューティング

- 問題: サインイン中にポップアップがブロックされる

  解決策: ブラウザのポップアップブロッカーを無効にして、Cloud Connect のオンボーディングを再試行してください。

- 問題: エンドポイントがブロックされる

  解決策: ダウンロード/信頼/サービスおよび Citrix Cloud ドメイン（または日本リージョン相当）の許可リストを確認してください。

- 問題: LAS グレース期間の警告

  NetScaler Console オンプレミスが Citrix Cloud に到達できること（直接またはプロキシ経由）を確認してください。エンタイトルメントブロブは自動的に更新されます。繰り返し失敗すると、グレース期間とアラートがトリガーされます。

# その他のオプション

Cloud Connect を有効にすると、次のオプションを使用できます。

- **テナントの変更** - 既存のテナントを変更できます。「**テナントの変更**」をクリックすると、新しいタブにリダイレクトされ、Citrix Cloud にサインインする必要があります。サインインに成功すると、別のテナントを選択できます。

  プロキシの変更(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-modify-tenant.png)

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

- **プロキシの変更** - NetScaler Consoleオンプレミスでプロキシ設定を構成できます。この操作は、NetScaler Consoleが管理ネットワークを介してインターネットに直接アクセスできない場合に必要です。リストから**プロキシの変更**をクリックし、詳細を更新して、**保存**をクリックします。

  プロキシの変更(/en-us/netscaler-application-delivery-management-software/media/cloud-connector-modify-proxy.png)

- **切断** - Cloud Connect機能を無効にします。無効にすることを選択した場合、Cloud Connectの一部として有効になっているすべての機能が動作を停止します。

  無効にするには、リストから**切断**をクリックします。

  Cloud Connectを無効にする(/en-us/netscaler-application-delivery-management-software/media/disconnect-cloud-connect.png)

- **接続設定** - この設定を無効にすると、サンプルファイルのアップロードおよびダウンロードの検証チェックがオフになります。その結果、LASライセンスなどの機能に影響を与える可能性のある問題が、事前に検出されない可能性があります。

  Cloud Connect診断でファイルアップロードチェックを有効にする(/en-us/netscaler-application-delivery-management-software/media/enable-file-upload.png)

## ビルド固有の機能動作

次の表は、さまざまなNetScaler ConsoleオンプレミスビルドにおけるCloud Connectを介した機能の可用性を示しています。

| ビルド | CLOUD CONNECTで利用可能な機能 | 必要なアクション | CLOUD CONNECTを介したデータ収集 |
|---|---|---|---|
| 14.1-66.x以降 | LASベースのライセンス | Cloud Connect の構成 | いいえ |
| | ServiceNow 統合 | | |
| | アセット配信 | | |
| | アップグレードアドバイザリ | | |
| 14.1-56.x 以降 | LASベースのライセンス | Cloud Connect の構成 | いいえ |

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

| ビルド | CLOUD CONNECTで利用可能な機能 | 必要なアクション | CLOUD CONNECTを介したデータ収集 |
|---|---|---|---|
| | ServiceNow 連携 | | |
| | アセット配信 | | |
| 14.1-51.x 以降 | LASベースのライセンス | Cloud Connect の構成 | いいえ |
| | ServiceNow連携 | | |
| 14.1-25.x以降 | ServiceNow連携 | Cloud Connectを設定し、ServiceNow連携を有効にします。 | いいえ |
| 14.1-8.xから14.1-21.xの間 | セキュリティアドバイザリとServiceNow連携 | Cloud Connectを設定し、機能を有効にします | はい。Cloud Connectを設定した後。詳細については、Cloud Connectのデータガバナンスを参照してください。 |
| 14.1-4.x以前 | 該当なし | NA | NA |

# よくある質問

1. ラップトップの許可リストに追加する必要がある正確なURLは何ですか？

   適切な接続を確保するために、NetScaler Consoleサービスアカウントの環境に基づいて、以下のURLをブラウザの許可リストに追加してください。

   - 商用クラウド
     - トラストサービス
     - シトリックス クラウド
     - Citrix Cloudアカウント
   - 日本クラウド
     - トラストサービス

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

    - シトリックス クラウド
    - Citrix Cloudアカウント
  - 政府機関向けクラウド
    - トラストサービス
    - シトリックスクラウド

2. Cloud Connect は、NetScaler インスタンスに構成をプッシュしますか？

   いいえ。Cloud Connect は NetScaler インスタンスに構成をプッシュしません。NetScaler Console オンプレミスへのクラウド提供サービスを有効にし、ライセンスまたはアセットの配信を容易にするだけです。

3. Citrix Cloud から私の環境へのインバウンド接続はありますか？

   いいえ。Cloud Connect は、NetScaler Console オンプレミスから開始されるアウトバウンドのみの通信を使用します。

4. NetScaler インスタンスを NetScaler Console サービスに移行する必要がありますか？

   いいえ。Cloud Connect の機能を使用するために、インスタンスを NetScaler Console サービスに移行する必要はありません。

5. どのプロキシ認証タイプがサポートされていますか？

   Cloud Connect はプロキシ経由で使用できます。基本認証と認証なしのプロキシ統合の両方をサポートしています。

6. Cloud Connect を介してセキュリティアドバイザリはまだ有効になっていますか？

   特定の古い 14.1 ビルド (8.x から 21.x) のみです。それ以降のビルドでは、Cloud Connect は主にこのトピックで説明されている機能を有効にします。ビルド 14.1-25.x 以降では、セキュリティアドバイザリは自動有効化チャネルを通じて使用できます。詳細については、自動テレメトリ収集モード を参照してください。

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

# 設定

NetScaler Consoleサーバーには、GUIを使用してのみアクセスできます。インスタンスの追加、インスタンスとアプリの管理と監視、分析の表示、およびNetScaler Consoleサーバーの設定を行うには、GUIにアクセスする必要があります。

ワークステーションには、構成ユーティリティとダッシュボードにアクセスするためにサポートされているWebブラウザが必要です。

以下のブラウザがサポートされています。

| WEBブラウザ | バージョン |
| --- | --- |
| インターネットエクスプローラー | 11.0以降 |
| グーグルクローム | Chrome 19以降 |
| サファリ | Safari 5.1.1以降 |
| モジラファイアフォックス | Firefox 3.6.25以降 |

**NetScaler Console GUIにアクセスするには：**

管理者資格情報を使用してNetScaler Consoleにログオンします。

NetScaler Consoleにログオンした後、開始するには、次の操作を行う必要があります。

- NetScaler Consoleにインスタンスを追加する。これらのインスタンスを管理および監視するには、NetScaler Consoleサーバーにインスタンスを追加する必要があります。
- 仮想サーバーでアナリティクスを有効にする。アプリケーショントラフィックフローのアナリティクスデータを表示するには、特定のアプリケーションのトラフィックを受信する仮想サーバーでアナリティクス機能を有効にする必要があります。
- NetScaler ConsoleでNTPサーバーを構成する。NetScaler Consoleのクロックを NTPサーバーと同期させるには、NetScaler Consoleでネットワークタイムプロトコル (NTP) サーバーを構成する必要があります。
- NetScaler Consoleの最適なパフォーマンスのためのシステム設定を構成する。NetScaler Consoleを使用してインスタンスとアプリケーションの管理と監視を開始する前に、NetScaler

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

Consoleサーバーの最適なパフォーマンスを確保するためのいくつかのシステム設定を構成することをお勧めします。

# NetScaler Consoleにインスタンスを追加する

インスタンスとは、NetScaler Consoleから検出、管理、監視したいNetScalerアプライアンスまたは仮想アプライアンスのことです。これらのインスタンスを管理および監視するには、NetScaler Consoleサーバーにインスタンスを追加する必要があります。NetScaler Consoleには、次のNetScalerアプライアンスおよび仮想アプライアンスを追加できます。

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- ネットスケーラー ゲートウェイ

インスタンスは、NetScaler Consoleサーバーを初めてセットアップするとき、または後で追加できます。その後、NetScaler Consoleがインスタンスにアクセスするために使用できるインスタンスプロファイルを指定する必要があります。

**注:**

- NetScaler Consoleは、通信にNetScalerインスタンスのNetScaler IP (NSIP) アドレスを使用します。NetScalerインスタンスとNetScaler Consoleの間で開いている必要があるポートについては、「ポート」を参照してください。
- NetScaler Consoleがインスタンスを検出する方法については、「インスタンスの検出」を参照してください。

## NetScalerプロファイルの作成方法

NetScalerプロファイルには、NetScaler Consoleにインスタンスを追加するための資格情報、ポート、および認証タイプが含まれています。インスタンスタイプごとに、デフォルトプロファイルが利用可能です。たとえば、`nsroot` はNetScalerインスタンスのデフォルトプロファイルです。デフォルトプロファイルは、デフォルトのNetScaler管理者資格情報を使用して定義されます。インスタンスのデフォルト管理者資格情報を変更した場合は、それらのインスタンスのカスタムインスタンスプロファイルを定義できます。インスタンスが検出された後にインスタンスの資格情報を

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

変更した場合は、インスタンスプロファイルを編集するか、プロファイルを作成してから、インスタンスを再検出する必要があります。

NetScalerプロファイルは、**インスタンス**ページから、またはインスタンスの追加または変更中に作成できます。

**注記:**

インスタンスプロファイルを作成するには、スーパー管理者アカウントを使用してください。

**インスタンスページからNetScalerプロファイルを作成するには:**

1. **Infrastructure > Instances** に移動します。
2. インスタンスを選択します。例: NetScaler。
3. NetScalerページで、**Select Action** の下にある **Profiles** を選択します。



4. **Admin Profiles** ページで、**Add** を選択します。



5. **Create NetScaler Profile** ページで、次の操作を行います。



   a. **Profile Name**: NetScalerインスタンスのプロファイル名を指定します。
   b. **User Name**: NetScalerインスタンスにログオンするためのユーザー名を指定します。
   c. **Password**: NetScalerインスタンスにログオンするためのパスワードを指定します。
   d. **SSH Port**: NetScaler ConsoleとNetScalerインスタンス間のSSH通信に使用するポートを指定します。
   e. **HTTPポート**: NetScaler ConsoleとNetScalerインスタンス間のHTTP通信に使用するポートを指定します。

      **注:**

      デフォルトのHTTPポートは80です。NetScaler CPXインスタンスで構成した、デフォルト以外のカスタムHTTPポートを指定することもできます。カスタムHTTPポートは、NetScaler ConsoleとNetScaler CPX間でのみ通信に使用できます。

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

f. **HTTPSポート**: NetScaler ConsoleとNetScalerインスタンス間のHTTPS通信に使用するポートを指定します。

> **注:**
>
> デフォルトのHTTPSポートは443です。NetScaler CPXインスタンスで構成した、デフォルト以外のカスタムHTTPSポートを指定することもできます。カスタムHTTPSポートは、NetScaler ConsoleとNetScaler CPX間でのみ通信に使用できます。

g. **NetScaler通信にグローバル設定を使用**: NetScaler ConsoleとNetScalerインスタンス間の通信にシステム設定を使用する場合は、このオプションを選択します。それ以外の場合は、HTTPまたはHTTPSのいずれかを選択します。

h. **SNMPバージョン**: **SNMPv2**または**SNMPv3**のいずれかを選択し、次の操作を行います。

   i. SNMPv2を選択した場合は、認証用の**コミュニティ**名を指定します。

   ii. SNMPv3を選択した場合は、**セキュリティ名**と**セキュリティレベル**を指定します。セキュリティレベルに基づいて、**認証タイプ**と**プライバシータイプ**を選択します。

> **注:**
>
> NetScaler SDXでは、**SNMPv2**のみがサポートされています。

i. **タイムアウト設定**: 再起動後、NetScaler ConsoleがNetScalerインスタンスに接続要求を送信するまでに待機する時間を指定します。

j. **作成**を選択します。

## NetScalerインスタンスをNetScaler Consoleに追加する

インスタンスは、NetScaler Consoleサーバーを初めてセットアップするとき、または後で追加できます。

インスタンスを追加するには、各NetScalerインスタンスのホスト名またはIPアドレス、あるいはIPアドレスの範囲を指定する必要があります。

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

**注:**

- クラスターで構成されたNetScalerインスタンスを追加するには、クラスターIPアドレスまたはクラスター設定内の個々のノードのいずれかを指定する必要があります。ただし、NetScaler Consoleでは、クラスターはクラスターIPアドレスのみで表されます。
- HAペアとして設定されたNetScalerインスタンスの場合、1つのインスタンスを追加すると、ペア内のもう一方のインスタンスが自動的に追加されます。

エージェントで構成されたリモートデータからインスタンスを追加すると、トラフィックソースはエージェントを介して行われます。

**NetScaler Consoleにインスタンスを追加するには：**

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Infrastructure > Instances > NetScaler** に移動します。追加するインスタンスのタイプ（例：NetScaler VPX）を選択し、**Add** をクリックします。

   

3. 次のいずれかのオプションを選択します。

   - **デバイスIPアドレスを入力** - NetScalerインスタンスの場合、次のいずれかを指定します。
     - ホスト名
     - 各NetScalerインスタンスのIPアドレスまたはNAT IP
     - IPアドレスの範囲

     例えば、1つ以上のホスト名、IPアドレスまたはNAT IP、および/またはIPアドレスの範囲（例：10.10.20.10-10.10.20.45）をコンマ区切りで入力します。NAT HAインスタンス検出の入力形式は `10.10.20.10#10.10.20.32` (両方のNetScaler HAインスタンスのNAT IPアドレス) です。

     SNIPを使用してNetScaler HAペアを検出する場合は、独立ネットワーク構成 (INC) モードが有効になっていることを確認してください。そして、SNIPアドレスを次の形式で指定します。

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     ```

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

- **ファイルからインポート** - ローカルシステムから、追加するすべてのインスタンスのIPアドレスを含むテキストファイルをアップロードします。

4. **プロファイル名**から、適切なインスタンスプロファイルを選択するか、+アイコンをクリックしてプロファイルを作成します。
5. **サイト**から、インスタンスを追加する場所を選択するか、**+**アイコンをクリックして場所を作成します。
6. **OK**をクリックして、NetScaler Consoleにインスタンスを追加するプロセスを開始します。

**注:**

インスタンスを再検出する場合は、**Infrastructure > Instances > NetScaler**に移動します。インスタンスタイプ（例：VPX）を選択し、再検出するインスタンスを選択してから、**Select Action**リストから**Rediscover**をクリックします。

## NetScaler ConsoleにNetScaler CPXインスタンスを追加する

NetScaler Consoleは、CPX機能で達成された改善をサポートするように強化されました。NetScaler CPXインスタンスは、CPXのIPアドレスとデバイスプロファイルを提供することで、NetScaler Consoleに追加されるようになりました。CPXインスタンスの追加プロセスは、NetScaler ConsoleにVPXやMPXなどの他のNetScalerタイプを追加する方法と同様になりました。また、NetScaler ConsoleでのCPXの登録も強化されました。CPXが起動すると、NetScaler ConsoleはCPXインスタンスを自動的に検出し、登録します。CPXインスタンスは、Dockerホストを介して検出されなくなりました。

1. **Infrastructure > Instances > NetScaler**に移動し、**CPX**をクリックします。
2. **追加**をクリックして、NetScaler Consoleに新しいCPXインスタンスを追加します。
3. **NetScaler CPXの追加**ページが開きます。次のパラメーターの値を入力します。

   a. CPXインスタンスの到達可能なIPアドレス、またはCPXインスタンスがホストされているDockerコンテナのIPアドレスのいずれかを提供することで、CPXインスタンスを追加できます。

   b. CPXインスタンスのプロファイルを選択します。

   c. インスタンスをデプロイするサイトを選択します。

   d. エージェントを選択します。

   e. オプションとして、インスタンスにキーと値のペアを入力できます。キーと値のペアを追加すると、後でインスタンスを簡単に検索できるようになります。

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

NetScaler CPXを追加(/en-us/netscaler-application-delivery-management-software/media/add-cpx-instances.png)

**注：**

NetScaler CPXインスタンスの場合、CPXインスタンスプロファイルの作成時に、ホストの**HTTP**、**HTTPS**、**SSH**、および**SNMP**ポートの詳細を指定する必要があります。また、**開始ポート**フィールドと**ポート数**フィールドで、ホストによって公開されたポートの範囲を指定することもできます。

4. **OK**をクリックします。

## NetScaler ConsoleでスタンドアロンのNetScaler BLXインスタンスを追加する

スタンドアロンのNetScaler BLXインスタンスは、専用ホストのLinuxサーバーで実行されている単一のインスタンスです。

1. **インフラストラクチャ > インスタンス > NetScaler**に移動します。
2. **BLX**タブで、**追加**をクリックします。
3. **インスタンスタイプ**リストから**スタンドアロン**オプションを選択します。
4. **IPアドレス**フィールドに、BLXインスタンスのIPアドレスを指定します。
5. **ホストIPアドレス**フィールドに、BLXインスタンスがホストされているLinuxサーバーのIPアドレスを指定します。
6. **プロファイル名**リストで、BLXインスタンスに適したプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、**追加**をクリックします。

   **重要:**

   プロファイルにLinuxサーバーの正しいホストユーザー名とパスワードが指定されていることを確認してください。

7. **サイト**リストで、インスタンスを追加するサイトを選択します。

   サイトを追加する場合は、**追加**をクリックします。

8. **エージェント**リストで、インスタンスを関連付けるNetScalerエージェントを選択します。

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

NetScaler Consoleにエージェントが1つしか設定されていない場合、そのエージェントがデフォルトで選択されます。

9. **OK**をクリックします。

## NetScaler Consoleで高可用性NetScaler BLXインスタンスを追加する

高可用性NetScaler BLXインスタンスは、異なるホストLinuxサーバー上で実行されます。Linuxサーバーは、複数のBLXインスタンスをホストできません。

1. **BLX**タブで、**追加**をクリックします。
2. **インスタンスタイプ**リストから**高可用性**オプションを選択します。
3. **IPアドレス**フィールドに、BLXインスタンスのIPアドレスを指定します。
4. **ホストIPアドレス**フィールドに、BLXインスタンスがホストされているLinuxサーバーのIPアドレスを指定します。
5. 「**ピアIPアドレス**」フィールドで、ピアBLXインスタンスのIPアドレスを指定します。
6. 「**ピアホストIPアドレス**」フィールドで、ピアBLXインスタンスがホストされているLinuxサーバーのIPアドレスを指定します。
7. 「**プロファイル名**」リストで、BLXインスタンスに適したプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、「**追加**」をクリックします。

   **重要:**

   プロファイルでLinuxサーバーの正しいホストユーザー名とパスワードを指定してください。

8. 「**サイト**」リストで、インスタンスを追加するサイトを選択します。

   サイトを追加する場合は、「**追加**」をクリックします。
9. 「**エージェント**」リストで、インスタンスを関連付けるNetScalerエージェントを選択します。

   NetScaler Consoleにエージェントが1つしか構成されていない場合、そのエージェントがデフォルトで選択されます。
10. 「**OK**」をクリックします。

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

NetScaler BLX高可用性インスタンスをNetScaler Consoleに追加(/en-us/netscaler-application-delivery-management-software/media/add-blx-ha-instance.png)

### NetScaler ConsoleからインスタンスGUIにアクセスする

1. **インフラストラクチャ > インスタンス** > **NetScaler** に移動します。
2. アクセスするインスタンスのタイプ (例: VPX、MPX、CPX、SDX、またはBLX) を選択します。
3. 必要なNetScaler IPアドレスまたはホスト名をクリックします。

選択したインスタンスのGUIがポップアップウィンドウに表示されます。

## クラウドに展開されたNetScaler VPXインスタンスをNetScaler Consoleに追加する

NetScaler Consoleを使用して、Amazon Web Services (AWS)、Microsoft Azure、Google Cloudなどのパブリッククラウドに展開されたNetScaler VPXインスタンスを管理および監視できます。NetScaler Consoleとパブリッククラウドに展開されたNetScaler VPXインスタンスとの間にレイヤー3接続を確立する必要があります。レイヤー3接続を確立するには、AWSへのDirect Connect、AzureのVPN、またはEquinixなどのサードパーティ製コネクタなどのソリューションを使用できます。

次のサンプル構成では、NetScaler Consoleとクラウドに展開されたNetScaler VPXインスタンスとの間のレイヤー3接続にCitrix CloudBridge Connectorを使用しています。

Citrix CloudBridgeコネクタ(/en-us/netscaler-application-delivery-management-software/media/cb-dc-dc-console.png)

データセンターDC内のNetScalerアプライアンスNS_Appliance-DCと、パブリッククラウド内のNetScaler仮想アプライアンス (VPX) NS_VPX_CBCの間にCitrix CloudBridge Connectorトンネルが設定されます。NS_Appliance-DCとNS_VPX_CBCは、NetScaler Consoleとパブリッククラウドに展開されたNetScaler VPXインスタンスNS_VPX_1との間の通信を可能にします。通信が確立された後、NetScaler ConsoleでNS_VPX_1を検出できます。

**このトポロジを構成するには：**

1. パブリッククラウドにNetScaler VPXインスタンスをインストール、構成、および起動します。
   - 手順については、「AWSにNetScaler VPXをインストールする」を参照してください。

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

- 手順については、「Microsoft AzureにNetScaler VPXをインストールする」を参照してください。
- 手順については、「Google CloudにNetScaler VPXをインストールする」を参照してください。

2. データセンターの仮想化プラットフォームにNetScaler物理アプライアンスを展開および構成するか、NetScaler仮想アプライアンス (VPX) をプロビジョニングおよび構成します。
   - 手順については、「Citrix HypervisorにNetScaler VPXインスタンスをインストールする」を参照してください。
   - 手順については、「VMware ESXiにCitrix仮想アプライアンスをインストールする」を参照してください。
   - 手順については、「Microsoft Hyper-VにNetScaler仮想アプライアンスをインストールする」を参照してください。
3. データセンターとパブリッククラウドの間にCitrix CloudBridge Connectorを構成します。手順については、「Citrix CloudBridge Connectorの構成」を参照してください。
4. NetScaler Consoleとクラウドに展開されたNetScaler VPXインスタンス間の接続を確立するための静的ルートを、次のように構成します。
   a. NetScaler Consoleにログオンします。
   b. **System \> Static Routes**に移動し、**Add**をクリックします。

      静的ルートの作成(/en-us/netscaler-application-delivery-management-software/media/static_route.jpg)

   c. **Network Address**フィールドに、コネクタを介してNetScaler Consoleから静的ルートを確立したいネットワークのアドレスを入力します。
   d. **Netmask**フィールドに、ネットワークのネットマスクを入力します。
   e. **Gateway**フィールドに、ゲートウェイのアドレスを入力します。
5. パブリッククラウド内のNetScaler VPXインスタンスのIPアドレス範囲を指定して、NetScaler VPXクラウドインスタンスをNetScaler Consoleに追加します。詳細な手順については、NetScaler Consoleへのインスタンスの追加を参照してください。

# 分析の設定

- 14.1-17.x までのビルドの場合
- 14.1-21.x 以降のビルドの場合

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

# 仮想サーバーのライセンス管理とアナリティクス有効化

**注**

- デフォルトでは、**Auto Licensed Virtual Servers** オプションが有効になっています。仮想サーバーをライセンスするには、十分なライセンスがあることを確認する必要があります。ライセンスが限られており、要件に基づいて選択的な仮想サーバーのみをライセンスしたい場合は、**Auto Licensed Virtual Servers** オプションを無効にしてください。**Settings > Licensing & Analytics Configuration** に移動し、**Virtual Server License Allocation** の下にある **Auto Licensed Virtual Servers** オプションを無効にします。

アナリティクスを有効にするプロセスが簡素化されました。仮想サーバーのライセンス付与とアナリティクスの有効化を単一のワークフローで行うことができます。

**Settings > Licensing & Analytics Configuration** に移動して、次の操作を行います。

- **Virtual Server Licence Summary** を表示する
- **仮想サーバー分析サマリー** を表示する



**Configure License** または **Configure Analytics** をクリックすると、**All Virtual Servers** ページが表示されます。



**All Virtual Servers** ページでは、次の操作を行うことができます。

- ライセンスのない仮想サーバーにライセンスを適用する
- ライセンスのある仮想サーバーからライセンスを削除する
- ライセンスのある仮想サーバーでアナリティクスを有効にする
- アナリティクスを編集する
- アナリティクスを無効にする

**注**

アナリティクスを有効にするためにサポートされている仮想サーバーは、負荷分散、コンテンツスイッチング、およびNetScaler Gatewayです。

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

### 仮想サーバーでのライセンス管理

仮想サーバーをライセンスするには、**すべての仮想サーバー**ページから次の手順を実行します。

1. 検索バーをクリックし、**ライセンス済み**を選択し、**いいえ**を選択します。

   

   フィルターが適用され、ライセンスのない仮想サーバーのみが表示されます。
2. 仮想サーバーを選択し、**ライセンス**をクリックします。

   

仮想サーバーのライセンスを解除するには、**すべての仮想サーバー**ページから次の手順を実行します。

1. 検索バーをクリックし、**ライセンス済み**を選択し、**はい**を選択します。
2. 仮想サーバーを選択し、**ライセンス解除**をクリックします。

### アナリティクスを有効にする

仮想サーバーのアナリティクスを有効にするための前提条件は次のとおりです。

- 仮想サーバーが**ライセンスされている**ことを確認します。
- 分析ステータスが**無効**であることを確認します。
- 仮想サーバーが**UP**ステータスであることを確認します。

結果をフィルタリングして、前提条件に記載されている仮想サーバーを特定できます。

1. 検索バーをクリックして**State**を選択し、次に**UP**を選択します。
2. 検索バーをクリックして**Licensed**を選択し、次に**Yes**を選択します。
3. 検索バーをクリックして**Analytics Status**を選択し、次に**Disabled**を選択します。
4. フィルターを適用した後、仮想サーバーを選択し、**Enable Analytics**をクリックします。

   

   **注**

   または、特定のインスタンスに対して分析を有効にすることもできます。

   a. **Infrastructure > Instances > NetScaler**に移動し、インスタンスタイプを選択します。例: VPX。
   b. インスタンスを選択し、**Select Action**リストから**Configure Analytics**を選択します。

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

c. 「Configure Analytics on Virtual Servers」ページで、仮想サーバーを選択し、**Enable Analytics**をクリックします。

5. **Enable Analytics**ウィンドウで:

a. インサイトの種類 (Web Insight または WAF Security Violations) を選択します。

b. トランスポートモードとして **Logstream** を選択します。

> **注**
>
> NetScaler 12.0 以前の場合、トランスポートモードのデフォルトオプションは **IPFIX** です。NetScaler 12.0 以降の場合、トランスポートモードとして **Logstream** または **IPFIX** のいずれかを選択できます。

IPFIX と Logstream の詳細については、「Logstream の概要」を参照してください。

c. **インスタンスレベルオプション**で:

- **HTTP X-Forwarded-For を有効にする** - このオプションを選択すると、HTTP プロキシまたはロードバランサーを介したクライアントとアプリケーション間の接続の IP アドレスを識別できます。
- **NetScaler Gateway** - このオプションを選択すると、NetScaler Gateway の分析を表示できます。

d. 式はデフォルトで true です。

e. **OK** をクリックします。

> **注**
>
> - ライセンスが付与されていない仮想サーバーを選択した場合、NetScaler Console はまずそれらの仮想サーバーにライセンスを付与し、その後分析を有効にします。
> - 管理パーティションでは、**Web Insight** のみがサポートされます。
> - キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にできません。エラーメッセージが表示されます。

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

「**OK**」をクリックすると、NetScaler Consoleは選択した仮想サーバーでアナリティクスを有効にする処理を行います。

**注**

NetScaler Consoleは、LogstreamにはNetScaler SNIPを、IPFIXにはNSIPを使用します。NetScalerエージェントとNetScalerインスタンスの間にファイアウォールが有効になっている場合は、NetScaler ConsoleがAppFlowトラフィックを収集できるように、次のポートを開いていることを確認してください。

| トランスポートモード | 送信元IP | タイプ | ポート |
|---|---|---|---|
| IPFIX | NSIP | UDP | 4739 |
| ログストリーム | SNIP | TCP | 5557 |

### アナリティクスを編集

仮想サーバーでアナリティクスを編集するには：

1. 仮想サーバーを選択します

   注

   または、特定のインスタンスのアナリティクスを編集することもできます。

   a. **インフラストラクチャ > インスタンス > NetScaler** に移動し、インスタンスタイプを選択します。たとえば、VPX。

   b. インスタンスを選択し、**アナリティクスを編集** をクリックします。

2. **アナリティクスを編集** をクリックします
3. **アナリティクス設定の編集** ウィンドウで適用するパラメーターを編集します
4. **OK** をクリックします。

### アナリティクスを無効にする

選択した仮想サーバーでアナリティクスを無効にするには：

1. 仮想サーバーを選択します
2. **アナリティクスを無効にする** をクリックします

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

NetScaler Console は、選択した仮想サーバーのアナリティクスを無効にします

以下の表は、トランスポートモードとしてIPFIXおよびLogstreamをサポートするNetScaler Consoleの機能を示しています。

| 機能 | IPFIX | ログストリーム |
|---|---|---|
| ウェブインサイト | • | • |
| WAFセキュリティ違反 | • | • |
| ゲートウェイインサイト | • | • |
| HDX インサイト | • | • |
| SSL インサイト | サポートされていません | • |
| CR インサイト | • | • |
| IPレピュテーション | • | • |
| AppFirewall | • | • |
| クライアント側測定 | • | • |
| Syslog/Auditlog | • | • |

### アナリティクスをグローバルに設定する

既存のアナリティクス有効化プロセスとは別に、シングルペインワークフローを使用して、以下のアナリティクスを設定することもできます。

- 既存のすべてのライセンスされた仮想サーバー
- 後続のライセンスされた仮想サーバー

設定後、この機能により、既存および後続の仮想サーバーでアナリティクスを手動で有効にする必要がなくなります。

**注意点**:

アナリティクスを設定する前に、NetScaler Console の以下の動作を理解しておく必要があります。

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

- この機能を初めて設定する際は、このドキュメントに記載されている前提条件が満たされていることを確認する必要があります。
- 後でアナリティクス設定を変更する。

  Web Insight、HDX™ Insight、および Gateway Insight を選択して、最初にアナリティクス設定を構成したとします。後でアナリティクス設定を変更し、Gateway Insight の選択を解除した場合でも、その変更はすでにアナリティクスが有効になっている仮想サーバーには影響しません。
- すでにアナリティクスが有効になっている仮想サーバー。

  10個のライセンスされた仮想サーバーがあり、そのうち2つはすでにアナリティクスが有効になっているとします。このシナリオでは、この機能は残りの8つの仮想サーバーに対してのみアナリティクスを有効にします。
- アナリティクスが手動で無効化された仮想サーバー。

  10個のライセンスされた仮想サーバーがあり、そのうち2つの仮想サーバーでアナリティクスを手動で無効にしたとします。このシナリオでは、この機能は残りの8つの仮想サーバーに対してのみアナリティクスを有効にし、アナリティクスが手動で無効化された仮想サーバーはスキップします。
- **Bot Security Violations** および **WAF Security Violations** オプションは、プレミアムライセンスの仮想サーバーでのみサポートされています。仮想サーバーがプレミアムライセンスでない場合、**Bot Security Violations** および **WAF Security Violations** は有効になりません。

### 前提条件

以下を確認してください。

- 既存のすべての仮想サーバーがライセンスされています。
- 以降のすべての仮想サーバーをライセンスするために、自動ライセンスオプションが有効になっています。**Settings > Licensing & Analytics Config** に移動し、**Virtual Server License Allocation** の下にある **Auto Licensed Virtual Servers** オプションをオンにします。

### アナリティクスを有効にする

1. **Settings > Licensing & Analytics Config** に移動します。
2. **Analytics Summary** の下にある **Global Analytics Configuration** をクリックします。

   
3. 仮想サーバーでアナリティクスを有効にするアナリティクス機能を選択します。

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

4. 以降の仮想サーバーでアナリティクスを有効にするには、**Apply this analytics settings on the subsequent licensed virtual servers** チェックボックスをオンにします。
5. **Submit** をクリックします。



## 仮想サーバーでアナリティクスを構成する

アナリティクスを有効にするための前提条件は、仮想サーバーがライセンスされていることです。フレックスライセンスを使用している場合、既存のすべての仮想サーバーと後続の仮想サーバーは自動的にライセンスされます。アナリティクスの構成に進むことができます。

アナリティクスは2つの方法で構成できます。**設定 > アナリティクス構成** に移動して、以下を表示します。

- **仮想サーバーアナリティクス概要** - 既存の仮想サーバーでアナリティクスを構成できます。
- **グローバルアナリティクス概要** - 既存および後続の仮想サーバーの両方でアナリティクスを構成できます。



### 既存の仮想サーバーでアナリティクスを構成する

**注記:**

アナリティクスを有効にする仮想サーバーが **UP** ステータスであることを確認してください。

1. **仮想サーバーアナリティクス概要** で、**アナリティクスを構成** をクリックします。

   **すべての仮想サーバー** ページが表示されます。次のことができます。

   - アナリティクスを有効にする
   - アナリティクスを編集する
   - アナリティクスを無効にする

   **注記:**

   アナリティクスを有効にするためにサポートされている仮想サーバーは、負荷分散、コンテンツスイッチング、およびNetScaler Gatewayです。

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

2. 仮想サーバーを選択し、**Enable Analytics**をクリックします。

   アナリティクスを有効にする(/en-us/netscaler-application-delivery-management-software/media/enable-analytics.png)

   **注**

   または、インスタンスのアナリティクスを有効にすることもできます。

   a. **Infrastructure > Instances > NetScaler**に移動し、インスタンスタイプを選択します。たとえば、VPXです。
   b. インスタンスを選択し、**Select Action**リストから**Configure Analytics**を選択します。
   c. 「Configure Analytics on Virtual Servers」ページで、仮想サーバーを選択し、**Enable Analytics**をクリックします。

3. **Enable Analytics**ウィンドウで：

   a. インサイトタイプを選択します。
   b. トランスポートモードとして**Logstream**を選択します。

      **注：**

      NetScaler 12.0以前の場合、トランスポートモードのデフォルトオプションは**IPFIX**です。NetScaler 12.0以降の場合、トランスポートモードとして**Logstream**または**IPFIX**のいずれかを選択できます。

      IPFIXとLogstreamの詳細については、「Logstreamの概要」を参照してください。

   c. **インスタンスレベルのオプション**で：

      - **HTTP X-Forwarded-Forを有効にする** - HTTPプロキシまたはロードバランサーを介したクライアントとアプリケーション間の接続のIPアドレスを識別するには、このオプションを選択します。
      - **カスタムヘッダー** - プロキシIPアドレスの代わりに実際のクライアントIPアドレスを取得するために、X-Real-IP、X-Client-IP、またはその他のカスタムヘッダーなどのカスタムヘッダーを定義します。管理対象のNetScalerインスタンスが14.1–38.24以降のビルドであることを確認してください。
      - **NetScaler Gateway** - NetScaler Gatewayの分析を表示するには、このオプションを選択します。

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

d. 式はデフォルトでtrueです。

e. **OK**をクリックします。

**注:**

- 管理者パーティションでは、**Web Insight**のみがサポートされています。
- キャッシュリダイレクション、認証、GSLBなどの仮想サーバーでは、分析を有効にできません。エラーメッセージが表示されます。

**OK**をクリックすると、NetScaler Consoleは選択した仮想サーバーで分析を有効にする処理を開始します。

**注**

NetScaler Consoleは、LogstreamにはNetScaler SNIPを、IPFIXにはNSIPを使用します。NetScalerエージェントとNetScalerインスタンスの間にファイアウォールが有効になっている場合は、NetScaler ConsoleがAppFlowトラフィックを収集できるように、次のポートを開放してください。

| 転送モード | 送信元IP | タイプ | ポート |
|---|---|---|---|
| IPFIX | NSIP | UDP | 4739 |
| ログストリーム | SNIP | TCP | 5557 |

### 分析を編集

仮想サーバーで分析を編集するには、次の手順を実行します。

1. 仮想サーバーを選択します。

**注:**

または、インスタンスの分析を編集することもできます。

a. **インフラストラクチャ > インスタンス > NetScaler** に移動し、インスタンスタイプを選択します。たとえば、VPXです。

b. インスタンスを選択し、**分析の編集**をクリックします。

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

2. 「**アナリティクスを編集**」をクリックします。
3. 「**アナリティクス構成の編集**」ウィンドウで、適用するパラメーターを編集します。
4. 「**OK**」をクリックします。

### アナリティクスを無効にする

選択した仮想サーバーでアナリティクスを無効にするには：

1. 仮想サーバーを選択します。
2. 「**アナリティクスを無効にする**」をクリックします。

NetScaler Consoleは、選択した仮想サーバーのアナリティクスを無効にします。

次の表は、トランスポートモードとしてIPFIXとLogstreamをサポートするNetScaler Consoleの機能について説明しています。

| 機能 | IPFIX | ログストリーム |
|---|---|---|
| ウェブインサイト | • | • |
| WAFセキュリティ違反 | • | • |
| ゲートウェイインサイト | • | • |
| HDXインサイト | • | • |
| SSLインサイト | サポートされていません | • |
| CRインサイト | • | • |
| IPレピュテーション | • | • |
| AppFirewall | • | • |
| クライアント側測定 | • | • |
| Syslog/Auditlog | • | • |

## グローバルアナリティクスを構成する

カスタムポリシーまたはグローバルポリシーを作成することで、グローバルアナリティクスを有効にできます。

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

**注記:**

- 最大10個のポリシーを作成できます。ポリシーは、9つのカスタムポリシーと1つのグローバルポリシーの組み合わせ、または10個のカスタムポリシーのいずれかになります。
- カスタムポリシーとグローバルポリシーの両方がある場合、両方のポリシーで選択されたインサイトが仮想サーバーに適用されます。インサイトを削除したい場合は、手動で削除する必要があります。

### カスタムポリシー

カスタムポリシーを使用すると、特定のインサイトのみを必要とするインスタンスまたは仮想サーバーを制御できます。NetScaler Consoleで管理されているさまざまなNetScalerインスタンスを通じて、何百もの仮想サーバーが構成されている場合があります。特定のシナリオでは、一部の仮想サーバーまたはインスタンスにのみ選択的なインサイト（たとえば、ボットセキュリティ違反やWAFセキュリティ違反など）を適用したい場合があります。このようなシナリオでは、カスタムポリシーを構成し、特定の分析機能を選択して、関連するインスタンスと仮想サーバーに適用できます。

カスタムポリシーを構成するには：

1. **Global Analytics Summary**で、**Global Analytics Configuration**をクリックします。

   

2. **Policy details**で、**Custom policy**を選択し、任意のポリシー名を指定します。

   **注：**

   ポリシー名は後で編集できません。

   

3. **Define Conditions**で、インスタンスIPのセット、特定のインスタンス、仮想サーバー名、またはその両方を選択して条件を作成します。

   

4. **Enable analytics**で、分析機能のタイプを選択します。

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

**注：**

「**後続の仮想サーバーにこの分析設定を適用する**」を有効にすると、定義された分析機能に基づいて、後続の仮想サーバーに分析が適用されます。

分析を選択(/en-us/netscaler-application-delivery-management-software/media/bulk-analytics-custom-select-insight.png)

5. **保存**をクリックします。

**注意点:**

- 既存のインサイトを削除して別のインサイトを追加することでポリシーを変更した場合、更新されたポリシーには新しいインサイトが適用されます。いずれかのインサイトを削除したい場合は、すでに設定されているインサイトを手動で削除する必要があります。

  HDX InsightとWeb Insightを含むカスタムポリシーを作成したとします。HDX Insightを削除し、ボットセキュリティ違反を追加するようにポリシーを更新した場合、仮想サーバー/インスタンスは、HDX Insight、Web Insight、およびボットセキュリティ違反で更新されます。HDX Insightを削除したい場合は、分析の編集オプションを使用して手動で削除する必要があります。
- 既存のポリシーを削除し、同じインスタンスまたは仮想サーバーを追加して別のポリシーを作成した場合にも、同じロジックが適用されます。

### グローバルポリシー

グローバルポリシーを使用すると、検出された仮想サーバーと後続の仮想サーバーの両方で分析を有効にできます。グローバルポリシーを作成するには：

1. **グローバル分析の概要**で、**グローバル分析の構成**をクリックします。
2. **ポリシーの詳細**で、**グローバルポリシー**を選択します。
3. **分析を有効にする**で、分析機能の種類を選択します。

**注:**

「**後続の仮想サーバーにこの分析設定を適用する**」を有効にすると、定義されたカテゴリに基づいて、後続の仮想サーバーに分析が適用されます。

4. **保存**をクリックします。

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

設定後、アナリティクスは検出された仮想サーバーと後続の仮想サーバーの両方で有効になります。

### 注意点

- 初めてグローバルポリシーを設定する際に、**Web Insight**、**HDX™ Insight**、および**Gateway Insight**を選択したとします。後でアナリティクス設定を再度変更し、**Gateway Insight**の選択を解除しても、その変更はすでにアナリティクスが有効になっている仮想サーバーには影響しません。仮想サーバー上のGateway Insightは手動で削除する必要があります。
- 仮想サーバーが10台あり、そのうち2台は**アナリティクスを設定**オプションを使用してすでにアナリティクスが有効になっているとします。このシナリオでは、グローバルポリシーを設定すると、アナリティクスは残りの8台の仮想サーバーにのみ適用されます。
- 仮想サーバーが10台あり、そのうち2台のアナリティクスを手動で無効にしたとします。このシナリオでは、グローバルポリシーを設定すると、アナリティクスは残りの8台の仮想サーバーにのみ適用され、手動でアナリティクスが無効にされた仮想サーバーはスキップされます。

## アナリティクスを移行する

**14.1-43.x**ビルド以降、仮想サーバーでアナリティクスを有効にすると、アナリティクスはプロファイルベースの構成を通じて適用されます。以前は、アナリティクスはAppFlowポリシーを通じて構成されていました。プロファイルベースの構成には、次の利点があります。

- パフォーマンスと柔軟性の向上
- 構成と管理の簡素化

**注：**

アナリティクス構成に関連する機能強化は、プロファイルベースの構成を通じてのみサポートされます。アナリティクスが有効になっている既存のすべての仮想サーバーをプロファイルベースの構成に移行することをお勧めします。

1. **設定 > アナリティクス構成**に移動し、**アナリティクスを移行**を選択します。

   アナリティクスを移行(/en-us/netscaler-application-delivery-management-software/media/migrate-analytics.png)

2. **アナリティクスを移行**ページで、AppFlow®ポリシーを通じて1つ以上の仮想サーバーが構成されているインスタンスを表示できます。

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

インスタンスを選択(/en-us/netscaler-application-delivery-management-software/media/select-instances-migrate-analytics.png)

確認ウィンドウが表示されます。移行を完了するには、「**はい**」をクリックします。

# 管理対象のNetScalerインスタンスにネットプロファイルを割り当てる

NetScaler Consoleで仮想サーバーのアナリティクスまたはメトリクスコレクターを有効にすると、NetScalerからのAppFlowまたはメトリクスデータは、NetScalerサブネットIPアドレス (SNIP) を介してNetScaler Consoleにエクスポートされます。場合によっては、ネットワーク内のファイアウォールによってSNIPがブロックされることがあります。そのようなシナリオでは、SNIPとは異なるIPアドレスを使用する必要がある場合があります。ネットプロファイルの詳細は、「バックエンド通信に指定された送信元IPを使用する」(/ja-jp/citrix-adc/current-release/load-balancing/load-balancing-manage-clienttraffic/use-specified-srcip.html)を参照してください。

NetScalerからNetScaler ConsoleにAppFlowデータをエクスポートするために、NetScaler Consoleを介してNetScalerインスタンスにネットプロファイルを割り当てることができます。

## 前提条件

以下を確認してください。

- NetScalerインスタンスのバージョンは **13.0-48.4以降** です。
- ネットプロファイルがNetScalerインスタンスで構成されています。

NetScaler Consoleでネットプロファイルを割り当てるには：

1. **Infrastructure > Instances > NetScaler** に移動します。
2. インスタンスを選択し、**Select Action** リストから以下を実行します。
    - AppFlow のネットプロファイルを割り当てるには、「**Configure Net Profiles**」をクリックします。
    - メトリクスコレクターのネットプロファイルを割り当てるには、「**Configure Net Profiles for Metrics Collector**」をクリックします。
3. リストからネットプロファイルを選択し、**Apply** をクリックします。

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

**注記：**

- AppFlow の場合、インスタンスにネットプロファイルを割り当てる前に、すべての仮想サーバーの analytics を無効にしてください。
- Metrics Collectorについては、インスタンスにネットプロファイルを割り当てる前に、すべての仮想サーバーのメトリクスを無効にしてください。

# NTPサーバーを構成する

NetScaler Consoleでネットワークタイムプロトコル（NTP）サーバーを構成し、そのクロックをNTPサーバーと同期させることができます。NTPサーバーを構成することで、NetScaler Consoleのクロックがネットワーク上の他のサーバーと同じ日付と時刻設定を持つことが保証されます。

**NetScaler ConsoleでNTPサーバーを構成するには**:

1. NetScaler Console GUIから、 **>** の順に移動します。 ページで、 の下にある をクリックします。次に、 をクリックします。
2. ページで、次の詳細を入力します。

   - **サーバー名/IPアドレス** – NTPサーバーのドメイン名またはIPアドレスを入力します。NTPサーバーを追加した後、名前またはIPアドレスは変更できません。
   - **最小ポーリング間隔** – 送信されるNTPメッセージ間の間隔の最小値を、2の累乗として秒単位で指定します。たとえば、最小ポーリング間隔を64秒（2\^6と表現できる）にする場合は、「6」と入力します。
   - **最大ポーリング間隔** – 送信されるNTPメッセージ間の間隔の最大値を、2の累乗として秒単位で指定します。たとえば、最大ポーリング間隔を256秒（2\^8と表現できる）にする場合は、「8」と入力します。
   - **キー識別子** - NTPサーバーとの対称キー認証に使用できるキー識別子を入力します。Autokeyを選択する場合は、キー識別子を追加しないでください。キー識別子を見つけるには、NTPサーバーのドキュメントを参照してください。
   - **Autokey** - NTPサーバーで公開キー認証を使用する場合は、 を選択します。キー識別子を追加する場合は選択しないでください。
   - **優先** – このNTPサーバーをクロック同期の優先サーバーとして指定する場合は、このオプションを選択します。これは、複数のサーバーが構成されている場合にのみ適用されます。

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

3. をクリックします。

**NetScaler ConsoleでNTP同期を有効にするには:**

1. ホームページに移動します。
2. をクリックし、 チェックボックスをオンにします。
3. 「**OK**」をクリックします。

   NetScaler Console を再起動するための確認ウィンドウが表示されます。続行するには「**Yes**」をクリックします。

# システム設定を構成する

インスタンスとアプリケーションの管理および監視にNetScaler Consoleを使用し始める前に、NetScaler Consoleサーバーの最適なパフォーマンスを確保するために、いくつかのシステム設定を構成することをお勧めします。

## システムアラームを構成する

重大または主要なシステム問題に気づくように、システムアラームを構成します。たとえば、CPU使用率が高い場合や、サーバーへのログイン失敗が複数回発生した場合に通知を受けたい場合があります。cpuUsageHighやmemoryUsageHighなどの一部のアラームカテゴリでは、しきい値を設定し、それぞれの重大度（CriticalやMajorなど）を定義できます。inventoryFailedやloginFailureなどの一部のカテゴリでは、重大度のみを定義できます。アラームカテゴリのしきい値が破られた場合（例：memoryUsageHigh）、またはアラームカテゴリに対応するイベントが発生した場合（例：loginFailure）、メッセージがシステムに記録され、そのメッセージをsyslogメッセージとして表示できます。

**システムアラームを構成するには：**

1. **Settings > SNMP** に移動し、右上隅にある **Alarms** タブをクリックします。
2. 構成するアラームを選択し、**Edit** をクリックします。
3. **Configure Alarm** ページで、アラームの重大度を選択し、しきい値を設定します。
4. しきい値を超えたアラーム、またはイベントが発生したアラームを表示するには、**Settings > Auditing** に移動し、**Syslog Messages** をクリックします。

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

## システム通知を構成する

さまざまなシステム関連機能について、選択したユーザーグループに通知を送信できます。NetScaler Consoleで通知サーバーを設定し、電子メールおよびショートメッセージサービス（SMS）ゲートウェイサーバーを構成して、ユーザーに電子メールおよびテキスト通知を送信できます。通知を設定することで、ユーザーログインやシステム再起動などのシステムレベルのアクティビティが通知されるようになります。

**システム通知を構成するには：**

1. 「**設定 > 管理**」に移動します。「**システム管理**」ページで、「**イベント通知**」の下にある「**イベント通知とダイジェストの設定 > イベント通知**」をクリックします。
2. **Configure System Notification Settings** ページで、NetScaler Consoleによって生成されるイベントのカテゴリまたはカテゴリを選択します。
3. 次に、電子メールサーバーまたはSMSサーバーのいずれかを構成して、電子メールまたはSMS、あるいはその両方で通知を受信します。

## システムバックアップ設定の構成

NetScaler Console は、毎日 00:30 にシステムを自動的にバックアップします。デフォルトでは、3 つのバックアップファイルが保存されます。システムのバックアップをより多く保持したい場合があります。バックアップファイルを暗号化することもできます。バックアップを外部サーバーに保存することも選択できます。

**システムバックアップ設定を構成するには:**

1. **>** に移動します。
2. で、 をクリックします。
3. をクリックし、 ページで、必要な値を指定します。

## インスタンスバックアップ設定の構成

NetScaler インスタンスの現在の状態をバックアップすると、インスタンスが不安定になった場合に、バックアップファイルを使用して安定性を復元できます。これは、アップグレードを実行する前に特に重要です。デフォルトでは、12 時間ごとにバックアップが取得され、3 つのバックアップファイルがシステムに保持されます。

**インスタンスバックアップ設定を構成するには：**

1. **>** に移動します。
2. で、 をクリックします。

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

3. をクリックし、 で、必要な値を指定します。

## 基本認証を有効にする

基本認証は、一時的に有効にする必要があります。

- エージェントとディザスタリカバリノードの初期登録を完了します。
- NetScaler GUIからライセンスアクティベーションシステム (LAS) のチェックアウトを開始します。

**注：**

基本認証は、最初の登録時にのみ必要です。

### 基本認証を構成する

1. **設定 > 管理 > システム設定 > システム、タイムゾーン、許可されたURL、およびエージェント設定** に移動します。
2. **Basic Settings** をクリックします。
3. **Enable Allow Basic Authentication** を選択します。
4. **OK** をクリックします。

## NetScaler Console機能を有効または無効にする

管理者として、**Settings > Administration > Configurable Features** ページで次の機能を有効または無効にできます。

- **エージェントフェイルオーバー** - エージェントフェイルオーバーは、2つ以上のアクティブなエージェントを持つサイトで発生する可能性があります。サイトでエージェントが非アクティブ (DOWN状態) になると、NetScaler Consoleサービスは、非アクティブなエージェントのNetScalerインスタンスを他のアクティブなエージェントに再配布します。詳細については、「マルチサイト展開用のオンプレミスエージェントの構成」を参照してください。
- **エンティティポーリングネットワーク機能** - エンティティとは、NetScalerインスタンスにアタッチされたポリシー、仮想サーバー、サービス、またはアクションのいずれかです。デフォルトでは、NetScaler Consoleは構成されたネットワーク機能エンティティを60分ごとに自動的にポーリングします。詳細については、「ポーリングの概要」を参照してください。
- **インスタンスバックアップ** - NetScalerインスタンスの現在の状態をバックアップし、後でバックアップファイルを使用してNetScalerインスタンスを同じ状態に復元します。詳細については、「NetScalerインスタンスのバックアップと復元」を参照してください。

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

- **インスタンス構成監査** - 管理対象NetScalerインスタンス全体の構成変更を監視し、構成エラーをトラブルシューティングし、保存されていない構成を回復します。
- **インスタンスイベント** - イベントは、管理対象NetScalerインスタンスで発生したイベントまたはエラーを表します。NetScaler Consoleで受信したイベントは、**Events Summary** ページ (**Infrastructure > Events**) に表示され、すべてのアクティブなイベントはEvent Messagesページ (**Infrastructure > Events > Event Messages**) に表示されます。詳細については、「イベント」を参照してください。
- **インスタンスネットワークレポート** - インスタンスのレポートをグローバルレベルで生成できます。また、仮想サーバーやネットワークインターフェースなどのエンティティについても生成できます。詳細については、「ネットワークレポート」を参照してください。
- **インスタンスSSL証明書** - NetScaler Consoleは、管理対象のすべてのNetScalerインスタンスにインストールされているSSL証明書の一元的なビューを提供します。詳細については、「SSLダッシュボード」を参照してください。
- **インスタンスSyslog** - デバイスを構成してすべてのsyslogメッセージをNetScaler Consoleにリダイレクトするように設定している場合、NetScalerインスタンスで生成されたsyslogイベントを監視できます。

機能を有効にするには、次の手順を実行します。

1. 有効にする機能をリストから選択します。
2. **有効にする**をクリックします。

**重要**

機能が無効になっている場合、ユーザーはその機能に関連する操作を実行できません。

# NetScaler Console を ServiceNow インスタンスと統合する

NetScaler および NetScaler Console イベントの ServiceNow 通知を有効にするには、NetScaler Console を ServiceNow インスタンスと統合します。この統合では、Citrix ITSM コネクタを使用して NetScaler Console と ServiceNow インスタンス間で通信します。

NetScaler Console との ServiceNow 統合では、トークンベース認証に ITSM Adapter サービスを使用します。そのため、ServiceNow にエンドポイントインスタンスを作成します。詳細については、「ITSM Adapter の仕組み」を参照してください。

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

NetScaler Console のオンプレミス展開を ITSM アダプタに接続するには、Cloud Connect が構成されていることを確認してください。詳細については、「Cloud Connect」を参照してください。

NetScaler Console ビルド 14.1-4.x 以前との ServiceNow 統合の場合、顧客 ID を構成していることを確認してください。詳細については、「顧客 ID の構成」を参照してください。

## 前提条件

NetScaler Console を ServiceNow と統合する前に、以下を確認してください。

1. Citrix Cloud にサインアップする。Citrix Cloud 管理者を管理するアクセス権があることを確認してください。詳細については、「Citrix Cloud 管理者の管理」を参照してください。

## NetScaler Console を ServiceNow と統合する方法?

ITSM コネクタを使用して NetScaler Console を ServiceNow と統合するには、次の手順を実行します。

- [ ]

1. Citrix Cloud™ で ITSM Adapter サービスを購読する。
2. ServiceNow インスタンスでエンドポイントアクセスを作成する。
3. ServiceNow インスタンスを追加する。
4. NetScaler ConsoleでのServiceNowチケットの自動生成をテストする(#step-4---test-auto-generation-of-servicenow-tickets-in-adm)。

### ステップ1 - Citrix CloudでITSMアダプターサービスを購読する

1. **ITSM Adapter**タイルで、**Request Trial**をクリックします。

   ITSMトライアルをリクエストする(/en-us/netscaler-application-delivery-management-software/media/itsm-adpater-request-trial.png)

2. **Identity Access and Management** > **API Access**に移動し、**Client ID**と**Client Secret**の情報をメモします。

### ステップ2 - ServiceNowインスタンスでエンドポイントアクセスを作成する

1. 管理者資格情報を使用してServiceNowインスタンスにログインします。
2. ServiceNowストアに移動します。**Citrix ITSM connector**をダウンロードしてインストールします。
3. **Citrix ITSM Connector**ペインで、**Home**を選択し、**Authenticate**をクリックします。Citrix CloudからメモしたクライアントIDとシークレットを入力します。

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

4. 接続をテストします。
5. 設定を保存します。接続がアクティブであることを示すServiceNowからの確認メッセージが表示されます。
6. ServiceNowインスタンスにアクセスするためのエンドポイントを作成します。クライアントがインスタンスにアクセスするためのエンドポイントを作成するを参照してください。
7. クライアントIDとクライアントシークレットを使用してアクセスおよびリフレッシュトークンを取得します。OAuthトークンを参照してください。

   アクセスおよびリフレッシュトークンを取得する(/en-us/netscaler-application-delivery-management-software/media/obtain-access-refresh-token-itsm.png)

### ステップ3 - ServiceNowインスタンスを追加する

1. 「**Manage**」タブで、「Add ServiceNow Instance」を選択します。
2. **インスタンス名**、**クライアント ID**、**クライアント シークレット**、**リフレッシュ トークン**、および**アクセス トークン**を指定します。
3. 「**Test**」をクリックします。

   ITSMアダプターにServiceNowインスタンスを登録する(/en-us/netscaler-application-delivery-management-software/media/register-servicenow-itsm-instance.png)

   ServiceNowインスタンスがITSMアダプターサービスに接続されました。
4. 接続テストが成功したら、「**Save**」をクリックしてServiceNowインスタンスを追加します。

### ステップ4 - NetScaler ConsoleでのServiceNowチケットの自動生成をテストする

1. NetScaler Consoleにログインします。
2. 「**Account > Notifications**」に移動し、「**ServiceNow**」を選択します。
3. リストからServiceNowプロファイルを選択します。
4. 「**Test**」をクリックしてServiceNowチケットを自動生成し、構成を確認します。

   NetScaler Console GUIでServiceNowチケットを表示する場合は、「**ServiceNow Tickets**」を選択します。

## NetScaler ConsoleでServiceNow通知を設定する

ITSMアダプターにServiceNowインスタンスが登録されたら、NetScaler Console GUIで以下のイベントのServiceNow通知を設定できます。

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

**重要**

この機能はServiceNow Cloudでサポートされています。

- **NetScalerイベント**: NetScaler Consoleは、選択した管理対象NetScalerインスタンスからの選択したNetScalerイベントのセットに対して、ServiceNowインシデントを生成できます。

  管理対象インスタンスからのNetScalerイベントのServiceNow通知を送信するには、イベントルールを設定し、ルールアクションを**Send ServiceNow Notifications**として割り当てる必要があります。

  NetScaler Consoleで、**Infrastructure > Events > Rules**に移動してイベントルールを作成します。詳細については、「Send ServiceNow notifications」を参照してください。

- **アプリケーション分析**: NetScaler Consoleは、指定されたしきい値を超えたアプリケーションに対してServiceNowインシデントを生成できます。

  アプリケーション分析のServiceNowインシデント(/en-us/netscaler-application-delivery-management-software/media/configure-appscore-threshold-servicenow.png)

  この例では、アプリケーションのAppスコアが90を下回ると、ServiceNowインシデントが生成されます。

- **SSL証明書とNetScaler Consoleライセンスイベント**: NetScaler Consoleは、SSL証明書の有効期限切れおよびNetScaler Consoleライセンスの有効期限切れイベントに対してServiceNowインシデントを生成できます。

  SSL証明書の有効期限切れに関するServiceNow通知を送信するには、「The SSL certificate expiry」を参照してください。

  NetScaler Consoleライセンスの有効期限切れに関するServiceNow通知を送信するには、「The NetScaler Console license expiry」を参照してください。

# レポートのエクスポートまたはエクスポートのスケジュール

NetScaler Consoleでは、選択したNetScaler Console機能の包括的なレポートをエクスポートできます。このレポートは、インスタンス、パーティション、および対応する詳細間のマッピングの概要を提供します。

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

NetScaler Consoleは、個々のNetScaler Console機能の下に機能固有のスケジュールされたエクスポートレポートを表示し、これらを表示、編集、または削除できます。たとえば、NetScalerインスタンスのエクスポートレポートを表示するには、 **> >** に移動し、エクスポートアイコンをクリックします。これらのレポートは、PDF、JPEG、PNG、およびCSVファイル形式でエクスポートできます。

では、次のアクションを実行できます。

- レポートをローカルコンピューターにエクスポートする
- エクスポートレポートをスケジュールする
- スケジュールされたエクスポートレポートを表示、編集、または削除する

## レポートのエクスポート

NetScaler Consoleからローカルコンピューターにレポートをエクスポートするには、次の手順を実行します。

1. ページ右上のエクスポートアイコンをクリックします。
2. を選択します。
3. 次のいずれかのエクスポートオプションを選択します。

    - - このオプションは、NetScaler Consoleレポートをスナップショットとしてエクスポートします。
    - - このオプションは、NetScaler Consoleレポートを表形式でエクスポートします。表形式でエクスポートするデータレコードの数を選択することもできます。

    NetScaler Consoleレポートのエクスポート(/en-us/netscaler-application-delivery-management-software/media/export-snapshot.png)
4. レポートをローカルコンピューターに保存するファイル形式を選択します。
5. **エクスポート**をクリックします。

## エクスポートレポートをスケジュールする

エクスポートレポートを定期的にスケジュールするには、繰り返し間隔を指定します。NetScaler Console は、エクスポートされたレポートを設定済みのメールまたは Slack プロファイルに送信します。

1. ページ右上のエクスポートアイコンをクリックします。
2. **エクスポートのスケジュール**を選択し、以下を指定します。

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

- **件名** - デフォルトでは、このフィールドには選択した機能名が自動入力されます。ただし、意味のあるタイトルに書き換えることができます。
- **エクスポートオプション** - NetScaler Console レポートをスナップショット形式または表形式でエクスポートします。表形式でエクスポートするデータレコードの数を選択することもできます。
- **形式** - 設定済みのメールまたは Slack プロファイルでレポートを受信するファイル形式を選択します。
- **繰り返し** - リストから**毎日**、**毎週**、または**毎月**を選択します。
- **説明** - レポートに意味のある説明を指定します。
- **エクスポート時間** - レポートをエクスポートする時間を指定します。
- **メール** - チェックボックスを選択し、リストボックスからプロファイルを選択します。プロファイルを追加する場合は、**追加**をクリックします。
- **Slack** - チェックボックスを選択し、リストボックスからプロファイルを選択します。プロファイルを追加する場合は、**追加**をクリックします。

3. **スケジュール**をクリックします。

## スケジュールされたエクスポートレポートの表示と編集

エクスポートレポートを表示するには、次の手順を実行します。

1. ページの右上隅にあるエクスポートアイコンをクリックします。

   **エクスポートレポート**ページには、すべての機能固有のエクスポートレポートが表示されます。

2. 編集するレポートを選択し、**編集**をクリックします。

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

# アップグレード

NetScaler Consoleの各リリースでは、機能が強化された新しい機能と更新された機能が提供されます。新しい機能やバグ修正を利用するために、NetScaler Consoleを最新リリースにアップグレードすることをお勧めします。強化点、既知の問題、バグ修正の包括的なリストは、各リリース発表に付随するリリースノートに含まれています。アップグレードを開始する前に、ライセンスフレームワークと使用できるライセンスの種類を理解することも重要です。NetScaler Consoleのライセンス情報については、ライセンスを参照してください。

## アップグレードする前に

NetScaler Consoleのダウンロードページからアップグレードパッケージをダウンロードし、この記事の手順に従ってシステムを最新の14.1ビルドにアップグレードしてください。アップグレードプロセスが開始されると、NetScaler Consoleが再起動し、既存の接続は終了され、アップグレードが完了すると再接続されます。既存の構成は保持されますが、アップグレードが完了するまでNetScaler Consoleはデータを処理しません。

**重要**

NetScaler Consoleのバージョンとビルドは、NetScalerのバージョンとビルドと**同等かそれ以上**である必要があります。たとえば、NetScaler Console 12.1 Build 50.39をインストールしている場合、NetScaler 12.1 Build 50.28/50.31以前がインストールされていることを確認してください。

**14.1へのアップグレードに関する注意点**:

- バージョン11.1またはバージョン12.0 56.xおよびそれ以前のビルドからアップグレードする場合は、次の手順を実行します。
  a. 既存のバージョンから12.0ビルド57.24にアップグレードします。
  b. バージョン12.1の最新ビルドにアップグレードします。
  c. バージョン13.1にアップグレードします。
  d. バージョン14.1にアップグレードします。
- 12.0ビルド57.24以降からアップグレードする場合は、まず12.1に、次に13.1に、そして14.1にアップグレードします。

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

- 12.1からアップグレードする場合は、まず13.0 64.xxにアップグレードし、その後直接14.1にアップグレードする必要があります。
- 13.0 64.xxより前のバージョンからアップグレードする場合は、より良いユーザーエクスペリエンスのために、まず13.0 64.xxにアップグレードし、その後14.1にアップグレードします。
- バージョン13.1からバージョン14.1にアップグレードするには、まずバージョン13.1の最新ビルドにアップグレードしてから、バージョン14.1にアップグレードしてください。
- 14.1へのアップグレードが成功し、GUIにログインすると、デフォルトのパスワードを使用している場合はパスワードの変更が推奨されます。

## 14.1-xx.xx以降へのアップグレード前に注意すべき重要な点

NetScaler Consoleをバージョン14.1-xx.xxにアップグレードすると、NetScaler Consoleデータベースも移行されます。このデータ移行は、NetScaler ConsoleがPostgreSQLバージョン10.11を使用するようになったために発生します。

**注記:**

NetScaler Consoleのダウングレードはサポートされていません。ダウングレードを試みないでください。

**推奨される注意事項**:

- 14.1-xx.xx以降にアップグレードする場合は、アップグレードごとにNetScaler Consoleサーバーのスナップショットを取得してください。
- アップグレードする前に、NetScaler Consoleサーバーをバックアップしてください。
- アップグレード後、NetScaler Consoleサーバーと管理対象インスタンス間の接続を再確立する必要がある場合があります。続行すると接続が失敗する可能性があることを警告する確認プロンプトが表示されます。
- 高可用性設定のNetScaler Consoleサーバーの場合、アップグレード中はどちらのノードでも構成変更を行わないでください。

**警告:**

アップグレードプロセスが正常に完了するまで、ブラウザを更新しないでください。
アップグレードが完了するまでのおおよその時間はGUIで確認してください。

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

# 単一のNetScaler Consoleサーバーを14.1-xx.xxにアップグレードする

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **設定** > **管理** に移動します。**システムメンテナンス** で、**NetScaler Consoleのアップグレード** をクリックします。

   NetScaler Consoleのアップグレード(/en-us/netscaler-application-delivery-management-software/media/nmas-kamet-release-upgrade-1.png)
3. **NetScaler Consoleのアップグレード** ページで、**アップグレード成功時にソフトウェアイメージをクリーンアップ** チェックボックスをオンにして、アップグレード後にイメージファイルを削除します。このオプションを選択すると、アップグレード時にNetScaler Consoleイメージファイルが自動的に削除されます。

   **注：**

   このオプションはデフォルトで選択されています。アップグレードプロセスを開始する前にこのチェックボックスを選択しない場合、イメージを手動で削除する必要があります。
4. その後、**ローカル** (お使いのローカルマシン) または **アプライアンス** のいずれかを選択して、新しいイメージファイルをアップロードできます。ビルドファイルはNetScaler Console仮想アプライアンスに存在している必要があります。

   イメージのアップロード(/en-us/netscaler-application-delivery-management-software/media/nmas-kamet-release-upgrade-2-new.png)
5. **OK** をクリックします。 確認ダイアログボックスが表示されます。**はい** をクリックします。

   アップグレードプロセスが開始されます。

設定が移行された後、NetScaler Console GUIにログオンできます。ログオンすると、履歴データはバックグラウンドで移行を開始し、その間もNetScaler Consoleでの作業を続行できます。

履歴データ移行中、一部の古いデータは利用できない場合があります。データベースの移行にかかる時間は、データのサイズとテーブルの数によって異なります。

NetScaler Console GUIを使用してデータベースの移行を監視できます。**アップグレードの進行状況を表示** をクリックすると、**データベース移行ステータス** が表示されます。

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

# 高可用性ペアを14.1リリースにアップグレードする

高可用性モードのNetScaler Consoleサーバーの場合、アクティブノードまたはフローティングIPアドレスのいずれかにアクセスしてアップグレードできます。いずれかのサーバーでアップグレードプロセスを開始すると、両方のNetScaler Consoleサーバーが自動的に最新ビルドにアップグレードされます。

# NetScaler Consoleディザスタリカバリ展開のアップグレード

**注記:**

- HAペアと災害復旧ノードの両方でパスワードが同じであることを確認してください。
- 災害復旧ノードは、スタンドアロンノードまたはHAノードをアップグレードした後にのみアップグレードしてください。プライマリノードまたはHAノードをアップグレードする前に災害復旧ノードをアップグレードすると、データベース同期の問題が発生する可能性があります。

NetScaler Consoleの災害復旧展開のアップグレードは、2段階のプロセスです。

- プライマリサイトで高可用性モードに構成されているNetScaler Consoleノードをアップグレードします。その後、災害復旧ノードをアップグレードする必要があります。
- 災害復旧ノードをアップグレードする前に、高可用性で展開されているNetScaler Consoleサーバーをアップグレード済みであることを確認してください。

## NetScaler Console災害復旧ノードをアップグレードする

1. NetScalerサイトからNetScaler Consoleアップグレードイメージファイルをダウンロードします。
2. このファイルを`nsrecover`資格情報を使用して災害復旧ノードにアップロードします。
3. `nsrecover`資格情報を使用して災害復旧ノードにログオンします。
4. イメージファイルを配置したフォルダに移動し、ファイルを解凍します。
5. 次のスクリプトを実行します。

   ./インストールマス

   

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

# マルチサイト展開用のオンプレミスエージェントをアップグレードする

NetScalerエージェントの展開のアップグレードは3段階のプロセスです。 オンプレミスエージェントをアップグレードする前に、以下のタスクを完了していることを確認してください。

1. 高可用性で展開されているNetScaler Consoleサーバーをアップグレードします。
2. NetScaler Consoleのディザスタリカバリノードをアップグレードします。

   詳細については、NetScaler Consoleのディザスタリカバリ展開のアップグレードを参照してください。

## オンプレミスエージェントのアップグレード

1. NetScalerサイトからNetScalerエージェントアップグレードイメージファイルをダウンロードします。
2. `nsrecover`の資格情報を使用して、このファイルをエージェントノードにアップロードします。
3. 正しいエージェントアップグレードイメージをダウンロードしたことを確認してください。
4. `nsrecover`の資格情報を使用して、オンプレミスエージェントにログオンします。
5. イメージファイルを配置したフォルダーに移動し、ファイルを解凍します。

   ☐
6. 次のスクリプトを実行します。

   ```
   ./installmasagent
   ```

   ☐

# NetScaler Consoleサーバーにディスクを追加する

NetScaler Console のストレージ要件がデフォルトのディスク容量 (120 GB) を超える場合、追加のディスクを接続できます。シングルサーバー展開と高可用性展開の両方で、ディスクを追加できます。

NetScaler Console をリリースバージョン 12.1〜13.10 からアップグレードする場合、以前のバージョンで追加ディスクに作成したパーティションは変更されません。パーティションが削除されたり、サイズ変更されたりすることはありません。

アップグレードされたビルドでも、ディスクを追加する手順は同じです。NetScaler Console の新しいディスクパーティションツールを使用して、新しく追加されたディスクにパーティションを作

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

成できるようになりました。また、このツールを使用して、既存の追加ディスクのパーティションのサイズを変更することもできます。ディスクの追加方法と新しいディスクパーティションツールの使用方法の詳細については、「NetScaler Console に追加ディスクを接続する方法」を参照してください。

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

# 認証

ユーザーは、NetScaler Consoleによる内部認証、認証サーバーによる外部認証、またはその両方で認証できます。ローカル認証を使用する場合、ユーザーはNetScaler Consoleのセキュリティデータベースに存在する必要があります。ユーザーが外部認証される場合、ユーザーの「外部名」は、選択された認証プロトコルに応じて、認証サーバーに登録されている外部ユーザーIDと一致する必要があります。

NetScaler Consoleは、RADIUS、LDAP、およびTACACSサーバーによる外部認証をサポートしています。この統合サポートにより、システムにアクセスするすべてのローカルおよび外部の認証、承認、アカウンティングサーバーユーザーを認証および承認するための共通インターフェイスが提供されます。NetScaler Consoleは、ユーザーがシステムとの通信に使用する実際のプロトコルに関係なく、ユーザーを認証できます。ユーザーが外部認証用に構成されたNetScaler Consoleの実装にアクセスしようとすると、要求されたアプリケーションサーバーはユーザー名とパスワードをRADIUS、LDAP、またはTACACSサーバーに送信して認証します。認証が成功すると、ユーザーはNetScaler Consoleへのアクセスを許可されます。

## 外部認証サーバー

NetScaler Consoleは、すべての認証、承認、および監査サービス要求をリモートのRADIUS、LDAP、またはTACACSサーバーに送信します。リモートの認証、承認、および監査サーバーは要求を受信し、要求を検証し、NetScaler Consoleに応答を送信します。リモートのRADIUS、TACACS、またはLDAPサーバーを認証に使用するように構成されている場合、NetScaler ConsoleはRADIUS、TACACS、またはLDAPクライアントになります。これらの構成のいずれにおいても、認証レコードはリモートホストサーバーデータベースに保存されます。アカウント名、割り当てられた権限、および時間会計レコードも、各ユーザーの認証、承認、および監査サーバーに保存されます。

また、NetScaler Consoleの内部データベースを使用して、ユーザーをローカルで認証することもできます。ユーザーとそのパスワード、およびデフォルトの役割のデータベースエントリを作成します。特定の種類の認証の認証順序を選択することもできます。サーバーグループ内のサーバーのリストは順序付けられたリストです。リストの最初のサーバーは、利用できない場合を除き常に使用され、その場合はリストの次のサーバーが使用されます。構成された認証、承認、および監査サーバーのリストへのフォールバック認証バックアップとして、内部データベースを含めるようにサーバーを構成できます。

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

NetScaler Consoleで次のサーバーを構成および追加できます。

- LDAP認証サーバー(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/add-ldap-authentication-server.html)
- RADIUS認証サーバー(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/add-radius-authentication-server.html)
- TACACS認証サーバー(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/add-tacacs-authentication-server.html)
- 外部認証サーバーとフォールバックオプションを有効にする(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/enable-fallback-local-authentication.html)
- LDAP、RADIUS、およびTACACSによる二要素認証（2FA）のサポート(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/two-factor-authentication-for-external-servers.html)

## NetScaler Consoleでユーザーを認証する

NetScaler Consoleでユーザーを認証する方法は2つあります。

- NetScaler Consoleで構成されたローカルユーザー

  「認証ローカルユーザー」(/en-us/netscaler-application-delivery-management-software/media/auth-local-users-console.png)

  設定後、ローカルサーバーでのユーザー認証のワークフローは次のとおりです。

  「認証ローカルユーザー」(/en-us/netscaler-application-delivery-management-software/media/auth-local-users1-console.png)

  **1** – ユーザーがNetScaler Consoleにログオンします

  **2** – NetScaler Consoleは、認証のためにユーザーに資格情報の入力を求め、NetScaler Consoleデータベースで資格情報が一致するかどうかを確認します。
- 外部認証サーバーの使用

  「認証外部ユーザー」(/en-us/netscaler-application-delivery-management-software/media/auth-external-console.png)

  設定後、外部認証、承認、および監査サーバーでのユーザー認証のワークフローは次のとおりです。

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

「認証外部ユーザー」(/en-us/netscaler-application-delivery-management-software/media/auth-external1-console.png)

**1** – ユーザーがNetScaler Consoleに接続します

**2** – NetScaler Consoleはユーザーに資格情報の入力を求めます

**3** – NetScaler Consoleは、外部認証、承認、および監査サーバーでユーザー資格情報を検証します。検証が成功した場合、ユーザーはログオンを続行できます。

# LDAP認証サーバーを追加

LDAPプロトコルをRADIUSおよびTACAS認証サーバーと統合すると、NetScaler Consoleを使用して分散ディレクトリからユーザー資格情報を検索および認証できます。

1. **>** の順に移動します。
2. タブを選択し、 をクリックします。
3. ページで、次のパラメーターを指定します。

   a. **名前** – LDAPサーバー名を指定します

   b. **サーバー名/IPアドレス** – LDAPのIPアドレスまたはサーバー名を指定します

   c. **セキュリティの種類** – システムとLDAPサーバー間で必要な通信の種類。リストから選択します。プレーンテキスト通信が不十分な場合は、トランスポート層セキュリティ (TLS) またはSSLのいずれかを選択して、暗号化された通信を選択できます。

   d. **ポート** – デフォルトでは、ポート389がPLAINTEXTに使用されます。SSL/TLSにはポート636を指定することもできます。

   e. **サーバーの種類** – LDAPサーバーの種類として、Active Directory (AD) またはNovell Directory Service (NDS) を選択します。

   f. **タイムアウト (秒)** – NetScaler Consoleシステムが LDAPサーバーからの応答を待機する時間 (秒単位)。

   g. **LDAPホスト名** – チェックボックスをオンにし、証明書に入力するホスト名を指定します。

      オプションをクリアし、SSH公開キーを指定します。キーベース認証を使用すると、SSHを介してLDAPサーバーのユーザーオブジェクトに保存されている公開キーのリストを取得できます。

      LDAP(/en-us/netscaler-application-delivery-management-software/media/ldap.png)

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

接続設定で、次のパラメーターを指定します。

i. **ベースDN** – LDAPサーバーが検索を開始するためのベースノード
ii. **管理者バインドDN** – LDAPサーバーにバインドするためのユーザー名。例: admin@aaa.local。
iii. **バインドDNパスワード** – 認証用のパスワードを指定するには、このオプションを選択します
iv. **パスワード変更を有効にする** – パスワード変更を有効にするには、このオプションを選択します



**その他の設定**で、次のパラメータを指定します

i. **サーバーログオン名属性** – システムが外部LDAPサーバーまたはActive Directoryを照会するために使用する名前属性。リストから**samAccountname**を選択します。
ii. **検索フィルター** – LDAPサーバーで構成された検索フィルターに従って、二要素認証用の外部ユーザーを構成します。例: ldaploginame `samaccount` とユーザーが指定したユーザー名 bob を使用した vpnallowed=true は、次のLDAP検索文字列を生成します: `&(vpnallowed=true)(samaccount=bob)`。

注

デフォルトでは、検索フィルターの値は角括弧で囲まれています。

iii. **グループ属性** – リストからmemberOfを選択します。
iv. **サブ属性名** – LDAPサーバーからのグループ抽出用のサブ属性名。
v. **デフォルト認証グループ** – 抽出されたグループに加えて、認証が成功した場合に選択するデフォルトのグループ。



4. **作成**をクリックします。

LDAPサーバーが設定されました。

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

**注**

ユーザーがActive Directoryグループのメンバーである場合、NetScaler Console上のグループ名とユーザー名は、Active Directoryグループメンバーの名前と同じである必要があります。

5. 外部認証サーバーを有効にします。

   外部認証サーバーの有効化とフォールバックオプションの詳細については、「外部認証サーバーとフォールバックオプションを有効にする」を参照してください。

## RADIUS認証サーバーを追加

1. **設定 > 認証**に移動します。
2. **RADIUS**タブを選択し、**追加**をクリックします。

   **RADIUSサーバーの作成**ページで、次のパラメータを指定します。

   a. **名前** – RADIUSサーバー名を指定します
   b. **サーバー名 / IPアドレス** – RADIUSサーバーのIPアドレスを指定します
   c. **ポート** – RADIUSサーバーがホストされているポート番号を指定します。デフォルトのポートは1812です。
   d. **タイムアウト (秒)** – NetScaler ConsoleシステムがRADIUSサーバーからの応答を待機する時間（秒単位）
   e. **シークレットキー** – 認証用のRADIUSシークレットキーを指定します
   f. **シークレットキーの確認** – 確認のため、キーを再度指定します

   ☐ **詳細**で、次のパラメータを指定します。

      i. **NAS ID** – 識別子をRADIUSサーバーに送信するためのIDを指定します
      ii. **グループベンダー識別子** – RADIUSグループ抽出に使用するベンダーIDを指定します
      iii. **グループプレフィックス** - RADIUSグループ抽出のために、RADIUS属性内のグループ名の前に付加される文字列
      iv. **グループ属性タイプ** – RADIUSグループ抽出の属性タイプを指定します。

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

v. **グループセパレーター** – RADIUSグループ抽出のために、RADIUS属性内のグループ名を区切る文字列。

vi. **IPアドレスベンダー識別子** – RADIUSのベンダーIDはイントラネットIPを示します。値が0の場合、属性がベンダーエンコードされていないことを示します。

vii. **パスワードベンダー識別子** – ユーザーパスワードを抽出するためのRADIUS応答におけるベンダーIDパスワード。

viii. **IPアドレス属性タイプ** – RADIUSが応答するためのリモートIPアドレス属性。

ix. **パスワード属性タイプ** – RADIUSが応答するためのパスワード属性。

x. **パスワードエンコーディング** – リストからpap、chap、mschapv1、またはmschapv2を選択します。これは、システムからRADIUSサーバーに送信されるRADIUSパケットでパスワードがどのようにエンコードされるべきかを示します。

xi. **デフォルト認証グループ** – 抽出されたグループに加えて、認証が成功したときに選択するデフォルトグループ。

アプライアンスがRADIUSサーバーで監査情報をログに記録する場合は、「アカウンティング」を選択します。

3. **作成**をクリックします。

RADIUSサーバーが構成されました。

4. 外部認証サーバーを有効にします。

外部認証サーバーの有効化の詳細については、「外部認証サーバーとフォールバックオプションの有効化」(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/enable-fallback-local-authentication.html#configure-fallback-and-cascade-external-servers)を参照してください。

# TACACS認証サーバーを追加する

1. **設定 > 認証**に移動します。
2. **TACACS**タブを選択し、**追加**をクリックします。
3. **TACACSの作成**ページで、次のパラメーターを指定します。

a. **名前** – TACACSサーバー名を指定します

b. **IPアドレス** – TACACSのIPアドレスを指定します

c. **ポート** – TACACSサーバーがホストされているポート番号を指定します。デフォルトのポートは49です

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

d. **タイムアウト（秒）** – NetScaler ConsoleシステムがLDAPサーバーからの応答を待機する時間（秒）

e. **TACACSキー** – 認証用のTACACSキーを指定します

f. **TACACSキーの確認** – 確認のため、TACACSキーを再度指定します

g. **グループ属性名** – グループ名を指定します

アプライアンスで監査情報をTACACSサーバーにログ記録する場合は、**アカウンティング**を選択します。

4. **作成**をクリックします。



5. 外部認証サーバーを有効にします。

外部認証サーバーの有効化に関する詳細については、「外部認証サーバーとフォールバックオプションを有効にする」(/ja-jp/netscaler-application-delivery-management-software/current-release/authentication/enable-fallback-local-authentication.html#configure-fallback-and-cascade-external-servers)を参照してください。

# NetScaler Console のユーザー

NetScaler Console でローカルにユーザーアカウントを作成して、認証サーバー上のユーザーを補完できます。たとえば、コンサルタントや訪問者などの一時的なユーザーのために、認証サーバーにエントリを作成せずにローカルユーザーアカウントを作成したい場合があります。

ユーザーの設定の詳細については、ユーザーの設定を参照してください。

注

ユーザーがActive Directoryにいる場合は、NetScaler Consoleのグループ名が、外部サーバー上のActive Directoryグループの名前と同じであることを確認してください。

## NetScaler Console のユーザーグループ

NetScaler Consoleでは、グループを作成し、ユーザーをグループに追加することで、ユーザーを認証および承認できます。グループには「管理者」または「読み取り専用」のいずれかの権限を設定でき、そのグループ内のすべてのユーザーは同等の権限を受け取ります。

NetScaler Consoleでは、次のようになります。

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

- グループは、同様の権限を持つユーザーの集合として定義されます
- グループは1つまたは複数のロールを持つことができます
- ユーザーは、割り当てられた権限に基づいてアクセスできるエンティティとして定義されます
- ユーザーは1つまたは複数のグループに属することができます

NetScaler Consoleでローカルグループを作成し、グループ内のユーザーにローカル認証を使用できます。認証に外部サーバーを使用している場合は、NetScaler Console上のグループを、内部ネットワーク内の認証サーバーで設定されているグループと一致するように構成します。ユーザーがログオンして認証されたときに、グループ名が認証サーバー上のグループと一致する場合、ユーザーはNetScaler Console上のグループの設定を継承します。 ローカル認証を使用している場合は、ユーザーを作成し、NetScaler Consoleで構成されたグループに追加します。その後、ユーザーはそれらのグループの設定を継承します。

グループの設定とグループ権限の割り当ての詳細については、グループの設定を参照してください。

## 認証サーバーグループを抽出する

**注**

TACACSサーバーの抽出は、**NetScaler Console 13.0**からサポートされています。

NetScaler Consoleでは、次のことが可能です。

- 外部認証サーバー上でユーザーが属するグループのリストを抽出します。
- 外部サーバーで構成されたグループと一致するグループ設定にそれらを割り当てます。

**利点**:

- ユーザーは外部サーバーで管理されているため、NetScaler Consoleでユーザーを作成する必要はありません。
- NetScaler Consoleは、特定のロードバランサー仮想サーバーへのアクセス、およびシステム上の特定のアプリケーションに対するグループ権限を割り当てることにより、ユーザーの承認を実行します。

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

# 外部認証サーバーとフォールバックオプションを有効にする

フォールバックオプションを使用すると、外部サーバー認証が失敗した場合にローカル認証が引き継ぐことができます。NetScaler Consoleと外部認証サーバーの両方で設定されたユーザーは、設定された外部認証サーバーがダウンしているか到達不能な場合でも、NetScaler Consoleにログオンできます。フォールバック認証が機能するようにするには、次の点を確認してください。

- 外部サーバーがダウンしているか到達不能な場合でも、nsroot以外のユーザーがNetScaler Consoleにアクセスできる必要があります
- 少なくとも1つの外部サーバーを追加する必要があります

NetScaler Consoleは、ローカル認証とともに、認証、認可、アカウンティング (AAA) プロトコル (LDAP、RADIUS、TACACS) の統合システムもサポートしています。この統合サポートにより、システムにアクセスするすべてのユーザーと外部AAAクライアントを認証および認可するための共通インターフェイスが提供されます。

NetScaler Consoleは、システムと通信するために使用する実際のプロトコルに関係なく、ユーザーを認証できます。 外部認証サーバーをカスケード接続することで、外部ユーザーを認証および認可するための継続的で失敗しないプロセスが提供されます。最初の認証サーバーで認証が失敗した場合、NetScaler Consoleは2番目の外部認証サーバーを使用してユーザーを認証しようとします。カスケード認証を有効にするには、NetScaler Consoleに外部認証サーバーを追加する必要があります。サポートされている外部認証サーバー (RADIUS、LDAP、TACACS) の任意のタイプを追加できます。

たとえば、4つの外部認証サーバーを追加し、2つのRADIUSサーバー、1つのLDAPサーバー、1つのTACACSサーバーを設定するとします。NetScaler Consoleは、設定に基づいて外部サーバーで認証を試みます。このシナリオ例では、NetScaler Consoleは次を試みます。

- 最初のRADIUSサーバーに接続する
- 最初のRADIUSサーバーでの認証が失敗した場合、2番目のRADIUSサーバーに接続する
- 両方のRADIUSサーバーでの認証が失敗した場合、LDAPサーバーに接続する
- 両方のRADIUSサーバーとLDAPサーバーでの認証が失敗した場合、TACACSサーバーに接続する。

注

> NetScaler Consoleでは、最大32の外部認証サーバーを設定できます。

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

### フォールバックおよびカスケード外部サーバーを設定する

1. **設定 > 認証 > 認証設定** に移動します。
2. 「**Authentication Settings**」ページで、「**External server authentication**」の下にある「**Enable single-factor authentication**」をクリックします。
3. 「**Enable single-factor authentication**」ページで、「**Select servers**」をクリックします。1つまたは複数の認証サーバーを選択し、「**Add**」をクリックします。
4. 外部認証が失敗した場合にローカル認証に切り替えたい場合は、「**Fallback to local authentication if external authentication fails**」を選択します。
5. システム監査ログに外部ユーザーグループ情報を記録したい場合は、「**Record external user group information in system logs**」を選択します。
6. ページを閉じるには、「**Submit**」をクリックします。

   選択したサーバーは「**Authentication Settings**」ページに表示されます。

   外部サーバー(/en-us/netscaler-application-delivery-management-software/media/external-servers.png)

サーバー名の横にあるアイコンを使用して、リスト内でサーバーを上下に移動することで、認証の順序を指定することもできます。

## LDAP、RADIUS、TACACS を使用した二要素認証 (2FA) のサポート

多要素認証は今日のセキュリティのベストプラクティスであり、ほとんどの組織はコンプライアンス基準を満たすために、ネットワークアプライアンスに対して少なくとも2つの認証要素を要求しています。二要素認証は、製品がユーザーを2つのレベルで認証するセキュリティメカニズムです。両方のレベルで検証が成功した場合にのみ、アクセスが許可されます。

NetScaler Console 14.1-43.x 以降では、NetScaler Console オンプレミスで二要素認証 (2FA) がサポートされています。NetScaler Console オンプレミスへの認証要素として、LDAP、RADIUS、TACACS を使用できます。

**注:**

二要素認証のサポートは、外部サーバー認証でのみ利用可能です。

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

二要素認証が有効になっているNetScaler Consoleにユーザーがログインしようとすると、最初の外部認証のためにユーザー名とパスワードの入力を求められます。最初の認証が成功すると、ユーザーは2番目のレベルの認証を求められます。

ユーザーは、両方のパスワードが正常に検証された後にのみ完全に認証されます。認証が失敗した場合、失敗の理由がユーザーに表示されます。

ユーザーがローカルで認証される場合、ユーザープロファイルはNetScaler Consoleデータベースに作成されている必要があります。ユーザーが外部で認証される場合、ユーザー名とパスワードは外部認証サーバーに登録されているユーザーIDと一致している必要があります。

外部サーバーの二要素認証(/en-us/netscaler-application-delivery-management-software/media/two-factor-authentication.png)

## 二要素認証を構成する

1. NetScaler Console オンプレミスにログインし、**Settings > Authentication > Authentication Settings** に移動します。 認証設定(/en-us/netscaler-application-delivery-management-software/media/authentication-settings.png)
2. **External server authentication** セクションで、**Authentication modes** の下にある **Enable two-factor authentication** をクリックします。
3. **Enable two-factor authentication** ページで、**Step 1: Primary servers** の下にある **Add Servers** をクリックします。

   二要素認証(/en-us/netscaler-application-delivery-management-software/media/enable-two-factor-authentication.png)
4. **Select Servers** をクリックし、必要なサーバーを選択します。**Add** をクリックし、次に **Done** をクリックします。

   
5. 「**2要素認証を有効にする**」ページで、「**ステップ2: セカンダリサーバー**」の下にある「**サーバーの追加**」をクリックします。
6. 「**2要素認証フィールドのラベル**」に、2要素認証用に構成されたサーバーへの認証に使用するラベルを入力します。
7. 「**サーバーの選択**」をクリックし、必要なサーバーを選択します。「**追加**」をクリックし、次に「**完了**」をクリックします。

   
8. 「**送信**」をクリックします。

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

## 2要素認証を使用したNetScaler® Consoleへのユーザーアクセス

1. WebブラウザでNetScaler ConsoleのIPアドレスを入力します。ログインページが表示されます。

   

2. 「**ユーザー名**」フィールドと「**パスワード**」フィールドにユーザー名とパスワードを入力します。この手順が最初の要素認証です。
3. 最初の要素認証が成功すると、ユーザーは2要素認証を求められます。2要素認証用に構成されたラベルを入力します。

   

4. 2番目の要素認証が成功すると、ユーザーはNetScaler Console GUIにログインします。

   

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

# アクセスコントロール

認証とは、ある人物が主張する本人であることを確認するプロセスです。認証を実行するには、ユーザーは認証メカニズムによって照会可能なシステムにアカウントがすでに作成されているか、最初認証のプロセスの一部としてアカウントが作成される必要があります。NetScalerは、ローカルユーザーと外部ユーザーの両方を認証する方法を提供します。ローカルユーザーは内部で認証されますが、NetScaler ConsoleはRADIUS、LDAP、TACACSプロトコルを使用した外部認証をサポートしています。外部認証用に構成されたNetScaler Consoleにユーザーがアクセスしようとすると、要求されたアプリケーションサーバーはユーザー名とパスワードをRADIUS、LDAP、またはTACACSサーバーに送信して認証します。認証が完了すると、必要なプロトコルを使用してNetScaler Console上でユーザーを識別します。

Access Control is the process of enforcing the required security for a particular resource. It is a security technique that can be used to regulate who can view or use resources in a computing environment. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, and what programs running on behalf of the users are allowed to do. In this way access control seeks to prevent activity that can lead to a breach of security. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control through a reference monitor. NetScaler Console allows fine-grained, role-based access control (RBAC) by which the administrators can provide access permissions to users based on the roles of individual users within an enterprise. RBAC in NetScaler Console is achieved by creating access policies, roles, groups, and users.

## ロールベースのアクセス制御

NetScaler Console は、きめ細かなロールベースのアクセス制御 (RBAC) を提供します。これにより、企業内の個々のユーザーの役割に基づいてアクセス権限を付与できます。この文脈において、アクセスとは、ファイルの表示、作成、変更、削除などの特定のタスクを実行する能力を指します。役割は、企業内のユーザーの権限と責任に応じて定義されます。たとえば、あるユーザーはすべてのネットワーク操作を実行できる一方で、別のユーザーはアプリケーションのトラフィックフローを監視し、構成テンプレートの作成を支援できます。

役割はポリシーによって決定されます。ポリシーを作成した後、役割を作成し、各役割を1つ以上のポリシーにバインドし、ユーザーに役割を割り当てます。ユーザーのグループに役割を割り当てることもできます。

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

A group is a collection of users who have permissions in common. For example, users who are managing a particular data center can be assigned to a group. A role is an identity granted to users or groups based on specific conditions. In NetScaler Console, creating roles and policies are specific to the RBAC feature in NetScaler. Roles and policies can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

役割は、機能ベースまたはリソースベースにすることができます。たとえば、SSL/セキュリティ管理者とアプリケーション管理者を考えてみましょう。SSL/セキュリティ管理者は、SSL証明書の管理および監視機能への完全なアクセス権を持つ必要がありますが、システム管理操作に対しては読み取り専用アクセス権を持つ必要があります。アプリケーション管理者は、スコープ内のリソースのみにアクセスできる必要があります。

**例:**

Chris, the NetScaler group head, is the super administrator of NetScaler Console in his organization. Chris creates three administrator roles: security administrator, application administrator, and network administrator.

セキュリティ管理者であるDavidは、SSL証明書の管理と監視に対して完全なアクセス権を持つ必要がありますが、システム管理操作に対しては読み取り専用アクセス権も持つ必要があります。

アプリケーション管理者であるSteveは、特定のアプリケーションと特定の構成テンプレートにのみアクセスする必要があります。

ネットワーク管理者であるGregは、システムおよびネットワーク管理へのアクセスを必要とします。

Chrisはまた、ユーザーがローカルであるか外部であるかに関わらず、すべてのユーザーにRBACを提供する必要があります。

NetScaler Console ユーザーはローカルで認証することも、外部サーバー (RADIUS/LDAP/TACACS) を介して認証することもできます。RBAC 設定は、採用されている認証方法に関わらず、すべてのユーザーに適用可能である必要があります。

次の画像は、管理者およびその他のユーザーが持つ権限と、組織における彼らの役割を示しています。



## 制限事項

RBAC は、以下の NetScaler Console 機能では完全にサポートされていません。

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

- **Analytics** - RBAC は、Analytics モジュールでは完全にサポートされていません。RBAC のサポートはインスタンスレベルに限定されており、Web Insight、SSL Insight、Gateway Insight、HDX™ Insight、および WAF Security Violations の各 Analytics モジュールではアプリケーションレベルには適用されません。例:

**例 1**: インスタンスベースの RBAC (サポート対象)

割り当てられたインスタンスがいくつかある管理者は、**Web Insight** \> **Instances** の下にそれらのインスタンスのみを表示でき、**Web Insight** \> **Applications** の下には対応する仮想サーバーのみを表示できます。これは、RBAC がインスタンスレベルでサポートされているためです。

**例 2**: アプリケーションベースの RBAC (サポート対象外)

割り当てられたアプリケーションがいくつかある管理者は、**Web Insight** \> **Applications** の下にすべての仮想サーバーを表示できますが、それらにアクセスすることはできません。これは、RBAC がアプリケーションレベルでサポートされていないためです。

- **Orchestration** - RBAC は Orchestration ではサポートされていません。

## アクセス ポリシーを構成する

アクセス ポリシーは権限を定義します。ポリシーは、単一のユーザーまたはグループ、あるいは複数のユーザーと複数のグループに適用できます。NetScaler Console には、次の 4 つの事前定義されたアクセス ポリシーが用意されています。

1. **adminpolicy**。すべての NetScaler Console 機能へのアクセスを許可します。ユーザーは表示権限と編集権限の両方を持っており、すべての NetScaler Console コンテンツを表示でき、すべての編集操作を実行できます。つまり、ユーザーはリソースに対して追加、変更、削除の操作を実行できます。
2. **readonlypolicy**。読み取り専用権限を付与します。ユーザーは NetScaler Console のすべてのコンテンツを表示できますが、いかなる操作も実行する権限はありません。
3. **appAdminPolicy**。NetScaler Console のアプリケーション機能にアクセスするための管理者権限を付与します。このポリシーにバインドされたユーザーは、カスタムアプリケーションの追加、変更、削除、およびサービス、サービスグループ、コンテンツスイッチング、キャッシュリダイレクション、HAProxy仮想サーバーなどのさまざまな仮想サーバーの有効化または無効化を行うことができます。
4. **appReadOnlyPolicy**。アプリケーション機能に対する読み取り専用権限を付与します。このポリシーにバインドされたユーザーはアプリケーションを表示できますが、追加、変更、削除、有効化、または無効化の操作を実行することはできません。

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

**注:**

事前定義されたポリシーは編集できません。

独自の (ユーザー定義の) ポリシーを作成することもできます。

**ユーザー定義のアクセス ポリシーを作成するには:**

1. NetScaler Console で、 **> >** の順に移動します。
2. をクリックします。
3. フィールドにポリシーの名前を入力し、 フィールドに説明を入力します。

   セクションには、すべての NetScaler Console 機能が一覧表示され、読み取り専用、有効化/無効化、または編集アクセスを指定するオプションがあります。
4. (+) アイコンをクリックして、各機能グループを複数の機能に展開します。

   a. ユーザーに権限を付与するには、機能名の横にある権限チェックボックスを選択します。

   - **表示:** このオプションを使用すると、ユーザーはNetScaler Consoleで機能を表示できます。
   - **有効化/無効化:** このオプションは、NetScaler Consoleで有効化または無効化アクションを許可する**ネットワーク機能**機能でのみ使用できます。ユーザーは機能を有効または無効にできます。また、ユーザーは**今すぐポーリング**アクションを実行することもできます。

     ユーザーに**有効化/無効化**権限を付与すると、**表示**権限も付与されます。このオプションの選択を解除することはできません。
   - **編集:** このオプションは、ユーザーに完全なアクセス権を付与します。ユーザーは機能とその機能を変更できます。

     **編集**権限を付与すると、**表示**権限と**有効化/無効化**権限の両方が付与されます。自動選択されたオプションの選択を解除することはできません。

   機能のチェックボックスを選択すると、その機能のすべての権限が選択されます。

**注:**

負荷分散とGSLBを展開して、その他の構成オプションを表示します。

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

次の画像では、負荷分散機能の構成オプションに異なる権限があります。

役割ベースのアクセスポリシーを構成する(/en-us/netscaler-application-delivery-management-software/media/service-rbac-configure-policies-2.png)

**仮想サーバー**機能に対して、ユーザーに**表示**権限が付与されます。ユーザーはNetScaler Consoleで負荷分散仮想サーバーを表示できます。仮想サーバーを表示するには、**インフラストラクチャ > ネットワーク機能 > 負荷分散**に移動し、**仮想サーバー**タブを選択します。

**サービス**機能に対して、ユーザーに**有効化/無効化**権限が付与されます。この権限は**表示**権限も付与します。ユーザーは負荷分散仮想サーバーにバインドされているサービスを有効または無効にできます。また、ユーザーはサービスに対して**今すぐポーリング**アクションを実行できます。サービスを有効または無効にするには、**インフラストラクチャ > ネットワーク機能 > 負荷分散**に移動し、**サービス**タブを選択します。

> **注:**
>
> ユーザーが**有効化/無効化**権限を持っている場合、サービスに対する有効化または無効化アクションは次のページで制限されます。

a. **Infrastructure > Network Functions**に移動します。
b. 仮想サーバーを選択し、「**Configure**」をクリックします。
c. 「**Load Balancing Virtual Server Service Binding**」ページを選択します。 「**Enable**」または「**Disable**」を選択すると、このページにエラーメッセージが表示されます。

「**Service Groups**」機能に対して、ユーザーに「**Edit**」権限が付与されます。この権限は、「**View**」および「**Enable-Disable**」権限が付与されている場合にフルアクセスを許可します。ユーザーは、負荷分散仮想サーバーにバインドされているサービスグループを変更できます。サービスグループを編集するには、「**Infrastructure > Network Functions > Load Balancing**」に移動し、「**Service Groups**」タブを選択します。

5. 「**Create**」をクリックします。

### ユーザーにStyleBookの権限を付与する

インポート、削除、ダウンロードなどのStyleBook権限を付与するアクセスポリシーを作成できます。

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

**注:**

他のStyleBook権限を付与すると、View権限は自動的に有効になります。

ユーザーにStyleBook権限を付与する(/en-us/netscaler-application-delivery-management-software/media/access-policy-sb.png)

## グループを構成する

NetScaler Consoleでは、グループは機能レベルとリソースレベルの両方のアクセス権を持つことができます。たとえば、あるユーザーグループは選択されたNetScalerインスタンスのみにアクセスできる場合があります。別のグループは選択された少数のアプリケーションのみにアクセスできる、といった具合です。

グループを作成する際、グループにロールを割り当て、グループにアプリケーションレベルのアクセス権を付与し、ユーザーをグループに割り当てることができます。そのグループ内のすべてのユーザーには、NetScaler Consoleで同じアクセス権が割り当てられます。

NetScaler Consoleでは、ネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。エンティティレベルで、ユーザーまたはグループに特定の権限を動的に割り当てることができます。

NetScaler Consoleは、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。

- **仮想サーバー (アプリケーション)** - ロードバランシング (lb)、GSLB、コンテキストスイッチング (CS)、キャッシュリダイレクション (CR)、認証 ( `Auth` )、およびNetScaler Gateway (VPN)
- **サービス** - ロードバランシングおよびGSLBサービス
- **サービスグループ** - ロードバランシングおよびGSLBサービスグループ
- **サーバー** - ロードバランシングサーバー

### ユーザーグループを作成する

1. NetScaler Consoleで、 **> >** に移動します。
2. をクリックします。

   ページが表示されます。
3. フィールドに、グループの名前を入力します。最大許容長は64文字です。

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

4. フィールドに、グループの説明を入力します。グループの適切な説明を提供することで、後でグループの役割と機能をよりよく理解するのに役立ちます。
5. 「**ロール**」セクションで、1つ以上のロールを「**構成済み**」リストに追加または移動します。

「

**注:**

」.

「**利用可能**」リストの下で、「**新規**」または「**編集**」をクリックして、ロールを作成または変更できます。または、「**設定 > ユーザーとロール > ユーザー**」に移動して、ユーザーを作成または変更することもできます。

6. 「**ユーザーセッションタイムアウトの構成**」を選択して、ユーザーがアクティブな状態を維持する期間を構成します。

   有効にすると、次のパラメータを指定します。

   - 「**セッションタイムアウト**」: ユーザーセッションがアクティブな状態を維持する必要がある期間を入力します。デフォルト値は15です。
   - 「**セッションタイムアウト単位**」: リストからタイムアウト単位（分または時間）を選択します。デフォルト値は分です。

7. 「**ユーザーセッション制限**」フィールドに、ユーザーごとに許可されるセッションの最大数を入力します。

「

**注:**

」.

最大40のユーザーセッションを構成できます。デフォルトでは、20のユーザーセッションが割り当てられます。ただし、管理者および読み取り専用ユーザーグループに属している場合は、デフォルトで40のユーザーセッションが割り当てられ、この値は変更できません。

システムグループの作成(/en-us/netscaler-application-delivery-management-software/media/create-system-group.jpg)

1. 「**次へ**」をクリックします。「**承認設定**」タブで、次のリソースの承認設定を指定できます。

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

- Autoscale™ グループ
- インスタンス
- アプリケーション
- 構成テンプレート
- StyleBook
- 設定パック
- ドメイン名

承認設定のカテゴリ(/en-us/netscaler-application-delivery-management-software/media/categories-authorization-settings.png)

ユーザーがアクセスできるカテゴリから、特定のリソースを選択したい場合があります。

**オートスケールグループ:**

ユーザーが表示または管理できる特定のオートスケールグループを選択する場合は、次の手順を実行します。

a. **すべてのオートスケールグループ**チェックボックスをオフにし、**オートスケールグループの追加**をクリックします。
b. リストから必要なオートスケールグループを選択し、**OK**をクリックします。

**インスタンス:**

ユーザーが表示または管理できる特定のインスタンスを選択する場合は、次の手順を実行します。

a. **すべてのインスタンス**チェックボックスをオフにし、**インスタンスの選択**をクリックします。
b. リストから必要なインスタンスを選択し、**OK**をクリックします。

   インスタンスの選択(/en-us/netscaler-application-delivery-management-software/media/selecting-instances.png)

**タグ**:

関連付けられたタグに基づいて、特定のインスタンスを表示または管理する権限をユーザーに付与するには、次の手順を実行します。

a. **すべてのインスタンス**チェックボックスをオフにし、**タグの選択**をクリックします。

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

b. リストから必要なタグを選択し、**OK**をクリックします。



後で、選択したタグにインスタンスを追加すると、承認されたユーザーは新しいインスタンスに自動的にアクセスできるようになります。

タグとインスタンスへのタグの関連付けの詳細については、「タグを作成してインスタンスに割り当てる方法」を参照してください。

**アプリケーション:**

**アプリケーションの選択**リストを使用すると、必要なアプリケーションへのアクセスをユーザーに許可できます。

インスタンスを選択せずにアプリケーションへのアクセスを許可できます。ユーザーにアプリケーションへのアクセスを許可すると、インスタンスの選択に関係なく、そのアプリケーションにのみアクセスする権限がユーザーに付与されます。

次のオプションが利用可能です。

- **すべてのアプリケーション:** このオプションはデフォルトで選択されています。NetScaler Console に存在するすべてのアプリケーションを追加します。
- **選択したインスタンスのすべてのアプリケーション:** このオプションは、**すべてのインスタンス**カテゴリからインスタンスを選択した場合にのみ表示されます。選択したインスタンスに存在するすべてのアプリケーションを追加します。
- **特定のアプリケーション:** このオプションを使用すると、ユーザーにアクセスさせたい必要なアプリケーションを追加できます。**アプリケーションの追加**をクリックし、リストから必要なアプリケーションを選択します。
- **個々のエンティティタイプの選択:** このオプションを使用すると、特定の種類のネットワーク機能エンティティと対応するエンティティを選択できます。

  個々のエンティティを追加するか、必要なエンティティタイプの下にあるすべてのエンティティを選択して、ユーザーにアクセス権を付与できます。

  「**バインドされたエンティティにも適用**」オプションは、選択したエンティティタイプにバインドされているエンティティを承認します。たとえば、アプリケーションを選択し、「**バインドされたエンティティにも適用**」を選択すると、NetScaler Console は選択したアプリケーションにバインドされているすべてのエンティティを承認します。

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

**注:**

バインドされたエンティティを承認するには、1つのエンティティタイプのみを選択します。

正規表現を使用して、グループの正規表現条件を満たすネットワーク機能エンティティを検索して追加できます。指定された正規表現はNetScaler Consoleに保持されます。正規表現を追加するには、次の手順を実行します。

a. 「**正規表現の追加**」をクリックします。

b. テキストボックスに正規表現を指定します。

次の画像は、「**特定のアプリケーション**」オプションを選択したときに、正規表現を使用してアプリケーションを追加する方法を示しています。



次の画像は、「**個々のエンティティタイプを選択**」オプションを選択したときに、正規表現を使用してネットワーク機能エンティティを追加する方法を示しています。



さらに正規表現を追加する場合は、「**+**」アイコンをクリックします。

**注:**

正規表現は、「**サーバー**」エンティティタイプのサーバー名のみに一致し、サーバーIPアドレスには一致しません。

検出されたエンティティに対して「**バインドされたエンティティにも適用**」オプションを選択すると、ユーザーは検出されたエンティティにバインドされているエンティティに自動的にアクセスできます。

正規表現は、承認スコープを更新するためにシステムに保存されます。新しいエンティティがそのエンティティタイプの正規表現に一致すると、NetScaler Console は承認スコープを新しいエンティティに更新します。

**構成テンプレート:**

ユーザーが表示または管理できる特定の構成テンプレートを選択する場合は、次の手順を実行します。

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

a. **すべての構成テンプレート**チェックボックスをオフにし、**構成テンプレートの追加**をクリックします。

b. リストから必要なテンプレートを選択し、**OK**をクリックします。

**StyleBook:**

ユーザーが表示または管理できる特定のStyleBookを選択する場合は、次の手順を実行します。

a. **すべてのStyleBook**チェックボックスをオフにし、**グループにStyleBookを追加**をクリックします。個々のStyleBookを選択するか、フィルタークエリを指定してStyleBookを承認できます。

個々のStyleBookを選択する場合は、**個々のStyleBook**ペインからStyleBookを選択し、**選択を保存**をクリックします。

クエリを使用してStyleBookを検索する場合は、**カスタムフィルター**ペインを選択します。クエリは、キーが`name`、`namespace`、および`version`であるキーと値のペアの文字列です。

正規表現を値として使用して、グループの正規表現条件を満たすStyleBookを検索および追加することもできます。StyleBookを検索するためのカスタムフィルタークエリは、`And`と`Or`の両方の操作をサポートしています。

例:

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
version=1.0
```

このクエリは、次の条件を満たすStyleBookを一覧表示します。

- StyleBook名は`lb-mon`または`lb`です。
- StyleBookの名前空間は`com.citrix.adc.stylebooks`です。
- StyleBook のバージョンは `1.0` です。

キー式に定義されている値式の間で `Or` 演算を使用します。

例:

- `name=lb-mon|lb` クエリは有効です。名前が `lb-mon` または `lb` のいずれかである StyleBook を返します。

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

- `name=lb-mon | version=1.0` クエリは無効です。

検索結果を表示するには `Enter` を押し、**Save Query** をクリックします。



保存されたクエリは **Custom Filters Query** に表示されます。保存されたクエリに基づいて、NetScaler Console はそれらの StyleBook へのユーザーアクセスを提供します。

b. リストから必要な StyleBook を選択し、**OK** をクリックします。

グループを作成し、そのグループにユーザーを追加する際に、必要な StyleBook を選択できます。ユーザーが許可された StyleBook を選択すると、すべての依存 StyleBook も選択されます。

**構成パック:**

**構成パック**で、次のいずれかのオプションを選択します。

- **すべての構成**: このオプションはデフォルトで選択されています。これにより、ユーザーは NetScaler Console 内のすべての構成を管理できます。
- **選択した StyleBook のすべての構成**: このオプションは、選択した StyleBook のすべての構成パックを追加します。
- **特定の構成**: このオプションを使用すると、任意の StyleBook の特定の構成を追加できます。
- **ユーザーグループによって作成されたすべての構成**: このオプションを使用すると、ユーザーは同じグループのユーザーによって作成された構成のみにアクセスできます。

グループを作成し、そのグループにユーザーを割り当てるときに、該当する構成パックを選択できます。

**ドメイン名:**

ユーザーが表示または管理できる特定のドメイン名を選択する場合は、次の手順を実行します。

a. **すべてのドメイン名**チェックボックスをオフにし、**ドメイン名の追加**をクリックします。

b. リストから必要なドメイン名を選択し、**OK**をクリックします。

2. **グループの作成**をクリックします。
3. **ユーザーの割り当て**セクションで、**利用可能**リストからユーザーを選択し、そのユーザーを**構成済み**リストに追加します。

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

**注:**

**新規**をクリックしてユーザーを追加することもできます。

4. **完了**をクリックします。

### 複数のネットワーク機能エンティティにわたるユーザーアクセスを管理する

管理者として、NetScaler Console のネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。また、正規表現フィルターを使用して、エンティティレベルでユーザーまたはグループに特定の権限を動的に割り当てることができます。

このドキュメントでは、エンティティレベルでユーザー認証を定義する方法について説明します。

始める前に、グループを作成してください。詳細については、NetScaler Console でグループを構成するを参照してください。

**使用シナリオ:**

1つ以上のアプリケーション（仮想サーバー）が同じサーバーでホストされているシナリオを考えてみましょう。スーパー管理者（George）は、Steve（アプリケーション管理者）にApp1へのアクセスのみを許可し、ホスティングサーバーへのアクセスは許可しないようにしたいと考えています。

次の表は、Server-AがアプリケーションApp-1とApp-2をホストしているこの環境を示しています。

| ホストサーバー | アプリケーション（仮想サーバー） | サービス | サービスグループ |
|---|---|---|---|
| サーバーA | App1 | アプリサービス-1 | アプリサービスグループ-1 |
| サーバーA | App2 | アプリサービス-2 | アプリサービスグループ-2 |

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

**注**

NetScaler Console は、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。エンティティタイプである仮想サーバーは、アプリケーションとして参照されます。

ネットワーク機能エンティティにユーザー権限を割り当てるため、George はユーザー認証を次のように定義します。

1. **アカウント > ユーザー管理 > グループ** に移動し、グループを追加します。
2. **認証設定** タブで、 を選択します。
3. **個別のエンティティタイプの選択** を選択します。
4. **すべてのアプリケーション** エンティティタイプを選択し、利用可能なリストから App-1 エンティティを追加します。
5. **グループの作成** をクリックします。
6. **ユーザーの割り当て** で、権限を必要とするユーザーを選択します。このシナリオでは、George は Steve のユーザープロファイルを選択します。
7. **完了** をクリックします。

この認証設定により、Steve は App-1 のみを管理でき、他のネットワーク機能エンティティは管理できません。

**注:**

**バインドされたエンティティにも適用** オプションがオフになっていることを確認してください。そうしないと、NetScaler Console は App-1 にバインドされているすべてのネットワーク機能エンティティへのアクセスを許可します。その結果、ホスティングサーバーへのアクセスも許可されます。

スーパー管理者 は、各エンティティタイプに対して正規表現 (regex) を指定できます。正規表現は、ユーザー認証スコープを更新するためにシステムに保存されます。新しいエンティティがそのエンティティタイプの正規表現に一致する場合、NetScaler Console はユーザーに特定のネットワーク機能エンティティへのアクセスを動的に付与できます。

ユーザー権限を動的に付与するには、スーパー管理者権限を持つユーザーが**承認設定**タブに正規表現を追加できます。

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

このシナリオでは、Georgeがアプリケーションエンティティタイプに正規表現として`App*`を追加すると、正規表現の条件に一致するアプリケーションがリストに表示されます。この承認設定により、Steveは`App*`の正規表現に一致するすべてのアプリケーションにアクセスできます。ただし、彼のアクセスはホストされているサーバーではなく、アプリケーションのみに制限されます。

### 承認スコープに基づいてユーザーアクセスがどのように変化するか

管理者が異なるアクセス ポリシー設定を持つグループにユーザーを追加すると、そのユーザーは複数の承認スコープとアクセス ポリシーにマッピングされます。

この場合、NetScaler Consoleは、特定の承認スコープに応じて、ユーザーにアプリケーションへのアクセスを許可します。

Policy-1とPolicy-2の2つのポリシーを持つグループに割り当てられているユーザーを考えてみましょう。

- **Policy-1** – アプリケーションへの表示のみの権限。
- **Policy-2** – アプリケーションへの表示および編集権限。

ユーザーはPolicy-1で指定されたアプリケーションを表示できます。また、このユーザーはPolicy-2で指定されたアプリケーションを表示および編集できます。Group-1アプリケーションへの編集アクセスは、Group-1の承認スコープに含まれていないため制限されます。

### NetScaler Consoleを12.0からそれ以降のリリースにアップグレードする際のRBACのマッピング

NetScaler Consoleを12.0から13.1にアップグレードする場合、グループ作成時に「読み取り/書き込み」または「読み取り」権限を提供するオプションは表示されません。これらの権限は「ロールとアクセス ポリシー」に置き換えられ、ユーザーにロールベースの権限を付与する柔軟性が向上します。次の表は、リリース12.0の権限がリリース13.1にどのようにマッピングされるかを示しています。

| 12.0 | アプリケーションのみを許可 | 13.1 |
|---|---|---|
| 管理者 (読み書き) | いいえ | `admin` |
| 管理者 (読み書き) | はい | `appAdmin` |
| 管理者 (読み取り専用) | いいえ | `readonly` |

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

| 12.0 | アプリケーションのみを許可 | 13.1 |
| --- | --- | --- |
| 管理者 (読み取り専用) | はい | `appReadonly` |

## ロールの構成

NetScaler Consoleでは、各ロールは1つ以上のアクセスポリシーにバインドされます。ポリシーとロールの間で、1対1、1対多、多対多の関係を定義できます。1つのロールを複数のポリシーにバインドすることも、複数のロールを1つのポリシーにバインドすることもできます。

たとえば、あるロールが2つのポリシーにバインドされている場合、一方のポリシーはある機能のアクセス権限を定義し、もう一方のポリシーは別の機能のアクセス権限を定義する場合があります。あるポリシーはNetScaler ConsoleでNetScalerインスタンスを追加する権限を付与し、別のポリシーはStyleBookを作成および展開し、NetScalerインスタンスを構成する権限を付与する場合があります。

複数のポリシーが単一の機能に対して編集権限と読み取り専用権限を定義している場合、編集権限が優先されます。

NetScaler Consoleには、次の4つの事前定義されたロールが用意されています。

- **admin**。すべてのNetScaler Console機能にアクセスできます。(このロールはadminpolicyにバインドされています。)
- **readonly**。読み取り専用アクセス権があります。(このロールはreadonlypolicyにバインドされています。)
- **appAdmin**。NetScaler Consoleのアプリケーション機能のみに管理アクセス権があります。(このロールはappAdminPolicyにバインドされています。).
- **appReadonly**。アプリケーション機能への読み取り専用アクセス権があります。(このロールはappReadOnlyPolicyにバインドされています。)

**注:**

事前定義されたロールは編集できません。

独自の (ユーザー定義の) ロールを作成することもできます。

**ロールを作成してポリシーを割り当てるには:**

1. NetScaler Consoleで、 **>** に移動します。

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

2. をクリックします。
3. 「**ロール名**」フィールドにロール名を入力し、「**ロールの説明**」フィールドに説明を入力します（オプション）。
4. 「**ポリシー**」セクションで、1つ以上のポリシーを「**構成済み**」リストに追加または移動します。

   ロールの作成(/en-us/netscaler-application-delivery-management-software/media/create-roles.png)
5. 「**作成**」をクリックします。

## ユーザーを構成する

デフォルトでは、NetScaler Consoleには1人のユーザーがいます。

nsroot - ルートユーザー (nsroot) は、アプライアンスに対する完全な管理者権限を持っています。nsroot ユーザーはNetScaler Consoleのスーパー管理者です。

アカウントを構成することで、追加のユーザーを作成できます。NetScaler Consoleに新しいユーザーを追加する際、適切なグループ、ロール、およびポリシーを割り当てることで、そのユーザーの権限を定義できます。

ユーザーをグループに割り当て、そのグループをロールにバインドできます。ユーザー、グループ、ロール、およびアクセスポリシーの間で、1対1、1対多、または多対多の関係を定義できます。ユーザーは複数のグループに割り当てることができます。1つのグループは複数のロールを持つことができ、複数のグループが同じロールを持つこともできます。

**NetScaler Consoleでユーザーを構成するには：**

1. NetScaler Consoleで、**設定 > ユーザーとロール**に移動します。
2. **追加**をクリックします。
3. 次の詳細を入力します。

   a. **ユーザー名**。ユーザーの名前

   b. **パスワード**。ユーザーがNetScaler Consoleにログオンするためのパスワード
4. 必要に応じて、**外部認証を有効にする**を選択すると、ユーザーは外部認証サーバーを介して認証できるようになります。
5. グループを作成済みで、ユーザーをグループに割り当てる場合は、**グループ**セクションで、**利用可能**リストから**構成済み**リストに1つ以上のグループを移動します。

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

システムユーザーの作成(/en-us/netscaler-application-delivery-management-software/media/create-system-user.png)

6. **作成**をクリックします。

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

# 実行可能なタスクと推奨事項

**注:**

- **To Do** タブは **Recommendations** に名称変更されました。**Recommendations** では、既存のタスクを確認し、**Guide Me** をクリックしてタスクを完了できます。
- **Archive** タブは利用できなくなりました。代わりに、リストから推奨事項を **Dismiss** (却下) することを選択できます。

何百もの検出されたNetScalerインスタンスがあり、各インスタンスから複数の仮想サーバー（アプリケーション）を設定している場合があります。管理者として、すべてのNetScalerインスタンスとアプリケーションが効率的に管理され、優先順位付けとトラブルシューティングを改善するための洞察が得られるようにする必要があります。

インフラストラクチャをさらにスケールアップするにつれて、インスタンスやアプリケーションに影響を与え、即座の注意が必要な重大な問題にも焦点を当てる必要があるかもしれません。また、NetScaler Consoleの展開が効率的で、安全で、準拠していることを確認する必要があります。現在の利用状況とサブスクリプションに基づいて、NetScaler Consoleの**Tasks**機能を使用すると、即座に対応する必要がある実行可能な**Tasks**と、効率的な展開を確実にするための**Recommendations**の両方を表示できます。

管理者として、これらの実行可能な**Tasks**と**Recommendations**を利用することで、次のことが可能になります。

- 即座の対応が必要な観察結果や問題について、すぐに可視性を得られます。
- NetScaler Consoleがタスクを検出したときに通知を受け取り、積極的に対応するための通知を設定します。
- NetScaler ConsoleとNetScalerインスタンスの効率的な展開を実現します。
- 重要な問題の特定にかかる時間と労力を削減します。
- NetScaler Consoleのすべての機能を活用し、製品の発見と、展開の効率的な管理のために製品が推奨する機能を有効にします。

NetScaler Console GUIから、**Tasks**をクリックして**Tasks**と**Recommendations**の両方を表示します。

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

- **Tasks** - 即座の注意と対応が必要なタスクのリストを表示できます。インフラストラクチャをスケールアップするにつれて、一部の重大な問題が見過ごされ、セキュリティ侵害につながる可能性があります。たとえば、CVEを持つNetScalerインスタンスは即座の注意が必要であり、インスタンスが推奨されるビルドとバージョンで実行されていることを確認するために即座に対応する必要があります。**Tasks**では、これらの洞察をすぐに得ることができます。現在の利用状況に基づいて、合計4つのタスクを表示できます。タスクは重要度（CriticalとMedium）に基づいて表示されます。

- **推奨事項** - 現在の利用状況に基づいて、NetScaler Consoleの展開を改善するための特定の推奨事項を提供します。**ガイドミー**オプションを使用して、任意の推奨事項を完了できます。**ガイドミー**オプションを使用して完了した推奨事項は、「完了済み」に移動されます。推奨事項を却下することもでき、その場合は**却下済み**カテゴリに移動されます。却下された推奨事項を表示するには、フィルター**ステータス別**を使用し、**却下済み**を選択して、それらの却下された推奨事項を表示します。

  **カテゴリでフィルター**を使用して、カテゴリ（インフラストラクチャ、アプリケーション、セキュリティ）に基づいて特定の推奨事項をフィルターすることもできます。または、**検索**バーを使用して、最初の数文字を入力してタスクを絞り込むこともできます。

# タスク

**タスク**では、現在のNetScaler Consoleの展開に応じて、次の4つのタスクを表示できます。

- **期限切れSSL証明書** – NetScaler Consoleにインストールされている期限切れSSL証明書に関する情報を提供します。このタスクを選択して、次のタブを表示します。
  - **未使用の証明書を削除**: どのNetScalerインスタンスでも使用されていない証明書を表示します。タスクを完了するには、未使用の証明書を確認し、証明書を選択して、**表示して削除**をクリックします。

    **推奨されるアクション**: **インフラストラクチャ > SSLダッシュボード > SSL証明書 - 期限切れ**にリダイレクトされます。証明書を削除するには、**削除**をクリックします。証明書を更新する場合は、証明書を選択して**更新**をクリックします。詳細については、「インストール済み証明書を更新する方法」を参照してください。
  - **証明書を更新**: すでに期限切れになっている証明書を表示します。タスクを完了するには、証明書を確認し、証明書を選択して、**表示して更新**をクリックします。

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

**推奨されるアクション**: **インフラストラクチャ > SSLダッシュボード > SSL証明書 - 期限切れ**にリダイレクトされます。証明書を選択し、**更新**または**削除**をクリックします。詳細については、「インストール済み証明書を更新する方法」を参照してください。

- **期限切れ間近のSSL証明書** – 期限切れ間近のSSL証明書に関する情報を提供します。

  **推奨されるアクション:** このタスクを選択すると、有効期限までの日数に基づいてタブが表示されます。タスクを完了するには、タブから証明書を選択し、**表示して更新**をクリックします。**インフラストラクチャ > SSLダッシュボード**の関連ページにリダイレクトされます。証明書を選択し、**更新**をクリックします。詳細については、「インストール済み証明書を更新する方法」を参照してください。

- **構成ドリフト** – NetScalerインスタンスにおける構成のずれ（保存済みと実行中の差分、テンプレートと実行中の差分）に関する情報を提供します。このタスクを選択して、次のタブを表示します。

  - **未保存の構成を持つインスタンス**: 未保存の構成を持つインスタンスを表示できます。タスクを完了するには、インスタンスを選択し、**構成を表示して保存**をクリックします。

    **推奨されるアクション**: **Infrastructure > Configuration > Configuration Audit > Audit Reports** にリダイレクトされ、未保存の構成を持つインスタンスを表示できます。このタスクを完了するには、**Save Configuration** をクリックします。詳細については、ドキュメントを参照してください。

  - **テンプレートからのドリフトがあるインスタンス**: テンプレートからの逸脱があるインスタンスを表示できます。タスクを完了するには、インスタンスを選択し、**View and Run correct commands** をクリックします。

    **推奨されるアクション**: **Infrastructure > Configuration > Configuration Audit > Audit Reports** にリダイレクトされ、テンプレートからの逸脱があるインスタンスを表示できます。このタスクを完了するには、ドキュメントに従ってください。

- **セキュリティアドバイザリ** – NetScalerインスタンスに影響を与えているCVEに関する情報を提供します。このタスクを選択して、次のタブを表示します。

  - **検出されたCVE**: 検出されたCVEと、そのCVEに影響を与えているNetScalerインスタンスを表示します。このタスクを完了するには、CVEを選択し、**View and Remediate** をクリックします。

    **推奨されるアクション**: **Infrastructure > Instance Advisory > Security Advisory** の **Security Advisory** ページにリダイレクトされます。このタスクを完了するには、ドキュメントに従ってください。

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

- **影響を受けるインスタンス**: CVEの影響を受けているNetScalerインスタンスを表示します。このタスクを完了するには、インスタンスを選択し、**View and Remediate** をクリックします。

  **推奨されるアクション**: **Infrastructure > Instance Advisory > Security Advisory** の **Security Advisory** ページにリダイレクトされます。このタスクを完了するには、ドキュメントに従ってください。

- **アップグレードアドバイザリ**: 90日以内にEnd of Life (EOL) または End of Maintenance (EOM) に達している、または達しようとしているNetScaler®インスタンスに関する情報を提供します。

  **推奨されるアクション**: **Take Action** をクリックし、インスタンスを推奨されるビルドにアップグレードします。

- **SSL A+評価アップグレード**: A+評価に準拠していないアプリケーションに関する情報を提供します。

  **推奨されるアクション**: リストからアプリケーションを選択し、**Upgrade to A+** をクリックします。

  アップグレードが成功すると、次の成功メッセージが表示されます。

  アップグレードが完了すると、タスクからアプリケーションの詳細が削除されます。

  注意点：

  - 選択されたアプリケーションの数によって、アップグレード完了プロセスの所要時間は異なる場合があります。
  - アップグレードプロセスを開始した後、進行中のプロセスが完了してから、別のアップグレードプロセスを開始することをお勧めします。
  - アップグレードプロセスのステータスは、**Infrastructure > Configuration > Configuration Jobs** で確認することもできます。
  - アップグレードプロセスが成功しなかった場合は、**Infrastructure > Configuration > Configuration Jobs** でステータスを確認できます。タスクからアップグレードプロセスを再度開始できます。

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

- 一括アップグレードを実行し、1つ以上のアプリケーションのアップグレードに失敗した場合、タスクで失敗したアプリケーションの詳細のみを表示できます。アップグレードプロセスを再度開始して完了させることができます。

**注：**

- NetScaler Consoleに保留中のタスクがない場合、次のページが表示されます。

- シナリオによっては、すべてのインスタンスでチェックが行われるため、すべてのタスクをロードするのに時間がかかる場合があります。

## 推奨事項

次の表は、NetScaler Console GUIで表示できる推奨事項について説明しています。

**注記**

プールライセンスの場合、既存のプールライセンスの資格に基づいて推奨事項が表示されます。

| 推奨事項名 | タスクがGUIに表示されるタイミングは？ |
| --- | --- |
| NetScalerを追加 | NetScaler Consoleにオンボーディングした後、NetScalerインスタンスが検出されない場合。 |
| NetScaler Consoleで最大限の機能を利用するために外部エージェントを追加 | 外部エージェントが構成されていない場合。組み込みエージェントで開始できます。ただし、分析、プールライセンスなどのすべての機能を使用するには、外部エージェントが必要です。 |
| 組み込みエージェントから外部エージェントへNetScalerを登録 | Service Connectワークフローを使用してNetScaler Consoleにオンボーディングした後、NetScalerインスタンスは組み込みエージェントを使用してオンボーディングされます。それらのNetScalerインスタンスを外部 |

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

| 推奨事項名 | タスクがGUIに表示されるタイミングは？ |
| --- | --- |
| | エージェントに登録して、分析、プールライセンスなどのすべての機能を使用できます。 |
| NetScalerで帯域幅を再割り当てしたいですか？簡単です！ | プールライセンスがNetScaler GUIで割り当てられており、それらのNetScalerインスタンスがNetScaler Consoleで検出された場合、NetScaler Consoleを使用して再割り当てを行うことができます。 |
| 主要なエンタープライズユーザー向けにきめ細かなロールベースアクセスを有効にする | NetScaler Consoleでロールベースアクセス制御 (RBAC) がまだ構成されていない場合。 |
| ルールを構成して、NetScalerインスタンス上の重要なイベントを見逃さないようにする | カスタムイベントルールがまだ設定されていない場合。 |
| 複数のアプリケーションとそのパフォーマンスを監視する必要がありますか？カスタムアプリケーションを作成するだけです。 | カスタムアプリがまだ設定されていない場合。 |
| アプリケーションの重要なイベントを通知し、見逃さないようにします。 | アプリスコアの偏差、サーバー処理時間、クライアントネットワーク遅延、サーバーネットワーク遅延、または応答時間に対してアクションポリシーが設定されていない場合。 |
| アプリケーションの停止を回避し、アプリケーション内の期限切れSSL証明書を見逃さないようにします。 | 期限切れのSSL証明書に対してアラートまたは通知が設定されていない場合。 |
| セキュリティアドバイザリ - NetScalerインスタンスをCVEと緩和策で最新の状態に保ちます。 | NetScalerインスタンスにCVEの影響がある場合。 |
| エンタープライズポリシーを設定し、逸脱がないか監視します。 | SSLエンタープライズ設定が変更されていないか、まだデフォルトのままの場合。 |
| タスクを手動で繰り返していますか？構成ジョブを作成し、複数のNetScalerインスタンスに適用します。 | **Config Job**タスクがまだ設定されていない場合。 |
| 選択したカスタムインジケーターを選択して、インスタンススコアを管理および監視します。 | **Instance Score Settings**のデフォルト設定と閾値が変更されていない場合。 |

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

| 推奨事項名 | タスクがGUIに表示されるタイミングは？ |
| --- | --- |
| 任意のカスタムインジケーターを選択して、アプリケーションスコアを追跡します。 | App DashboardのApp Scoreコンポーネントがデフォルトで使用されており、カスタマイズが行われていない場合。 |
| Geo Mapでクライアント要求を視覚化するために、プライベートIPブロックを追加します。 | IPブロックが構成されていない場合。プライベートIP/範囲に基づいて、Geo Mapでクライアント要求をマッピングおよび視覚化するためのIPブロックを作成できます。 |
| AppSec違反を購読し、リアルタイムでSplunkにエクスポートします。 | NetScaler ConsoleでSplunk統合がまだ構成されていない場合。 |
| デフォルトのしきい値をカスタマイズするか、Kubernetesサービス用に新しいしきい値を作成します。 | サービスグラフでデフォルトのしきい値のみが使用されており、サービスに単一または二重のしきい値が適用されていない場合。 |
| プロアクティブに通知プロファイルを構成し、通信先で通知を受け取ります。 | 通知プロファイルがまだ構成されていない場合。 |
| 定期的なエクスポートをスケジュールし、インフラストラクチャの詳細に関する通知を受け取ります。 | **Infrastructure > Instances**でエクスポートスケジュールがまだ構成されていない場合。 |
| ServiceNowをお持ちで、NetScaler Consoleとの統合を検討していますか？ | NetScaler ConsoleでServiceNow統合がまだ構成されていない場合。 |
| VenafiとNetScaler Consoleを使用してSSL証明書管理を自動化します。 | NetScaler Console で Venafi サーバーがまだ構成されていない場合。 |
| プールライセンスの有効期限が切れる前に更新してください。 | 既存のライセンスが30日以内に期限切れになる場合。 |
| 購入したプール帯域幅をNetScalerインスタンスに割り当てて、プールライセンスの使用を開始してください。 | プールライセンスのエンタイトルメントの割り当てをまだ開始していない場合。 |
| より多くのプール帯域幅容量の購入を検討してください。 | プール帯域幅エンタイトルメントの90%以上を利用している場合。 |

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

| 推奨事項名 | タスクがGUIに表示されるタイミングは？ |
| --- | --- |
| 現在のプール帯域幅エンタイトルメントは十分に活用されていません。見直して、さらに割り当てることを検討してください。 | プールライセンス割り当ての利用率が70%未満の場合。 |

## ガイド付きワークフローを使用して推奨事項を完了する方法?

いずれかのイベントのルールを構成したいとします。次のタスクで **Guide me** をクリックします。

☐

**Guide me** をクリックすると、**Infrastructure > Events > Rules** にリダイレクトされます。**Add** をクリックしてルールを作成します。詳細については、「イベントルールの作成」を参照してください。

ルールの作成が完了すると、推奨事項は完了し、**Completed** に移動されます。

同様に、後で推奨事項を完了したい場合は、リストから **Dismiss** を選択すると、**Dismissed** に移動されます。

推奨事項を却下(/en-us/netscaler-application-delivery-management-software/media/dismiss-recommendation.png)

## 通知を構成する

NetScaler Console が即座の対応を必要とする未処理のタスクを特定するたびに、通知を構成して受け取ることができます。通知を構成していない場合は、右上隅にある **Configure Notification** をクリックできます。

通知(/en-us/netscaler-application-delivery-management-software/media/create-notification.png)

**Notifications** ページで、**Email** と **Slack** のプロファイルを構成し、**Save** をクリックして通知を受け取ることができます。通知タイプごとに、NetScaler Console GUI に構成済みの配布リストまたはプロファイルが表示されます。NetScaler Console は、選択した配布リストまたはプロファイルに通知を送信します。

## よくある質問

1. 管理者に提示される推奨事項の種類は何ですか？

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

現在、推奨事項は展開に特化しており、管理者が展開を効率化するための構成やセットアップタスクに役立ちます。また、製品の発見を向上させ、管理者は、NetScaler Console にその機能が存在するかどうかを知らなくても、タスクが何をするのか、どのように役立つのかを知ることができます。

2. 推奨事項を却下するとどうなりますか？

   却下した推奨事項は **Dismissed** に移動されます。これらの推奨事項は後で完了できます。

3. ガイドを開始して途中で中断した場合、推奨事項は **Completed** になりますか？

   いいえ、アクションが保存または完了されない限り、推奨事項は完了しません。

4. 検索やフィルタリングはできますか？

   はい！検索バーを使用するか、リストからカテゴリを選択して特定のタスクに絞り込むことができます。

5. 動的なイベントに対してアクションを実行するタスクを受け取りますか？

   はい！現在、合計4つの実行可能なタスクを表示できます。詳細については、タスクを参照してください。

6. NetScaler ConsoleにNetScalerインスタンスが追加されていない場合でも、すべての実行可能なタスクと20以上の推奨事項が表示されますか？

   いいえ。すべてのタスクと推奨事項を表示するには、NetScaler ConsoleでNetScalerインスタンスと仮想サーバーの両方が利用可能である必要があります。

7. タスクはどのくらいの頻度で更新されますか？

   左側のナビゲーションペインから**タスク**をクリックすると、それらは更新され、最新のステータスで利用可能になります。詳細が取得され、更新されます。

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

# インスタンスの主要なメトリックの詳細を表示する統合ダッシュボード

NetScaler Consoleでは、アプリケーションの使用状況とパフォーマンス、NetScalerインフラストラクチャ、セキュリティ（BotおよびWAF）違反などに関するさまざまなインサイトを表示できます。管理者として、複数のインサイトを表示するためにNetScaler Console GUIのさまざまなオプションに移動する必要がある場合があります。たとえば、仮想サーバー（アプリケーション）とNetScalerインスタンスのインサイトを確認するには、次の手順を実行します。

- まず、**Applications > Dashboard** に移動して、アプリケーションのインサイトを表示する必要があります。
- 次に、**Infrastructure > Infrastructure Analytics** に移動して、NetScalerインスタンスのインサイトを表示する必要があります。

より良い監視エクスペリエンスのために、必要なすべてのインサイトの概要を含む権限を持つことが必要です。**Overview > Dashboard** に移動して、以下のカテゴリに基づいた主要なメトリックの詳細の概要を示す単一ペインのダッシュボードを視覚化します。

- アプリケーション
- NetScalerインフラストラクチャ
- アプリケーションセキュリティ
- ゲートウェイ

## アプリケーション

**Applications** では、以下を表示できます。

- **Application Health** – **Down** および **Out-of-Service** の状態にあるアプリケーション、および **Critical**、**In Review**、**Good**、**Not Applicable** などのステータスに基づいたアプリケーションの概要を提供します。**View All Applications** をクリックすると、App Dashboardで詳細を表示できます。
- **Golden Signal Anomalies** – サーバーエラーや応答時間の異常があるアプリケーションの概要を提供します。詳細については、**View Details** をクリックしてください。

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

- **Application Config Optimization** – パフォーマンスの問題があるアプリケーション全体の概要を提供します。**See More** をクリックすると、アプリダッシュボードで問題の詳細を表示できます。
- **SSL Certificates** – SSL証明書の概要と有効性を提供します。**Manage SSL Certificates** をクリックすると、SSLダッシュボードで詳細情報を表示できます。
- **アプリケーションSSL構成の最適化** – SSL関連の問題を抱えるアプリケーションの総数の概要を提供します。**詳細を見る**をクリックして、問題の詳細を表示します。



## NetScalerインフラストラクチャ

**NetScalerインフラストラクチャ**の下で、以下のNetScalerインスタンス関連の主要メトリックを表示できます。

- **NetScalerインスタンスの健全性** – インスタンススコアに基づいたNetScalerインスタンスの総数の概要を提供します。
- **CVEの影響を受けるNetScalerインスタンス** – 共通脆弱性識別子 (CVE) の影響を受けるNetScalerインスタンスの総数の概要を提供します。
- **NetScalerインスタンスの問題** – 問題のカテゴリに応じたNetScalerインスタンスの問題の概要を提供します。詳細については、インフラストラクチャ分析を参照してください。
- **NetScalerインスタンスアップグレードの概要** – 最新ビルドではないNetScalerインスタンスの総数の概要を提供します。詳細については、NetScalerインスタンスダッシュボードを表示をクリックしてください。



## アプリケーションセキュリティ

選択した期間に報告された影響を受けるアプリケーションの総数と違反（ボットおよびWAF）の総数の概要を提供します。セキュリティおよびボット違反の詳細を表示するには、**セキュリティダッシュボードを表示**をクリックします。



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

## ゲートウェイ

アクティブなゲートウェイユーザーの総数、アクティブなICA®ユーザーの総数、およびアクティブなICA接続の総数の概要を提供します。エラー、ユーザーログオンの詳細、およびユーザーの場所に関する詳細を提供するジオマップも表示できます。



## ダッシュボードをカスタマイズ

**ダッシュボードの編集**オプションを使用して、好みに応じてダッシュボードビューをカスタマイズできます。**ダッシュボードの編集**オプションを使用すると、次のことができます。

- ウィジェットをドラッグする
- ウィジェット全体を削除する（アプリケーション、NetScalerインフラストラクチャ、Gateway、またはアプリケーションセキュリティ）。
- 各ウィジェットの下にある小さなウィジェットを削除する。
- **ウィジェットの追加**をクリックし、各ウィジェットの下に表示したい必要な主要メトリックを選択します。

  
- デフォルトにリセット
- 最後に保存した状態にリセット

変更後、**保存**をクリックします。

**注**

- デフォルトでは、すべてのウィジェットが表示されます。ダッシュボードをカスタマイズして変更を保存し、再度**デフォルトにリセット**オプションを使用すると、すべてのウィジェットがダッシュボードに追加されます。
- **最後に保存した状態にリセット**オプションは、以前に保存された構成を読み込みます。

## エージェントの詳細を表示

統合ダッシュボードでは、エージェントの詳細の概要を視覚化できます。**概要 > ダッシュボード**で、**NetScaler® Agent Status**の横に、エージェント全体の可用性を分析できる次のステータスが表示されます。

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

- **すべて利用可能**。すべてのエージェントが稼働中であることを示します。
- **すべて利用不可**。すべてのエージェントが停止しており、アクセスできないことを示します。
- **利用不可**。一部のエージェントが停止しており、アクセスできないことを示します。
- **すべてサービス停止中**。すべてのエージェントがサービス停止中であることを示します。
- **サービス停止中**。一部のエージェントがサービス停止中であることを示します。
- **外部エージェントが見つかりません**。エージェント（ハイパーバイザー経由）が設定されていないことを示します。

**詳細を表示**をクリックして、組み込みエージェントの合計数、外部エージェントの合計数、エージェントIP、ステータス、システム使用量、診断チェックなどのエージェント詳細の概要を視覚化します。

## フィルターの作成と適用

以下の選択されたインスタンスまたはアプリケーションに対してのみ、フィルターを適用してインサイトを表示できます。

- アプリケーション
- NetScalerインフラストラクチャ
- アプリケーションセキュリティ

デフォルトでは、すべてのアプリケーションが選択されています。タイルにあるフィルターアイコンをクリックすると、ダッシュボードからカスタマイズされたフィルターを作成できます。

**アプリケーションのフィルター**ウィンドウで：

1. 「**新しいフィルターを作成**」を選択します。
2. 選択に基づいてフィルター名を入力します。
3. 「**アプリケーションの選択**」をクリックし、フィルターに必要なすべてのアプリケーションを追加します。アプリケーションを選択する際に、フィルター（**アプリケーション名**と**タイプ**）を使用してアプリケーションを選択することもできます。

   アプリを選択(/en-us/netscaler-application-delivery-management-software/media/filter-applications-name.png)
4. 「**フィルターを作成して適用**」をクリックします。

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

フィルターを作成して適用(/en-us/netscaler-application-delivery-management-software/media/create-apply-filters.png)

フィルターが作成され、適用されました。同じ手順でさらにフィルターを作成できます。フィルターを作成した後、「**既存のフィルターからフィルターを選択**」リストからフィルターを選択して適用できます。

フィルターを選択(/en-us/netscaler-application-delivery-management-software/media/select-filters.png)

### フィルターの編集

リストからフィルターを選択し、「**編集**」をクリックしてフィルターを編集できます。編集オプションを使用して、アプリケーションを追加または削除し、フィルターを更新できます。

フィルターを編集(/en-us/netscaler-application-delivery-management-software/media/edit-filters.png)

フィルターを削除するには、リストからフィルターを選択し、「**削除**」をクリックします。

**注**

アプリケーションを含むフィルターを作成し、アプリダッシュボードでいずれかのアプリケーションが削除された場合、そのアプリケーションの詳細は統合ダッシュボードからすぐに削除されます。

## インスタンスの主要なメトリックの詳細を表示するためのカスタムダッシュボードを作成する

統合ダッシュボード（**概要 > ダッシュボード**）と同様に、カスタムダッシュボードを作成することで、選択に基づいてインスタンスのメトリック詳細を表示できます。各ダッシュボードに一意の名前を使用することで、最大30個のダッシュボードを作成できます。管理者として、この機能強化により、複数のダッシュボードを作成し、必要なインスタンスのインサイトのみを監視できるようになります。

まず、**アプリケーション**と**アプリケーションセキュリティ**の主要なメトリックを監視したいとします。

1. **概要 > カスタムダッシュボード**に移動します。
2. 新しいダッシュボードを作成するには、**+**をクリックします。

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

**カスタムダッシュボードの作成**ページで：

a. **カスタムダッシュボード名** - ダッシュボードの一意の名前を指定します。

b. **説明** - 追加の詳細情報のために簡単な説明を入力します。

c. **ダッシュボードにウィジェットを追加** - この例では、アプリケーションとアプリケーションセキュリティのウィジェットを追加する必要があります。**アプリケーション**および**アプリケーションセキュリティ**カテゴリから監視したいウィジェットを選択します。

d. **アプリケーションフィルター** - デフォルトでは、フィルターはすべてのアプリケーションに適用されます。フィルターを作成して、特定のアプリケーションのみを選択することもできます。詳細については、「フィルターの作成と適用」を参照してください。

e. **保存**をクリックします。

ダッシュボードが正常に作成されました。同様に、各ダッシュボードに一意の名前を指定することで、最大20個のダッシュボードを作成し、選択に基づいてカテゴリを選択できます。

カスタムダッシュボードを作成した後、次のオプションを使用できます。

- **編集**: ダッシュボードにウィジェットを追加したり、ウィジェットを削除したり、フィルターを適用したりして、ダッシュボードを編集できます。
- **名前変更**: ダッシュボード名を変更できます。
- **削除**: ダッシュボードを削除できます。

## ダッシュボードのその他のオプション

作成したカスタムダッシュボードでは、次のオプションを使用できます。

- **設定の編集**: このオプションを使用して、ウィジェットを追加したり、ウィジェットを削除したり、フィルターを適用したりして、ダッシュボードを編集することもできます。
- **レイアウトの編集**: このオプションを使用して、ダッシュボードをさらにカスタマイズできます。
  - 上に移動、下に移動、または削除を選択できます。
  - ウィジェットでは、「削除」オプションを選択して任意のウィジェットを削除できます。

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

- ウィジェットを好きな場所にドラッグアンドドロップして配置します。
- 特定のインサイトの視認性を高めるために、ウィジェットのサイズを増減します。

「ダッシュボードの変更」(/en-us/netscaler-application-delivery-management-software/media/custom-dashboard-customize.png)

変更を加えたら、**保存**をクリックして更新されたダッシュボードを表示します。

## 他のユーザーとダッシュボードを共有する

ダッシュボードを他のユーザーと共有できます。既存のダッシュボードを選択し、**共有**をクリックします。ユーザー名を入力し、**招待**をクリックしてダッシュボードを共有します。割り当てられたユーザーは、ダッシュボードを読み取り専用モードで表示できます。

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

# アプリケーション

NetScaler Consoleのアプリケーション分析および管理機能を使用すると、アプリケーション中心のアプローチでアプリケーションを監視できます。このアプローチは、次のことに役立ちます。

- アプリケーションのスコアを確認し、全体的なパフォーマンスを分析する
- サーバーまたはクライアントで発生している問題をチェックする
- アプリケーショントラフィックフローの異常を検出し、是正措置を講じる

> **注**
>
> アプリケーションとは、インスタンス (NetScaler) 上に構成されている1つ以上の仮想サーバーを指します。

アプリケーションは、1時間、1日、1週間、1か月などの期間で監視できます。

## 前提条件

- NetScaler ConsoleにNetScalerインスタンスを追加していることを確認します
- NetScalerインスタンスの有効なライセンスがあることを確認します。詳細については、「ライセンス」を参照してください。
- 仮想サーバーにライセンスが適用されていることを確認します。詳細については、「仮想サーバーでのライセンスの管理」を参照してください。

## アプリケーションの概要

アプリケーションには次のものがあります。

- 個別のアプリケーション
- カスタムアプリケーション
- マイクロサービスアプリケーション (k8s_discrete)

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

# ディスクリートアプリケーション

ライセンスが付与されているすべての仮想サーバーは、ディスクリートアプリケーションと呼ばれます。

# カスタムアプリケーション

1つのカテゴリに属する仮想サーバーは、カスタムアプリケーションと呼ばれます。管理者として、カテゴリに基づいてカスタムアプリケーションを追加する必要があります。その後、ダッシュボードを通じてアプリケーションを管理および監視できます。1つのカテゴリにグループ化された特定のアプリケーションを簡単に監視できます。

たとえば、データセンター1のカテゴリを作成し、そのNetScalerインスタンスを追加できます。カテゴリを定義し、データセンター1のインスタンスを追加すると、アプリケーションダッシュボードには、データセンター1に関連するすべてのアプリケーションを含む個別のカテゴリが表示されます。

## 注意点

- カスタムアプリケーションに追加されたディスクリートアプリケーションは、ディスクリートアプリケーションから削除されます。
- いずれのカテゴリにも追加されていないすべてのアプリケーションは、**「その他」**として利用できます。
- デフォルトでは、NetScaler Consoleは最大2つのアプリケーションのライセンスを追加できます。ライセンスに応じて、監視したいアプリケーションのライセンスを選択して適用できます。

# マイクロサービスアプリケーション

Kubernetesクラスターでは、NetScalerはNetScaler MPX（ハードウェア）、NetScaler VPX（仮想化）、およびNetScaler CPX（コンテナ化）用のIngress Controllerを提供します。詳細については、NetScaler Ingress Controllerを参照してください。

NetScaler CPXインスタンスを使用して構成されたディスクリートアプリケーションは、マイクロサービスアプリケーションと呼ばれます。

# アプリケーション管理とアプリケーションダッシュボード

NetScaler Console を使用すると、**アプリケーション**ページからアプリケーションを管理し、**ダッシュボード**ページからアプリケーションの詳細を表示できます。

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

## アプリケーションの管理

アプリケーションダッシュボードから、**アプリの管理**をクリックして、すべてのカスタムアプリケーションと個別アプリケーションを表示します。

**アプリケーションの管理**ページから、管理者として次のことができます。

- アプリケーションの追加
- アプリケーション名、アプリケーションタイプ、アプリケーションカテゴリ、関連付けられた仮想サーバー、関連付けられたサービスなどのアプリケーションの詳細を表示します。
- カスタムアプリケーションの編集または削除

詳細については、「アプリケーションの管理」を参照してください。

## アプリケーションダッシュボード

**アプリケーション** > **ダッシュボード**に移動して、アプリケーションのリストを表形式またはグラフ形式で表示します。



すべてのアプリケーションは、データが入力され始めてからのみダッシュボードに表示されます。ダッシュボードからアプリケーションをクリックすると、アプリケーションのパフォーマンスに関する詳細情報が表示されます。詳細については、「アプリケーションの詳細」を参照してください。

アプリケーション分析が約10〜15分経過しても表示されない場合は、「アプリダッシュボードのトラブルシューティング」でトラブルシューティング手順を実行してください。

### 以前のダッシュボードと比較した新しいダッシュボードの動作の更新点

- カスタムアプリケーションを追加または編集した後、ダッシュボードにアプリケーションが反映されるまでに数分かかる場合があります。
- カスタムアプリケーションを削除しても、NetScaler Consoleがその分析データ（最大1ヶ月間）を保持している間は、ダッシュボードに削除されたアプリケーションが表示され続けます。

  Jan 2, 2020にアプリケーションを作成し、Jan 4, 2020にそのアプリケーションを削除したシナリオを考えてみましょう。このシナリオでは、次のようになります。

  - 過去1日、1週間、1ヶ月の期間を選択した場合、Jan 4, 2020にはダッシュボードに削除されたアプリケーションが引き続き表示されます。

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

- 過去1週間、1ヶ月の期間を選択した場合、Jan 5, 2020にはダッシュボードに削除されたアプリケーションが引き続き表示されます。
- 期間がアプリケーションの削除日を超えると、アプリケーションはダッシュボードに表示されません。つまり、Jan 6, 2020（過去1日）、Jan 12, 2020（過去1週間）、およびFebruary 5, 2020以降（過去1ヶ月）には、削除されたアプリケーションがダッシュボードに表示されません。

  **注**

  アプリケーションを追加した後、関連するNetScalerインスタンスがダウンしている、サービス停止中である、または一時的なネットワーク障害のために到達不能である場合：

  -NetScalerインスタンスに関連付けられたアプリケーションは、**アプリケーション**ページでのみ表示され、ダッシュボードには表示されません。
  -NetScalerインスタンスが稼働状態になった後、アプリケーションはダッシュボードに表示されます。

# アプリケーションの管理

ダッシュボードから、 をクリックしてアプリケーションの詳細を表示し、カスタムアプリケーションを追加、編集、または削除します。

## アプリケーションの詳細を表示

アプリケーションの詳細(/en-us/netscaler-application-delivery-management-software/media/manage-applications.png)

- **アプリ名** – アプリケーション名を示します
- **可用性** – アプリケーションの現在の可用性を示します（例: **Up**、**Down**、**Partially Up**、**Out of Service**、**NA**）
  - **Up** – アプリケーションに関連付けられているすべての仮想サーバーがUpです。
  - **Down** – アプリケーションに関連付けられているすべての仮想サーバーがDownです
  - **Partially Up** – アプリケーションに関連付けられている仮想サーバーのいずれかがDownであるか、サービス停止中です
  - **Out of Service** – アプリケーションに関連付けられているすべての仮想サーバーがサービス停止中です

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

- **NA** – アプリケーション用に仮想サーバーが構成されていません

- **タイプ** – アプリケーションがカスタムまたはディスクリートのどちらに属するかを示します
- **カテゴリ** – グループ化されたアプリケーションカテゴリを示します
- **仮想サーバー/状態** – 構成されている仮想サーバーの合計数と、すべての仮想サーバーの現在の状態を示します。マウス ポインターを合わせると、仮想サーバーの合計数、仮想サーバーの種類、仮想サーバーの状態などの詳細が表示されます

  仮想サーバーの状態(/en-us/netscaler-application-delivery-management-software/media/virtual-server-status.png)
- **サービス/状態** – 設定されているサービスの総数と、すべてのサービスの現在の状態を示します
- **サービスグループ/状態** – 設定されているサービスグループの総数と、すべてのサービスグループの状態を示します
- **サーバー/状態** – アプリケーション用に設定されているサーバーの総数と、すべてのサーバーの現在の状態を示します
- **アクション** – カスタムアプリケーションを編集または削除できます

## アプリケーションを追加

1. **New Application** をクリックして新しいアプリケーションを作成します

   **Define Application** ページが表示されます

   

   **注**

   **Applications** をクリックし、次に **New Application** を選択して新しいアプリケーションを追加することもできます

2. 次のパラメータを設定します:

| フィールド | 説明 |
| --- | --- |
| 名前 | カスタムアプリケーションの名前。例: LB_TEST。 |

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

| フィールド | 説明 |
| --- | --- |
| カテゴリ | アプリケーションをグループ化できるカテゴリです。クリックすると、アプリケーションカテゴリページが表示されます。カテゴリを選択し、**選択**をクリックします。カテゴリを追加するには: |
| | 1. **追加**をクリックします |
| | 2. 任意の名前を入力します。 |
| | 3. **作成**をクリックします |
| 既存のアプリケーションを選択 | NetScalerインスタンスに追加された既存のアプリケーションを選択できます。 |
| アプリケーションの追加 | インスタンスで構成されているすべての仮想サーバーが表示されます。リストからアプリケーションを選択し、**OK**をクリックします。 |
| 選択基準の定義 | 仮想サーバー範囲、またはオリジンサーバー/サービスIPアドレス範囲でアプリケーションを定義するオプション。 |
| | - **サーバー。** アプリケーションが実行されているバックエンドサーバーのサーバーまたはサービスIPアドレス、サーバー名、またはポートを指定します。1つのIPアドレス、IPアドレスの範囲、またはその両方をコンマで区切って入力できます。例: 10.102.29.20、10.102.43.10-60、10.216.43.45と入力できます。 |
| | - **仮想サーバー。** 仮想サーバーIPアドレス、仮想サーバー名、またはアプリケーションが実行されているバックエンドサーバーのポートのいずれかを指定できます。1つのIPアドレス、IPアドレスの範囲、またはその両方をコンマで区切って入力できます。例: 10.102.29.20、10.102.43.10-60、10.216.43.45と入力できます。 |

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

| フィールド | 説明 |
| --- | --- |
| StyleBookから新しいアプリケーションを作成 | StyleBookを使用してアプリケーションを作成できます。詳細については、「StyleBookを使用してアプリケーションを作成する」を参照してください。 |

a. 「**OK**」をクリックします。

**注**

現在、アプリケーションダッシュボードは、負荷分散およびコンテンツスイッチング仮想サーバーのみをサポートしています。

アプリケーションダッシュボードがカテゴリとともに表示され、すべてのアプリケーションがその下にグループ化されます。

カスタムアプリケーションで「**StyleBookから新しいアプリケーションを作成**」オプションを選択した場合、NetScaler Consoleがライセンスのために仮想サーバーを自動選択することを許可する必要があります。仮想サーバーの自動選択を有効にするには:

a. 「**設定**」>「**ライセンスと分析の構成**」に移動します。

b. 「**仮想サーバーライセンス割り当て**」の下で、「**仮想サーバーを自動選択**」および「**アドレス指定不可能な仮想サーバーを自動選択**」をクリックして有効にします。

## StyleBookを使用してアプリケーションを作成する

StyleBookを使用してアプリケーションを作成するには:

1. NetScaler Consoleで、「**アプリケーション**」>「**ダッシュボード**」に移動し、「**カスタムアプリの定義**」をクリックしてカスタムアプリケーションを作成します。
2. 「**アプリケーションの定義**」ページで、「**名前**」フィールドにアプリケーションの名前を入力します。
3. 「カテゴリ」セクションからアプリケーションカテゴリを選択します。NetScaler Consoleでは、ユーザー定義アプリケーションをグループ化するためのカテゴリを定義できます。必要に応じて、さらにカテゴリを追加することもできます。
4. 「**StyleBookから新しいアプリケーションを作成**」をクリックして選択し、「**OK**」をクリックします。

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

「StyleBookの選択」ページが表示されます。このページには、NetScaler Consoleで利用可能なすべてのデフォルトStyleBookが含まれています。

5. StyleBookを選択します。 「**構成の詳細**」ページが表示されます。
6. StyleBook内のすべてのパラメータの値を入力します。使用する前に、をクリックしてStyleBookの構成を表示することもできます。

   詳細については、「デフォルトのStyleBookを使用する」を参照してください。
7. **作成**をクリックします。

   選択したNetScalerインスタンスでNetScaler Consoleが作成しようとする構成を確認するには、**ドライラン**をクリックすることもできます。このオプションは、構成の最終チェックを確認するためのテスト目的のみです。ドライランオプションが成功した場合でも、さまざまな理由（IP競合、インスタンスに到達できないなど）により、選択したNetScalerでの実際の構成は失敗する可能性があります。

## アプリケーションの編集または削除

**アプリケーション**ページから、カスタムアプリケーションを編集または削除できます。編集ボタンをクリックしてアプリケーションを編集し、削除ボタンをクリックしてアプリケーションを削除します。

## アプリダッシュボードとセキュリティダッシュボードのレポートをエクスポートする

NetScaler Consoleでは、現在のアプリダッシュボードのスナップショットを取得し、レポートとしてエクスポートできます。アプリ管理者は、これらのレポートを頻繁に使用して、アプリの使用状況とパフォーマンスのペナルティを更新する必要がある場合があります。

この機能により、管理者はこのデータを.png、.jpeg、または.pdfレポートとして抽出できます。

**注**

NetScaler Consoleの他のレポートエクスポートオプションとは異なり、アプリダッシュボードとセキュリティダッシュボードのレポートは.pdfまたは.pngファイルとしてのみエクスポートできます。.csv形式は現在サポートされていません。

レポートはシステムにダウンロードされます。アプリダッシュボードとアプリセキュリティダッシュボードのページから、セカンドレベルのページに移動してレポートとしてエクスポートすることもできます。現在、一度に1つのアプリケーションのレポートのみをダウンロードできます。

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

# アプリケーションの表示

デフォルトでは、アプリケーションダッシュボードにはすべてのアプリケーションが表示されます。要件に応じて、フィルターオプションを使用してアプリケーションを表示できます。

アプリケーションの表示(/en-us/netscaler-application-delivery-management-software/media/view-applications.png)

ダッシュボードには、以下のアプリケーション詳細が表示されます。

- **アプリ名** – アプリケーション名を示します
- **アプリスコア** – アプリケーションスコアと、**Critical**、**Good**、**Fair**、**Not Applicable** などのステータスを示します
- **可用性** – アプリケーションの現在の可用性を示します（例: **Up**、**Down**、**Partially Up**、**Out of Service**、**NA**）
  - **Up** – アプリケーションに関連付けられているすべての仮想サーバーがUpです。
  - **Down** – アプリケーションに関連付けられているすべての仮想サーバーがDownです。
  - **Partially Up** – アプリケーションに関連付けられている仮想サーバーのいずれかがDownまたはOut of Serviceです。
  - **Out of Service** – アプリケーションに関連付けられているすべての仮想サーバーがサービス停止中です。
  - **NA** – アプリケーション用に仮想サーバーが構成されていません。
- **上位の問題** – アプリケーションで最大のエラー数を記録している問題を示します
- **上位の問題カテゴリ** – 問題のカテゴリを示します
- **問題数** – アプリケーションの合計問題数を示します
- **応答時間** – アプリケーションからの平均応答時間を示します
- **エラー率** – アプリケーションの5xxエラーの合計エラー率を示します

> **注**
>
> 5xxエラー率メトリックは、**NetScaler 13.0以降**でのみ表示されます。それ以前のバージョンでは、値は**0**と表示されます。

- **合計リクエスト数** – アプリケーションが受信した合計リクエスト数を示します

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

- **スループット** – アプリケーションの合計ネットワークスループットを示します。スループットは、仮想サーバーのReq Bytes / Sec + Res Bytes / Secによって計算されます
- **データ量** – アプリケーションによって処理された合計データ量を示します
- **クライアント接続** – アプリケーションによって確立された平均クライアント接続数を示します
- **サーバー接続** – アプリケーションによって確立された平均サーバー接続数を示します

## アプリケーションを構成し、複数のカスタムアプリケーションに関連付ける

**アプリケーションダッシュボード**では、アプリケーションを構成し、複数のカスタムアプリケーションに関連付けることができます。この機能を使用すると、カスタムアプリごとに個別のアプリケーションを作成するのではなく、同じアプリケーションを複数のカスタムアプリケーションで再利用できます。

それぞれ**ComABC**と**ComCDE**という名前の2つのeコマースポータルを管理しており、両方のポータルで**PaymentApp**という名前の決済ゲートウェイサーバーを使用したいとします。このシナリオでは、次のことを行う必要があります。

- **ComABC**と**ComCDE**という名前の2つのカスタムアプリを作成します。
- **PaymentApp**という名前のアプリケーションを作成し、それを**ComABC**と**ComCDE**に関連付けます。

このシナリオを実装するには、次のことを行う必要があります。

- **カスタムアプリ（ComABCおよびComCDE）**を作成します。
  a. **アプリケーション > ダッシュボード**に移動し、**アプリの管理**をクリックします。
  b. **新しいアプリケーション**をクリックします。
  c. 名前とカテゴリを指定します。
  d. アプリケーションを選択するタイプを選択します。この例では、**既存のアプリケーションを選択**オプションが選択されています。詳細については、「アプリケーションの追加」を参照してください。
  e. **アプリケーション**の下で、**アプリケーションの追加**をクリックします。
  f. リストからアプリケーションを選択し、**OK**をクリックしてカスタムアプリを作成します。
- **PaymentApp**を作成します。これには、個別のアプリをカスタムアプリに変換する必要があります。

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

a. **アプリケーション > ダッシュボード**に移動し、**アプリの管理**をクリックします。
b. **New Application** をクリックします。
c. 名前とカテゴリを指定します。
d. アプリケーションを選択するタイプを選択します。この例では、 オプションが選択されています。詳細については、「アプリケーションの追加」を参照してください。
e. **Applications** で、**Add Applications** をクリックします。
f. リストからアプリケーションを選択し、**OK** をクリックしてカスタムアプリを作成します。

- 次に、**PaymentApp** を使用して、**ComABC** および **ComCDE** に関連付けることができます。

a. **Applications > Dasboard** に移動し、**Manage Apps** をクリックします。
b. **ComABC** アプリを見つけて、**Edit** をクリックします。



c. **Referenced Applications** で、**Add Custom Applications** をクリックし、**PaymentApp** を選択します。
d. **PaymentApp** が **Referenced Applications** で利用可能になりました。**OK** をクリックして、**PaymentApp** を **ComABC** カスタムアプリに関連付けます。



e. **ComCDE** カスタムアプリについても同じ手順を繰り返します。

**注：**

アプリケーションがカスタムアプリに関連付けられると、カスタムアプリの最終的なアプリスコアは、カスタムアプリと参照されるアプリの間の最低スコアに基づいて計算されます。この例では、**ComABC** アプリのスコアが85で、**PaymentApp** のスコアが69の場合、**ComABC** アプリの最終スコアは69になります。

## アプリケーションダッシュボードの概要

アプリケーションダッシュボードには、「**その他**」の下にある個別のアプリケーションと、それぞれのカテゴリにグループ化されたカスタムアプリケーションが表示されます。

アプリケーションダッシュボードを表示するには、「**アプリケーション**」>「**ダッシュボード**」に移動します。

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

(/en-us/netscaler-application-delivery-management-software/media/app-dashboard.png)

「**1**」 – 選択した期間（1時間、1日、1週間、1か月など）のアプリケーションの詳細を表示します。

「**2**」 – アプリケーションを管理し、新しいアプリケーションを追加できます。

「**3**」 – アプリケーションをテーブルビューまたはグラフビューのいずれかで表示できます。

「**4**」 – 検索バーを使用してアプリケーションを検索できます。

「**5**」 – アプリケーションを表示するためにフィルターを適用できます。クリックして詳細を表示します。

(/en-us/netscaler-application-delivery-management-software/media/app-dashboard-filter.png)

すべてのオプションに簡単にアクセスできるカルーセルスライダーを選択できます。

次のことができます。

- スコアに基づいてアプリケーションを表示するように選択します。
  - 「**重大**」 – アプリケーションスコアが0から40未満の場合
  - 「**良好**」 – アプリケーションスコアが40から75未満の場合
  - **良好** – アプリケーションスコアが75より大きい
  - **該当なし** – アプリケーション用にライセンスされた仮想サーバーが構成されていないか、仮想サーバーのタイプが負荷分散またはコンテンツスイッチングではありません。

    次の表は、以前のアプリスコアと現在のアプリスコアの違いについて説明しています。

| アプリケーションスコア（重大、レビュー、良好、該当なし） | アプリスコア（カラー凡例付きの以前のビュー） |
| --- | --- |
| スコアは、**すべてのアプリケーションの現在の問題のペナルティスコアを100から引いた値**として計算されます | スコアは、**100 – (アプリサーバーリソース + NetScalerシステムリソース)** として計算されます |
| アプリケーションは、**赤（重大）**、**オレンジ（レビュー）**、**緑（良好）**、**グレー（該当なし）**などの色で表示されます | アプリケーションはカラー凡例で表示されます。 |

- 稼働中、停止中、サービス停止中などのアプリケーションステータスに基づいてアプリケーションを表示するには、選択します

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

- 個別またはカスタムなどのアプリケーションタイプに基づいてアプリケーションを表示するには、選択します
- 下にグループ化されたカテゴリに基づいてアプリケーションを表示するには、選択します
- ヒストグラムをドラッグしてフィルターを適用し、アプリケーションを表示します。

  たとえば、仮想サーバーの健全性が0から20の間のアプリケーションを表示したい場合は、仮想サーバーの健全性ヒストグラムをドラッグして結果をフィルターします。

  

  **注**

  ヒストグラムをクリックして、関連するアプリケーションを表示することもできます。

  適用されたフィルターをクリアするには、**すべてクリア**をクリックします。

  

  以下は、フィルターを適用できるアプリケーションの概要です。

  - **応答時間** – アプリケーションが受信した平均応答時間を表示するヒストグラム
  - **エラー率** – アプリケーションの5xxエラーの平均エラー率を表示するヒストグラム
  - **合計リクエスト数** – アプリケーションが受信したリクエストの合計数を表示するヒストグラム
  - **スループット** – アプリケーションによって処理されたネットワークスループットの合計を表示するヒストグラム
  - **データ量** – アプリケーションによって処理されたデータの合計を表示するヒストグラム。データ量は、アプリケーションの合計リクエストバイトと応答バイトによって計算されます。
  - **クライアント接続** – アプリケーションによって確立された平均クライアント接続を表示するヒストグラム
  - **サーバー接続** – アプリケーションによって確立された平均サーバー接続を表示するヒストグラム
  - **送信パケット数** – アプリケーションによって送信されたパケットの合計数を表示するヒストグラム
  - **受信パケット数** – アプリケーションによって受信されたパケットの合計数を表示するヒストグラム

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

- **仮想サーバーの健全性** – 0%から100%のスコア範囲にあるアプリケーションの合計数を表示するヒストグラム。仮想サーバーの健全性は、アプリケーションに関連付けられているアクティブなサービスの割合（%）です。たとえば、仮想サーバーが2つのサービスで構成されており、そのうちの1つがダウンしている場合、スコアは50%です。

## 検索バーを使用して結果を検索およびフィルタリングする

検索バーにマウスポインターを置き、カテゴリを選択して検索を絞り込むことができます。

## アプリケーションにタグを作成して適用する

多数のアプリケーションがある場合は、アプリケーションにタグを作成して適用できます。これらのタグは検索機能を向上させます。

**例:**

次の手順は、負荷分散アプリケーションのタグを作成する手順を示しています。

1. **App Dashboard**で、タグを作成する負荷分散アプリケーションを選択し、**Tags**をクリックします。

   タグ(/en-us/netscaler-application-delivery-management-software/media/app-tags.png)
2. **タグの更新**で:
   - 任意の名前を指定します。例: **Type**。
   - タグを割り当てるための値を指定します。複数の値を入力することもできます。例: **Loadbalance**。
   - **Apply**をクリックします。

     タグの作成(/en-us/netscaler-application-delivery-management-software/media/app-tags1.png)

   タグが作成されます。

タグを適用して負荷分散アプリケーションを取得するには:

1. アプリケーションダッシュボードの検索バーで、テキストボックス内をクリックして作成されたタグを表示し、タグ名を選択します。

   検索バー(/en-us/netscaler-application-delivery-management-software/media/app-tags2.png)
2. オペレーター (**IN**) と作成された値を選択し、「**Search**」をクリックします。

   タグ(/en-us/netscaler-application-delivery-management-software/media/app-tags3.png)

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

**Loadbalance** の下にタグ付けされたすべてのロードバランシングアプリケーションが一覧表示されます。同様に、他のアプリケーションにもタグを作成できます。

# アプリケーションの詳細

**注:**

**14.1-21.x** ビルド以降、NetScaler 管理パーティションから作成されたアプリケーションのメトリック詳細を表示できます。

ダッシュボードからアプリケーションをクリックすると、さらに詳細な情報をドリルダウンして表示できます。

選択したアプリケーションページが表示されます。

アプリケーションの詳細ページから:

- リストから期間を選択して、特定の期間の詳細を表示します
- 選択したアプリケーションのサービスグラフを表示するには、**サービスグラフ**をクリックします。詳細については、「アプリケーションのサービスグラフ」を参照してください。
- 5xx エラーの詳細なトランザクションを表示するには、**トランザクションログ**をクリックします
- 詳細な監査ログ情報を表示するには、**監査ログ**をクリックします
- アプリケーションのサービスおよびサービスグループ構成を表示または編集するには、**構成**をクリックします
- アプリケーションにバインドされているサービスを表示するには、**サービス**をクリックします

期間を選択すると、次のアプリケーションの詳細が表示されます。

- **アプリスコア** – 選択した期間のアプリケーションスコアです。最終スコアは**100から合計ペナルティを引いた値**として計算されます。

  アプリスコア(/en-us/netscaler-application-delivery-management-software/media/app-score-new.png)

  このダッシュボードでは、アプリスコアに影響を与えている現在の問題も表示できます。問題の詳細は「問題」の下で確認できます。

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

- **仮想サーバー** –

  **注**

  **仮想サーバー**セクションは、カスタムアプリケーションに対してのみ表示されます。個別のアプリケーションの場合、**IPアドレス**をクリックして仮想サーバーの詳細を表示します。

  IPアドレス(/en-us/netscaler-application-delivery-management-software/media/app-ip-address.png)

  カスタムアプリケーションに関連付けられているすべての仮想サーバーを表示します

  仮想サーバー(/en-us/netscaler-application-delivery-management-software/media/app-detail-vir-ser.png)

  **詳細を表示**をクリックして、仮想サーバーの設定を表示および管理します。

  仮想サーバーの詳細(/en-us/netscaler-application-delivery-management-software/media/app-detail-vir-ser-details.png)

- **すべてのサービス** – アプリケーションにバインドされているサービス

  すべてのサービス(/en-us/netscaler-application-delivery-management-software/media/app-detail-all-serv.png)

  クリックしてサービスの詳細を表示し、サービス設定を管理します

  すべてのサービスの詳細(/en-us/netscaler-application-delivery-management-software/media/app-detail-all-serv-details.png)

  サービスを選択し、**Bound Monitors** オプションを使用してステータスを表示することもできます。

- **問題** – 選択したアプリケーションに適用される問題。以下の問題をそのカテゴリとともに表示できます。

| パフォーマンス | インスタンスの健全性 | 構成 | システムリソース |
|---|---|---|---|
| 応答時間 | 平均CPU使用率 | 不安定なサーバー | 不適切な永続性タイプ |

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

| パフォーマンス | インスタンスの健全性 | 構成 | システムリソース |
|---|---|---|---|
| アクティブなサービス | メモリ使用量 | 異常に大きなHTTPパケット | NICカードの飽和 |
| セッション再利用率が低い | | TCP再構成キュー制限ヒット | |
| SurgeQueueの蓄積 | | | |
| SSLリアルタイムトラフィック | | | |
| セッションの蓄積 | | | |
| サービスフラップ | | | |

各問題をクリックして、検出メッセージ、問題発生日時、推奨されるアクション、詳細などの情報を確認します。

詳細については、「アプリケーション分析のパフォーマンスインジケーター」を参照してください。

次の画像は、App Activity Investigatorページの以前のビューです。

これで、**Issues**セクションで、**App Activity Investigator**ページで表示できたカテゴリとともに、すべての問題を表示できます。

- **Current**タブに表示される問題は、選択した期間のアプリケーションの問題を指します。
- **All**タブに表示される問題は、アプリケーションの合計問題を指します。

次の例は、1日間のアプリケーションの問題です。**Current**タブは、アプリのスコアに影響を与える現在の問題がないことを示しています。

「**すべて**」タブには、1日間の期間で検出された合計問題が表示されます。

すべて(/en-us/netscaler-application-delivery-management-software/media/issue-all.png)

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

# App Score コンポーネントを選択し、しきい値を設定する

**App Dashboard** では、管理者として、コンポーネントを選択し、App Score 計算のしきい値を構成できます。App Score は、以下を定義するスコアリングシステムです。

- アプリケーションのパフォーマンスがどの程度良好か
- 応答性の観点からアプリケーションが適切に動作しているか

**Applications > Dashboard** に移動し、次に設定アイコンを選択します。

**App Score の構成**ページで、コンポーネントを選択し、しきい値を構成して最終的な App Score を決定できます。

App Score コンポーネント(/en-us/netscaler-application-delivery-management-software/media/app-score-components.png)

App Score の計算は、以下のコンポーネントに基づいています。

| APP SCORE コンポーネント | ユーザーが構成したしきい値 | 説明 |
|---|---|---|
| NetScaler メモリ使用量 | はい | NetScaler インスタンス内の合計メモリ使用量に対する低しきい値と高しきい値 |
| サージキューの蓄積 | はい | キューに入っており、応答が必要なサージリクエストの合計に対する低しきい値と高しきい値。 |
| NetScaler CPU使用率 | はい | NetScalerインスタンスにおけるCPU使用率の合計に対する低しきい値と高しきい値。 |
| 応答時間 | はい | リクエストパケットを送信してから、仮想サーバーで構成されたサービスから最初の応答パケットを受信するまでの時間間隔。 |
| アプリCPU使用率 | はい | アプリケーションによるCPU使用率の合計に対する低しきい値と高しきい値。 |

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

| APP SCORE コンポーネント | ユーザーが構成したしきい値 | 説明 |
|---|---|---|
| アクティブなサービス | はい | 仮想サーバーにバインドされているサービスのうち、アクティブである必要があるサービスの割合のしきい値。 |
| 不適切な永続性タイプ | いいえ | 仮想サーバーでの永続性使用量が低いかどうかを示します。 |
| サーバーエラー (5xx) | いいえ | Webサーバーが5xxエラーで応答するかどうかを示します。 |
| 異常に大きいHTTPパケット | いいえ | HTTPヘッダーサイズを持つHTTPメッセージが、NetScalerインスタンスで設定された値を超過した場合の発生回数を示します。 |
| SSLリアルタイムトラフィック | いいえ | SSLトラフィックを分析してリアルタイムトラフィックを特定し、レイテンシーを改善するための最適な構成設定を提案します。 |
| SSLセッションの蓄積 | いいえ | 一定期間にわたるセッションの蓄積を示します。これは、NetScalerインスタンスでこれらのセッションによって大量のメモリが占有される原因となる可能性があります。 |
| 低いセッション再利用率 | いいえ | NetScalerインスタンスによって再利用されているセッションの実際の数が少ないかどうかを示します。 |
| NICカードの飽和 | いいえ | インターフェイスによって破棄されたパケットの合計数を示します。 |

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

| APP SCORE コンポーネント | ユーザーが構成したしきい値 | 説明 |
| --- | --- | --- |
| TCP再構成キュー制限ヒット | いいえ | TCP接続上の順序が異なるパケットが、設定された順序が異なるパケットキューサイズを超えているかどうかを示します。 |

デフォルトでは、すべてのコンポーネントが有効になっています。いずれかのコンポーネントを無効にすると、NetScaler Consoleは選択されたコンポーネントのみに基づいて最終的なアプリスコア計算を実行します。

注

また、**Settings > Analytics Settings** に移動し、**Configure App Score** をクリックして、しきい値の設定を続行することもできます。

# マイクロサービスアプリケーションのアプリケーション詳細

ダッシュボードからマイクロサービスアプリケーションをクリックすると、さらに詳細な情報が表示されます。

選択したアプリケーションページが表示されます。アプリケーション詳細ページから、次の操作を行います。

- リストから期間を選択して、特定の期間の詳細を表示します
- 選択したアプリケーションのサービスグラフを表示するには、**サービスグラフ**をクリックします。詳細については、「アプリケーションのサービスグラフ」を参照してください。
- 選択したアプリケーションの詳細なトランザクションを表示するには、**トランザクションログ**をクリックします
- 詳細な監査ログ情報を表示するには、**監査ログ**をクリックします

期間を選択すると、次のアプリケーション詳細が表示されます。

- **アプリスコア** – 選択した期間のアプリケーションスコア。現在のアプリケーションの問題も表示できます。これは、問題カテゴリに基づいて適用されるペナルティスコアとして知られています。最終スコアは**100 - 合計ペナルティ**として計算されます。

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



**1** – 現在のアプリスコアを示します

**2** – CPX IPアドレス、ロードバランシングやコンテンツスイッチングなどのアプリケーションタイプ、およびサービスがホストされているサービス名前空間とクラスター名を示します

**3** – 現在のアプリケーションスコアに影響を与えている問題を示します

このダッシュボードでは、アプリスコアに影響を与えている現在の問題も表示できます。問題の詳細は「問題」の下で確認できます。

- **K8sサービスの詳細**

  以下の詳細を表示できます。

  

  - **サービス名** – サービスの名前
  - **クラスター名** – サービスがホストされているクラスターの名前
  - **名前空間** – サービスに割り当てられている名前空間
  - **サービスラベル** – サービスに割り当てられているサービスラベル

- **Podの詳細**

  Podは、Kubernetesクラスターでホストされているコンテナのグループです。Pod内には、複数のコンテナ化されたアプリケーションをデプロイできます。各PodにはIPアドレスが関連付けられています。

  

  Podの状態をクリックして詳細を表示します

  

  - **Pod IPアドレス** – PodのIPアドレスを示します
  - **ホスト名** – Podに割り当てられているホスト名を示します
  - **インスタンス** – NetScaler CPXのIPアドレスを示します
  - **Podの状態** – Podの現在のステータスを示します

- **主要メトリック – 応答時間、5xxエラー、1秒あたりのリクエスト数、スループット、クライアント接続数、サーバー接続数、データ量**などの主要メトリックの詳細が表示されます。

  各メトリックでは、選択した期間の平均値と差分値を表示できます。差分値は、選択した期間の**最初の値から最後の値を引いたもの**として計算されます。

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

選択した期間の以下のインスタンスメトリックをグラフ形式で表示できます。

次の画像は**データ量**の例で、選択された期間は1か月です。202.66 MBは1か月間の総データ量で、8.13 MBは差分値です。グラフでは、最初の値が14.11、最後の値が5.98です。差分値は14.11 – 5.98 = 8.13 MBです。

- **問題** – 選択したアプリケーションに適用される問題。以下の問題をカテゴリとともに表示できます。

| パフォーマンス | インスタンスの健全性 | 構成 | システムリソース |
|---|---|---|---|
| 応答時間 | 平均CPU使用率 | 高い5xx応答 | 不適切な永続性タイプ |
| セッション再利用率が低い | メモリ使用量 | 異常に大きいHTTPパケット | NICカードの飽和 |
| SurgeQueueの蓄積 | | TCP再構成キュー制限ヒット | |
| SSLリアルタイムトラフィック | | | |

各問題をクリックすると、以下の情報が表示されます。

  - 合計発生回数
  - 問題をトラブルシューティングするための推奨アクション
  - 時間、サービス名、合計発生回数、重大度、検出メッセージなどの問題の詳細

    すべての問題(/en-us/netscaler-application-delivery-management-software/media/app-detail-all-issues.png)

    - **Current**タブに表示される問題は、選択された期間のアプリケーションの問題を指します。
    - **All**タブに表示される問題は、アプリケーションのすべての問題を指します。

次の例は、1日間のアプリケーションの問題です。**Current**タブは、アプリのスコアに影響を与える現在の問題がないことを示しています。

「**すべて**」タブには、1日間の期間で検出された合計問題が表示されます。

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



# インテリジェントアプリ分析

インテリジェントアプリ分析を使用すると、機械学習とルールベースのアルゴリズムを使用して、アプリケーションのパフォーマンスの問題を特定できます。NetScaler Console のインテリジェントアプリ分析機能は次のとおりです。

- NetScalerインスタンスを介して配信されるアプリケーションの監視とトラブルシューティングのための、簡単でスケーラブルなソリューションを提供します。
- アプリケーションのあらゆるレベルを監視し、問題のトラブルシューティングにかかる時間を短縮し、アプリケーション全体の稼働時間を向上させます。

一般的な展開では、何千ものサーバーがユーザーのデータニーズに対応します。これらのサーバーに送信されるトラフィックは、NetScalerアプライアンスで構成された仮想サーバーによって負荷分散され、監視されます。各仮想サーバーは、バックエンドサーバーを表す複数のサービスにバインドされています。このような展開では、インテリジェントアプリ分析機能は次のことに役立ちます。

- 停止やその他のイベント中に監視、管理、意思決定を行う
- アプリケーション用に構成された仮想サーバーとサービスを監視する
- 仮想サーバーとサービスに関する重要な情報を表示し、必要に応じて構成を変更して、アプリケーションによる最適なパフォーマンスを達成できるようにします。

組織のサーバーファームをスケールアップすると、サーバーで受信される大量のトラフィックに関連する問題を追跡し、必要なトラブルシューティングに絞り込むことが困難になります。

アプリケーションが実行中で大量のトラフィックを受信している場合、さまざまな問題が発生する可能性があります。アプリケーション分析のパフォーマンスインジケーターを表示するには、**Applications** > **Dashboard** に移動し、アプリケーションを選択して、**Issues** セクションで問題をスクロールダウンして表示します。

## インテリジェントアプリ分析の構成

**注:**

**14.1-21.xビルド**以降、NetScaler Consoleに追加された新しいNetScalerインスタンスでは、Metrics Collectorはデフォルトで無効になっています。既存の管理対象インスタンスのメトリックコレクター構成は変更されません。

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

インテリジェントアプリ分析機能は、**NetScaler 12.1.50.x以降**でのみサポートされています。**Metrics Collector**は、NetScalerカウンターデータをNetScaler Consoleにプッシュし、これはアプリケーションの問題を検出するために使用されます。インテリジェントアプリ分析機能を使用するには、各NetScalerインスタンスで**Metrics Collector**を構成する必要があります。

14.1-29.xビルド以降、メトリックコレクターとリーン使用状況分析は、インスタンスレベルではなく仮想サーバーレベルで有効になります。この機能強化により、Metrics Collectorとリーン使用状況分析は、トラフィックの多いアクティブな仮想サーバーでのみ有効なままになります。

仮想サーバーを確認し、他の仮想サーバーでMetrics Collectorとリーン使用状況を有効にできます

**Metrics Collector**を確認して有効にするには:

1. **設定 > 分析構成**に移動します。
2. **仮想サーバーメトリックの概要**の下にある**メトリックの構成**をクリックします。

   メトリックの構成(/en-us/netscaler-application-delivery-management-software/media/metric-collector-configure.png)
3. **すべての仮想サーバー**ページで、各仮想サーバーのメトリックコレクターのステータスを表示できます。有効にする仮想サーバーを選択し、**メトリックの有効化**をクリックします。

   メトリックの有効化(/en-us/netscaler-application-delivery-management-software/media/metric-collector-enable.png)
4. Metrics Collectorを有効にするには、**メトリックの有効化**を選択します。リーン期間の使用状況分析を有効にして表示する場合は、**リーンデータ**も選択できます。選択後、**構成の保存**をクリックします。詳細については、「ピークとリーン使用状況分析」を参照してください。(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/dashboard/peak-lean-usage-analytics.html).

   構成の保存(/en-us/netscaler-application-delivery-management-software/media/metrics-collector-saveconfig.png)

または、NetScalerインスタンスページから仮想サーバーに対してメトリックコレクターとリーン使用状況を有効にすることもできます。

1. 「**Infrastructure > Instances**」に移動し、インスタンスタイプを選択し、「**Select Action**」リストから「**Metrics Collector**」を選択します。
2. メトリクスコレクターを有効にする仮想サーバーを選択し、「**Enable Metrics**」をクリックします。

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

3. メトリクスコレクターを有効にするには、「**Enable Metrics**」を選択します。リーン期間の使用状況分析を有効にして表示する場合は、「**Lean Data**」を選択することもできます。選択後、「**Save Configuration**」をクリックします。

仮想サーバーで「**Metrics Collector**」オプションが有効になったら、「**Applications**」> 「**Dashboard**」に移動します。「**Issues**」セクションで異常を表示するには、インスタンスを選択します。

「

**注**

」

「**Server Errors**」およびその「**詳細なWebトランザクション**」の異常を表示するには、仮想サーバーでanalyticsを有効にする必要があります。

# アプリケーション分析のパフォーマンス指標

NetScaler Webアプリケーションで発生するパフォーマンス指標とそのカテゴリを表示できます。これらの指標を表示するには、NetScalerインスタンスで分析とメトリクスコレクターを有効にする必要があります。

分析とメトリクスコレクターを有効にすると、**Applications** > **Dashboard** に移動し、アプリケーションを選択して、**Issues** セクションまでスクロールすると、次の指標を表示できます。

- 応答時間
- アクティブサービス
- 平均CPU使用率
- メモリ使用量
- NICカード飽和
- サービスフラップ
- 低セッション再利用
- 不適切なパーシステンスタイプ
- 不安定なサーバー (5xx)
- SSLリアルタイムトラフィック
- 異常に大きなHTTPパケット

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

- TCP再構成キュー制限ヒット
- サージキュー滞留

## レスポンスタイム

この問題は、クライアント要求に応答するアプリケーションの応答時間が、設定されたしきい値から逸脱した場合に検出されます。問題の詳細を表示するには、 タブをクリックします。

レスポンスタイム(/en-us/netscaler-application-delivery-management-software/media/pi-response-time.png)

で、以下を表示できます。

- 選択した時間の合計イベント数を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生した日時
- 選択した時間の合計発生回数
- 低、中、高などの問題の重大度
- 設定されたしきい値を超過した合計トランザクション応答時間を示す検出メッセージ

## アクティブサービス

この問題は、仮想サーバーにバインドされているアクティブサービスの割合が、設定されたしきい値を下回っている場合に検出されます。問題の詳細を表示するには、**アクティブサービス**タブをクリックします。

アクティブサービス(/en-us/netscaler-application-delivery-management-software/media/pi-active-services.png)

**詳細**の下で、以下を表示できます。

- 選択した期間の総イベント数を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生した日時
- 選択した期間の総発生回数
- 低、中、高などの問題の重大度
- アクティブサービスセッションの割合と設定されたしきい値を示す検出メッセージ

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

## 平均CPU使用率

この問題は、このアプリケーションのNetScaler CPU使用率が設定されたしきい値を超えたときに検出されます。問題の詳細を表示するには、**平均CPU使用率**タブをクリックします。

平均CPU(/en-us/netscaler-application-delivery-management-software/media/pi-average-cpu.png)

**詳細**で、以下を表示できます。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生した日時
- 選択した期間の合計発生回数
- 低、中、高などの問題の重大度
- NetScalerの平均CPU使用率（%）と設定されたしきい値を示す検出メッセージ

## メモリ使用量

この問題は、このアプリケーションのNetScalerメモリ使用量が設定されたしきい値を超えた場合に検出されます。問題の詳細を表示するには、**メモリ使用量**タブをクリックします。

**詳細**では、以下を表示できます。

- 選択した期間の合計イベント数を示すグラフ。クリックしてフィルターを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した期間の合計発生回数
- 問題の重大度（低、中、高など）
- NetScalerの平均メモリ使用率と設定されたしきい値を示す検出メッセージ

## サービスフラップ

ネットワーク管理者として、アプリケーションの最適な可用性を確保する必要があります。ネットワークの問題や構成の問題が発生した場合、アプリケーションサーバーのステータスと可用性が全体的なパフォーマンスに影響を与える可能性があります。

サービスフラップイベントを使用すると、問題のあるアプリケーションを特定できます。サービスフラップイベントは、次のことにも役立ちます。

- 特定の期間にどのサービスがDOWN状態であったかを理解する

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

- 特定の期間にいくつのサービスがUPまたはDOWN状態であったかを理解する

**サービスフラップ**タブをクリックして、サービスフラップの詳細を表示します。

サービスフラップ(/en-us/netscaler-application-delivery-management-software/media/service-flaps-new.png)

発生回数や最終発生時刻などの詳細を表示できます。

**詳細**の下で、以下を表示できます。

- サービスフラップの異常が発生した時刻
- サービス/サービスグループ名
- サービスIPアドレス
- 現在のサービスステータス

## 不安定なサーバー

特定のシナリオでは、Webサーバーは、無効なリクエスト、一時的な過負荷、サーバーメンテナンスなどの理由でリクエストを処理できない場合にステータスコードで応答します。これらのエラーは、さまざまなエラーシナリオを定義するエラーコードとともに表示されます。例えば、,

- **502 Bad Gateway** サーバーがゲートウェイまたはプロキシとして機能しており、アップストリームサーバーから無効な応答を受け取りました。
- **503 Service Unavailable** サーバーは現在利用できません。サーバーが過負荷になっているか、メンテナンスのために停止している可能性があります。
- **504 Gateway Time-out** サーバーがゲートウェイまたはプロキシとして機能しており、アップストリームサーバーからタイムリーな応答を受け取りませんでした。

これらは一時的な状態である可能性がありますが、Webページを稼働させ、利用可能にするために、Webサーバーで是正措置を講じる必要がある場合もあります。

**不安定なサーバー**インジケーターを使用すると、これらの障害を表示し、問題を克服し、クライアントリクエストが処理され、Webページが常に利用可能であることを確認するための是正措置について決定を下すことができます。

問題の詳細を表示するには、**不安定なサーバー**タブを選択します。

問題をトラブルシューティングするための**推奨されるアクション**は次のとおりです。

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

- 5xxエラーで応答するサーバーに対して、適切なパラメーターでL7モニターを構成します。モニターは、サービスの状態を追跡するエンティティです。アプライアンスは、各サービスにバインドされたモニターを使用して、サーバーを定期的にプローブします。サーバーが指定された応答タイムアウト内に応答せず、指定されたプローブが失敗した場合、サービスはDOWNとマークされます。その後、アプライアンスは残りのサービス間で負荷分散を実行します。モニターの構成の詳細については、「カスタムモニター」を参照してください。
- サーバーのトラブルシューティング

**詳細**では、以下を表示できます。

- 不安定なサーバーの異常が発生した時刻
- サービス/サービスグループ名
- 合計発生回数
- 高、低、中などの異常度
- このサービスからの応答の%が5xxエラーを報告していることを示す検出メッセージ

サーバーエラーのWebトランザクションの詳細については、Webトランザクション分析（サーバーエラー用）を参照してください。

## セッションビルドアップ

すべての保護されたトランザクションについて、NetScalerは最初のトランザクションに対してSSLオフロード処理を実行し、**セッション再利用**の設定に基づいてSSLセッションを保存します。

トラフィックレートによっては、セッションの蓄積が一定期間にわたって発生し、NetScalerでこれらのセッションによって大量のメモリが占有される可能性があります。

セッション蓄積イベントは管理者にアラートを送信し、このイベントを解決するための推奨アクションを提供します。問題の詳細を表示するには、**セッションビルドアップ**タブをクリックします。

**詳細**の下で、以下を表示できます。

- セッション蓄積の異常が発生した時刻
- 仮想サーバー名
- 高、低、中などの異常の重大度
- 仮想サーバーで利用可能なSSLセッションが**X**個あり、現在、設定されたタイムアウトセッション内で1秒あたり**Y**個のSSLハンドシェイクがあることを示すメッセージ。

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

この異常を修正するための**推奨アクション**は、セッションタイムアウトを短縮するか、セッション再利用を無効にすることです。詳細については、セッションタイムアウトを参照してください。

## 低セッション再利用

NetScalerインスタンスは、サーバーからSSLハンドシェイクプロセスをオフロードすることで、SSLトランザクションを処理します。サーバーから応答を受信すると、NetScalerインスタンスはクライアントとの安全なトランザクションを完了します。キャッシュされたセッションパラメータを使用して、NetScalerインスタンスは連続するリクエストのSSLハンドシェイクプロセスを完了します。

これらのセッションが再利用されない場合、NetScalerインスタンスにとってオーバーヘッドとなります。**低セッション再利用**インジケータを使用すると、実際に再利用されているセッション数が少ないかどうかを特定できます。

問題の詳細を表示するには、**低セッション再利用**タブをクリックします。

問題をトラブルシューティングするための**推奨されるアクション**は、セッションの再利用を無効にするか、セッションタイムアウトを短縮することです。詳細については、「セッション再利用」を参照してください。

**詳細**では、以下を表示できます。

- 低セッション再利用があるアプリケーションの総数
- 低セッション再利用の異常が発生した時刻
- 総発生回数
- 高、低、中などの異常の重大度
- 設定されたセッションの%のみが再利用されていることを示す検出メッセージ

## サージキューの蓄積

サーバーがリクエストの急増を受け取ると、クライアントへの応答が遅くなります。多くの場合、過負荷によりクライアントはエラーページを受け取ります。仮想サーバーは、受信するリクエストを処理するために十分なバックエンドサーバーが構成されている必要があります。

**サージキューの蓄積**インジケーターを使用して、サージキューの蓄積がある仮想サーバーを表示できます。**サージキューの蓄積**タブをクリックして、問題の詳細を表示します。

サージキュー(/en-us/netscaler-application-delivery-management-software/media/iaa-surgequeue.png)

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

この問題をトラブルシューティングするための**推奨されるアクション**は次のとおりです。

- クライアント接続数の制限を増やします。詳細については、「クライアント接続数の制限を設定する」を参照してください。
- アプリケーションリクエストを処理するためにバックエンドサーバーを増やします

**詳細**では、以下を表示できます。

- サージキューの蓄積異常が発生した時間
- 合計発生回数
- 高、低、中などの異常の重大度
- 仮想サーバーでのサージキューの蓄積を示す検出メッセージ

## 異常に大きいHTTPパケット

HTTPトランザクションは、クライアントとサーバー間で要求/応答メッセージを使用します。要求および応答メッセージでは、HTTPヘッダーはHTTPプロトコルに表示される値です。4xxエラーを回避するために、仮想サーバー、サービス、またはサービスグループでHTTPヘッダーの長さを構成できます。

HTTP要求/応答が最大ヘッダー長を超えると、攻撃の可能性があります。**異常に大きいHTTPパケット**インジケーターを使用すると、HTTPヘッダーサイズが構成された値を超えているHTTPメッセージの発生を表示できます。

問題の詳細を表示するには、**異常に大きいHTTPパケット**タブをクリックします。

異常に大きいHTTPパケット(/en-us/netscaler-application-delivery-management-software/media/iaa-unusually.png)

問題をトラブルシューティングするための**推奨されるアクション**は次のとおりです。

- トラフィックをレビューして、ヘッダーサイズが正規のものであるかどうかを判断します。ヘッダーサイズが正規のものである場合は、HTTPプロファイルでヘッダー値を更新します。詳細については、「バッファオーバーフローチェック」を参照してください。
- ヘッダーサイズが正規のものでない場合は、攻撃を回避するためにソースをブロックリストに登録します。

**詳細**では、以下を表示できます。

- 異常が発生した時刻
- 合計発生回数

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

- 高、低、中などの異常の重大度
- 仮想サーバー、サーバー、またはサービスグループで構成されている現在のHTTPヘッダー長を示す検出メッセージ

## 不適切なパーシステンスタイプ

仮想サーバーによって表されるサーバー上の接続の状態を維持したい場合（たとえば、eコマースで使用される接続など）、仮想サーバーでパーシステンスを構成する必要があります。アプライアンスは、最初のサーバー選択に構成された負荷分散方法を使用しますが、その後のすべてのリクエストを同じクライアントから同じサーバーに転送します。

既存のセッションが後続のリクエストを処理するために再利用される場合、パーシステンスは効果的です。パーシステンスセッションの再利用率が低い場合、NetScalerで作成されたセッションは単なるオーバーヘッドになります。

**不適切なパーシステンスタイプ**インジケーターを使用して、仮想サーバーでのパーシステンスの使用率が低いかどうかを判断できます。問題の詳細を表示するには、**不適切なパーシステンスタイプ**タブをクリックします。

不適切なパーシステンスタイプ(/en-us/netscaler-application-delivery-management-software/media/iaa-improper-persistence.png)

問題をトラブルシューティングするための**推奨されるアクション**は、パーシステンスタイプを確認するか、パーシステンスを無効にすることです。詳細については、「パーシステンス設定」を参照してください。

**詳細**では、以下を表示できます。

- 異常が発生した時刻
- 合計発生回数
- 高、低、中などの異常の重大度
- 未使用のセッションの割合を示す検出メッセージ

## TCP再構成キュー制限ヒット

TCPは、TCP通信におけるOOOパケットを保持するために、順序不同キューを維持します。パケットがランタイムメモリに保持される必要があるため、キューサイズが長い場合、この設定はNetScalerのメモリに影響を与えます。

このキューサイズは、ネットワークとアプリケーションの特性に基づいて最適化されたレベルである必要があります。

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

**TCP再構成キュー制限ヒット**インジケータを使用すると、TCP接続上の順序不同パケットが、設定された順序不同パケットキューサイズを超えているかどうかを確認できます。

問題の詳細を表示するには、**TCP再構成キュー制限ヒット**タブをクリックします。

TCP再構成キュー制限ヒット(/en-us/netscaler-application-delivery-management-software/media/iaa-tcp-limit.png)

問題をトラブルシューティングするための**推奨されるアクション**は次のとおりです。

- トラフィックを確認し、攻撃である場合はソースをブロックリストに登録します。
- この動作が予期されるネットワーク動作である場合、TCPプロファイルで順序不同パケットサイズ値を更新します。詳細については、「TCP最適化」を参照してください。
- 一時的なネットワークの不具合である場合は、それ以上の対応は不要です。

**詳細**では、以下を表示できます。

- 異常が発生した時刻
- 合計発生回数
- 低、中、高などの異常の重大度
- 現在のTCPプロファイルとoooQsize設定を示す検出メッセージ

## SSLリアルタイムトラフィック

NetScalerインスタンスでは、SSLトラフィックの処理にSSLプロファイルを使用できます。SSLプロファイルは、仮想サーバー、サービス、およびサービスグループの特定のSSLパラメータで構成されています。**SSLリアルタイムトラフィック**インジケーターは、SSLトラフィックを分析してリアルタイムトラフィックを特定し、レイテンシを改善するための最適な構成設定を提案します。

**SSLリアルタイムトラフィック**タブをクリックして、問題の詳細を表示します。

SSLリアルタイムトラフィック(/en-us/netscaler-application-delivery-management-software/media/iaa-ssl-traffic.png)

問題をトラブルシューティングするための**推奨されるアクション**は、SSLパラメータを更新してネットワークレイテンシを改善することです。詳細については、「グローバルSSLパラメータ」を参照してください。

**詳細**の下で、以下を表示できます。

- 異常が発生した時間

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

- サービス/サービスグループ名
- 低、中、高などの異常の重大度
- アプリケーションの現在の設定を含む検出メッセージ

# アプリダッシュボードのトラブルシューティング

アプリダッシュボードにアプリケーションを追加すると、ダッシュボードにはアプリの基本的な構成の詳細がすぐに表示されます。アプリスコア、主要メトリック、問題などのアプリケーション分析の詳細は、数分（約10〜15分）以内に表示され始めます。詳細については、「アプリケーション」を参照してください。

NetScalerインスタンスからのメトリックデータフロー（AppFlowコレクターまたは分析プロファイル）に問題がないことを確認する必要があります。AppFlowコレクターと分析プロファイルに関する詳細情報は、このドキュメントで確認できます。

このドキュメントでは、次の場合に実行する必要があるトラブルシューティング手順について説明します。

- アプリケーションをクリックしても、指定された期間（10〜15分）が経過しても、選択したアプリケーションの分析に必要なデータが表示されない。
- アプリダッシュボードで、CSまたはLBアプリケーションが常に灰色（**該当なし**ステータス）で表示される。

**注**

このドキュメントに記載されているトラブルシューティング手順は、**コンテンツスイッチング**および**負荷分散**仮想サーバーにのみ適用されます。

## トラブルシューティングのシナリオ

## アプリケーションはライセンスされています

アプリケーションがライセンスされていることを確認する必要があります。**14.1-21.x**ビルド以降、すべての仮想サーバーは自動的にライセンスされます。以前のビルドを使用している場合は、**設定 > ライセンスと分析の構成**に移動し、**仮想サーバーライセンスの概要**でアプリケーションがライセンスされていることを確認してください。アプリケーションがライセンスされていない場合は、ライセンスを管理し、仮想サーバーで分析を有効にする。

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

# メトリックコレクターが有効になっています

**注:**

**14.1-21.x以降のビルド**では、NetScaler Consoleに追加された新しいNetScalerインスタンスでは、メトリックコレクターはデフォルトで無効になっています。既存の管理対象インスタンスのメトリックコレクター構成は変更されません。

NetScalerインスタンスで**メトリクスコレクター**が有効になっていることを確認する必要があります。メトリクスコレクターが有効になっていることを確認するには：

1. **インフラストラクチャ > インスタンス**に移動します。インスタンスの下で、インスタンスのタイプ（例：NetScaler VPX）を選択します。
2. NetScalerインスタンスを選択します。
   a. **アクションの選択**リストから、**メトリクスコレクター**を選択します。



3. **メトリクスコレクター設定の構成**ページで、**有効にする**オプションが選択されていることを確認します。選択されていない場合は、**有効にする**オプションを選択し、**OK**をクリックします。

メトリクスコレクターを有効にした後もデータが表示されない場合は、以下を検証してください。

- NetScalerインスタンスバージョン13.0の**47.xビルドより前の**AppFlowコレクター。
- NetScalerインスタンスビルド**47.x以降**のアナリティクスプロファイル。

### NetScaler®インスタンスの以前のビルド

NetScalerの場合:

1. コレクターがポート5563で**UP**して実行されていることを確認するために、次のコマンドを実行します。

   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```



2. コレクターが利用できない場合は、NetScaler Consoleでインスタンスの手動ポーリングを実行します。
   a. 「**インフラストラクチャ > ネットワーク機能 > 今すぐポーリング**」に移動します。

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

b. インスタンスを選択し、「**Start Polling**」をクリックします。

ポーリング(/en-us/netscaler-application-delivery-management-software/media/polling.png)

ポーリングが失敗した場合は、NetScaler ConsoleからNetScalerインスタンスを削除し、再度NetScalerインスタンスを追加します。NetScalerインスタンスを追加すると、コレクターがNetScalerに追加されます。

コレクターが「**Down**」ステータスを示す場合：

1. SNIPが構成されていることを確認します。

   SNIP(/en-us/netscaler-application-delivery-management-software/media/snip.png)

   SNIPが構成されていない場合は、SNIPを構成する必要があります。詳細については、「SNIPの構成」を参照してください。
2. NetScalerインスタンスがNetScaler Consoleに到達可能であることを確認します。

   pingテストを実行して検証できます。`ping -S <SNIP> <adm_receiver_ip>`を実行します。

   pingテスト(/en-us/netscaler-application-delivery-management-software/media/ping.png)

### NetScalerインスタンスの後のビルド

NetScaler Consoleで、メトリックコレクターサービスが利用可能であることを確認します。

1. 「**インフラストラクチャ > ネットワーク機能 > 負荷分散 > サービス**」に移動します。
2. 検索バーで、「**Instance: (IP address)**」と「**Name: NetScaler Console**」でフィルタリングします。
3. `adm_metric_collector_svc_<adm_receiver ip>` が利用可能であることを確認します。IPアドレスは、NetScaler Consoleの管理IPまたはエージェントIPのいずれかです。

   このサービスが**UP**ステータスであり、ポート5563で実行されていることを確認します。

   ☐

データがまだ表示されない場合は、NetScalerでコレクターサービスが時系列分析プロファイルにバインドされていることを確認してください。

1. NetScalerにログオンします
2. 次のコマンドを実行します。

   ```
   sh analytics profile ns_analytics_time_series_profile
   ```

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



コレクターが**Down**ステータスを示す場合：

1. SNIPが構成されていることを確認します。

   

   SNIPが構成されていない場合は、SNIPを構成する必要があります。詳細については、SNIPの構成を参照してください。

2. NetScalerインスタンスがNetScaler Consoleに到達可能であることを確認します。

   pingテストを実行して検証できます。`ping -S <SNIP> <adm_receiver_ip>`を実行します。

   

3. telnet を介したトラフィック接続がサービスに接続できることを確認します。

   

   telnet がサービスに接続できる場合、ファイアウォールが存在し、メトリックデータフローをブロックしています。ファイアウォールのブロックの問題を解決する必要があります。

NetScaler の時系列分析プロファイルにコレクターサービスがバインドされていない場合、コレクターは空白で表示されます。



NetScaler Console でインスタンスの手動ポーリングを実行する必要があります。

1. **インフラストラクチャ > ネットワーク機能 > 今すぐポーリング** に移動します。
2. インスタンスを選択し、**Start Polling** をクリックします。

   

   ポーリングが失敗した場合は、次のコマンドを使用して NetScaler インスタンスにコレクターサービスを直接追加します。

   ```
   add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
   ```

   ```
   unset analyticsprofile ns_analytics_time_series_profile -collectors
   ```

   ```
   set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled
   ```

   分析時系列プロファイルが更新されます。

   

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

記載されているすべてのトラブルシューティング手順を実行した後でも問題が依然として解決しない場合は、**NetScalerサポート**にお問い合わせください。

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

# アプリケーションの使用状況と異常

管理者として、アプリケーションがどのように利用されているかを確認する必要があります。アプリケーションの主要メトリックは、アプリケーションの使用状況を特定するのに役立ちます。アプリケーションへのトラフィック範囲は予測できないため、特定の期間に異常なアプリケーションパフォーマンスの逸脱が発生する可能性があります。そのようなシナリオでは、管理者として、そのような突然の異常を表示および分析し、即座のトラブルシューティングが必要かどうかを確認したいと思うかもしれません。

NetScaler Consoleは、そのような異常を検出し、必要な詳細を提供します。**アプリケーション > ダッシュボード**に移動し、アプリケーションをクリックして、**主要メトリック**タブを選択します。NetScaler Consoleはトラフィックパターンを監視し、主要メトリックが期待される範囲内にあるかどうかを分析します。期待される範囲から逸脱がある場合、NetScaler Consoleはそれらの逸脱を異常として報告します。

以下の主要メトリックの異常を表示できます。

- 応答時間
- スループット
- データ量
- 1秒あたりのリクエスト数

  異常のあるメトリック(/en-us/netscaler-application-delivery-management-software/media/anomaly-metrics.png)

詳細を表示するには、**異常のあるメトリック**タブをクリックします。

異常のあるメトリック(/en-us/netscaler-application-delivery-management-software/media/anomaly-metrics1.png)

各メトリックで、**詳細を表示**オプションをクリックして詳細を表示することもできます。次の例は、アプリケーションのデータ量に関するものです。

詳細を表示(/en-us/netscaler-application-delivery-management-software/media/see-more-data-volume.png)

以下を表示できます。

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

- 最大値、合計値、期待される範囲、および異常を示すグラフ
- 問題のトラブルシューティングを行うための**推奨されるアクション**
- **詳細**の下にある時間と異常の詳細

# ピーク時と閑散時の使用状況分析

Webアプリケーションは、トラフィックが多い場合と少ない場合があり、日ごとまたは時間ごとのトラフィック範囲は確かに予測できません。同様に、Webアプリケーションは、スケジュールされたメンテナンスやアップグレード中に特定の期間のダウンタイムも必要とします。管理者として、トラフィックを分析し、適切な時間を見つける必要があります。

- Webアプリケーションをスケールアップする
- Webアプリケーションのダウンタイムを計画する

NetScaler Consoleのピーク使用量と閑散期分析機能を使用すると、選択した期間の主要なメトリックを分析できます。これらのメトリックから、トラフィックを分析し、Webアプリケーションをスケールアップする時期やスケジュールされたダウンタイムを計画する時期を決定できます。

## アプリケーションのスケール制限を評価する

**App Dashboard**からアプリケーションをクリックし、**Key Metrics**タブを選択して、すべてのメトリックの統合ビューを視覚化します。リストから期間を選択して、メトリックを分析します。

各メトリックについて、以下を表示できます。

- **最大** – 選択した期間の最大値を示します
- **平均** – 選択した期間の平均値を示します

画像の例によると、応答時間の最大値は1.3秒を示しています。グラフチャートから、選択した期間に高い応答時間が何回発生したかを分析できます。同様に、他のメトリックの詳細を表示したり、アプリケーションがピーク使用量に達したかどうかを分析したり、本番環境をスケールアップする決定を下したりすることもできます。

## アプリケーションのメンテナンスウィンドウ上位5つを特定する

**App Dashboard**からアプリケーションをクリックし、**Key Metrics**タブを選択して、アプリケーションの閑散期を表示します。アプリケーションの一般的なダウンタイムは、要件に応じて1時間、2時間、または4時間です。ダウンタイムを計画したい時間をリスト（1時間、2時間、または4時間）から選択できます。リストから時間を選択した後、合計リクエスト数、スループット、データ量などのメトリックのトラフィックを分析できます。アプリケーションの使用量が少ないとき

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

に、ダウンタイムをスケジュールする適切な時間を選択できます。 次の例は、1時間のダウンタイムを分析するものです。



ヒートマップビューは、選択した期間のアプリケーションの使用状況を示します。色が濃いほど（青色）、アプリケーションの使用状況が高いことを示します。

ヒートマップビューは、アプリケーションのダウンタイムを計画するための上位5つの最も少ない期間（1、2、3、4、5）も示唆しています。

**1** – 水曜日の午後4時から午後5時までの最初の提案を示します。

**2** – 木曜日の午後9時から午後10時までの2番目の提案を示します。

**3** – 日曜日の午前7時から午後8時までの3番目の提案を示します。

**4** – 水曜日の午後12時から午後1時までの4番目の提案を示します。

**5** – 月曜日の午前7時から午後8時までの5番目の提案を示します。

他のすべての日のトラフィックを分析した後、ダウンタイムをスケジュールするために、他の任意の日時を選択することもできます。

さらに詳細な情報を表示するには、**詳細を表示**をクリックします。上位5つの最も少ない期間および他の日の詳細を表示するには、**合計リクエスト数**、**スループット**、または**データ量**タブをクリックします。



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

# アプリケーション使用状況分析

アプリケーション所有者は、パフォーマンスと使用状況の観点から、アプリケーション全体を評価し、視覚化できる必要があります。

改善された**App Dashboard**を使用すると、すべてのアプリケーションのパフォーマンスと使用状況のメトリックをまとめて表示できます。アプリケーションをクリックすると、既存のアプリケーションパフォーマンスメトリックに加えて、**Web Insight**タブに次のメトリックの詳細が表示されます。

- アプリケーションの使用状況を把握する。
- パフォーマンスの偏差を使用状況メトリックと関連付ける。

**注**

- リリース14.1ビルド51.x以降、Web Insight分析は、IPv6アドレスで構成された仮想サーバーで表示されます。
- **14.1-4.x**リリース以降、メトリックをドリルダウンすると、時系列グラフの分析ビューには、選択した期間のnil値（たとえば、0ミリ秒と0リクエスト）が表示されます。以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、分析ビューはこれらのnil値をスキップしてグラフを表示していました。
- 各メトリックについて、最大値と合計値を示すオプションを表示できます。例：
  - - 選択した期間のクライアントネットワーク遅延の最大値。クライアント1のネットワーク遅延が644ミリ秒、クライアント2が15ミリ秒、クライアント3が3ミリ秒であるとします。このシナリオでは、**クライアントネットワーク遅延**は644ミリ秒と表示されます。
  - - 選択した期間に利用可能なすべてのクライアント/サーバーで消費された合計帯域幅。クライアント1の帯域幅消費量が79.54 MB、クライアント2が45 MB、クライアント3が40 MBであるとします。このシナリオでは、帯域幅は（79.54 MB + 45 MB + 40 MB）= 164.54 MBと表示されます。

**使用状況**タブから表示できるWeb Insightメトリックは次のとおりです。

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

- **クライアント** – アプリケーションにアクセスしているクライアントのインサイトを表示します。

  - **合計クライアント** – アプリケーションにアクセスしているクライアントの総数を表示します。**リクエスト**タブをクリックして表示します。

    - **クライアント** – クライアントIPアドレス。
    - **クライアントネットワーク遅延 (平均)** – クライアントからの平均ネットワーク遅延。
    - **クライアントネットワーク遅延 (最大)** – クライアントからの最大ネットワーク遅延。
    - **リクエスト** – クライアントからの合計リクエスト。
    - **リクエストによるパーセンテージ分布** – リクエストに基づくパーセンテージ分布。たとえば、クライアントの合計が4で、各クライアントが100リクエストを持っている場合、各クライアントのパーセンテージ分布は25%です。

  - **クライアントネットワーク遅延** – クライアントからNetScalerへのネットワーク遅延を表示します。**クライアントネットワーク遅延**タブをクリックして表示します。

    - **クライアント** – クライアントIPアドレス。
    - **クライアントネットワーク遅延 (平均)** – クライアントからの平均ネットワーク遅延。
    - **クライアントネットワーク遅延 (最大)** – クライアントからの最大ネットワーク遅延。
    - **リクエスト** – クライアントからの合計リクエスト。
    - **リクエストによるパーセンテージ分布** – リクエストに基づくパーセンテージ分布。

  - **レンダリング時間** – サーバー応答のレンダリングにかかった時間を表示します。**レンダリング時間**タブをクリックして表示します。

    - **クライアント** – クライアントIPアドレス。
    - **レンダリング時間 (平均)** – クライアントからの平均レンダリング時間。
    - **リクエスト** – クライアントからの合計リクエスト。
    - **リクエストによるパーセンテージ分布** – リクエストに基づくパーセンテージ分布。

- **サーバー** – アプリケーションにアクセスしているサーバーのインサイトを表示します。

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

**注**

統合キャッシュリクエストの場合、IC通知とともにNetScaler仮想サーバーのIPアドレスを表示できます。詳細については、統合キャッシュリクエストを参照してください。

- **合計サーバー** – アプリケーションにアクセスしているサーバーの合計数を表示します。**リクエスト**タブをクリックして表示します。
  - **サーバー** – サーバーのIPアドレス。
  - **サーバーネットワーク遅延 (平均)** – サーバーからの平均ネットワーク遅延。
  - **サーバーネットワーク遅延 (最大)** – サーバーからの最大ネットワーク遅延。
  - **リクエスト** – サーバーからの合計リクエスト数。
  - **リクエストによる割合分布** – リクエストに基づいた割合分布。たとえば、合計サーバー数が10で、各サーバーが1000リクエストを持っている場合、各サーバーの割合分布は10%です。
- **サーバーネットワーク遅延 (最大)** – サーバーからNetScalerへの最大ネットワーク遅延を表示します。**サーバーネットワーク遅延**タブをクリックして表示します。
  - **サーバー** – サーバーのIPアドレス。
  - **サーバーネットワーク遅延 (平均)** – サーバーからの平均ネットワーク遅延。
  - **サーバーネットワーク遅延 (最大)** – サーバーからの最大ネットワーク遅延。
  - **リクエスト** – サーバーからの合計リクエスト数。
  - **リクエストによる割合分布** – 合計リクエストに基づいた割合分布。
- **Server Response Time** – サーバーがリクエストに応答するのにかかった時間を表示します。**Server Response Time**タブをクリックして表示します。
  - **Server** – サーバーのIPアドレス。
  - **Server Response Time (avg)** – サーバーからの平均応答時間。
  - **Server Response Time (max)** – サーバーからの最大応答時間。
  - **Requests** – サーバーからの合計リクエスト数。
  - **Percentage distribution by requests** – 合計リクエスト数に基づくパーセンテージ分布。

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

- **Bandwidth** – サーバーによって消費された合計帯域幅を表示します。**Bandwidth**タブをクリックして表示します。
  - **Server** – サーバーのIPアドレス。
  - **Bandwidth** – サーバーから消費された合計帯域幅。
  - **Requests** – サーバーからの合計リクエスト数。
  - **Percentage distribution by requests** – 合計リクエスト数に基づくパーセンテージ分布。

- **Geo Locations** – 特定の場所からアプリケーションにアクセスしているクライアントのインサイトを表示します。

  地理的位置(/en-us/netscaler-application-delivery-management-software/media/wi-geo-locations.png)

  - **Total locations** – アプリケーションにアクセスしているクライアントの合計ロケーションを表示します。
  - **Response Time** – クライアントロケーションからの応答時間を表示します。
  - **帯域幅** – すべての場所のクライアントによって消費された合計帯域幅を表示します。
  - **リクエスト** – すべてのクライアントの場所からの合計リクエストを表示します。

    各タブをクリックして表示します。
    - **場所** – 場所の名前。
    - **応答時間** – クライアントの場所からの平均応答時間。
    - **帯域幅** – クライアントの場所から消費された帯域幅。
    - **リクエスト** – クライアントの場所からの合計リクエスト。
    - **リクエストによるパーセンテージ分布** – 合計リクエスト数に基づくパーセンテージ分布。たとえば、合計場所数が10、合計リクエスト数が100万で、国Aだけで90万のリクエストを受け取った場合、国Aのパーセンテージ分布は90%になります。その他の国は、各国で受け取ったリクエスト数に基づいて残りのパーセンテージ分布を受け取ります。

- **URL** – ロード時間とレンダリング時間が長いURLのインサイトを表示します。

  - **合計URL** – 合計URLを表示します。**リクエスト**タブをクリックして表示します。
    - **URL** – URL名。

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

- **ロード時間 (平均)** – URLのロードにかかる平均時間。
- **リクエスト** – そのURLからの合計リクエスト。
- **リクエストによるパーセンテージ分布** – 合計リクエスト数と各URLにおけるパーセンテージ分布。

- **ロード時間** – URLのロードにかかった時間を表示します。「**ロード時間**」タブをクリックして表示します。
  - **URL** – URL名。
  - **ロード時間 (平均)** – URLのロードにかかった平均時間。
  - **リクエスト** – URLからの合計リクエスト数。
  - **リクエストごとの割合** – 合計リクエスト数に基づく割合。
- **レンダリング時間** – URLがレンダリングされて表示されるまでにかかった時間を表示します。「**レンダリング時間**」タブをクリックして表示します。
  - **URL** – URL名。
  - **レンダリング時間 (平均)** – URLのレンダリングにかかった平均時間。
  - **リクエスト** – URLからの合計リクエスト数。
  - **リクエストごとの割合** – 合計リクエスト数に基づく割合。

- **HTTP応答ステータス** – 特定の完了したHTTPリクエストに関するインサイトを表示します。

  - **応答ステータス** – 2xx、4xx、5xxなどの応答コードを表示します。
  - **応答ステータスの理由** – 内部サーバーエラー、見つかりませんなどの応答理由を表示します。
  - **発生回数** – 合計発生回数を表示します。
- **オペレーティングシステム** – アプリケーションにアクセスしているOSのインサイトを表示します。

  - **リクエスト** – 各オペレーティングシステムからの合計リクエストを表示します。
  - **帯域幅** – 各オペレーティングシステムによって消費された合計帯域幅を表示します。
  - **ロード時間** – 各オペレーティングシステムがサーバーからロードするのにかかった合計時間を表示します。

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

- **ブラウザ** – クライアントがアプリケーションにアクセスするために使用したブラウザタイプのインサイトを表示します。

  

  - **リクエスト** – 各ブラウザからの合計リクエストを表示します。
  - **帯域幅** – 各ブラウザによって消費された合計帯域幅を表示します。
  - **ロード時間** – ブラウザがサーバーからロードするのにかかった合計時間を表示します。

- **SSLエラー** – フロントエンドサーバーとバックエンドサーバーからのSSLエラーのインサイトを表示します。

  

  - **合計エラー** – SSLエラーの合計発生回数を表示します。
  - **フロントエンド** – フロントエンドサーバーからの合計SSLエラーを表示します。**フロントエンド**タブをクリックして、SSLエラーの種類と合計発生回数を表示します。
  - **バックエンド** – バックエンドサーバーからの合計SSLエラーを表示します。**バックエンド**タブをクリックして、SSLエラーの種類と合計発生回数を表示します。

- **SSL使用状況** – SSL証明書、プロトコル、暗号、鍵強度などのSSL使用状況に関するインサイトを表示します。

  

  - **証明書** – 合計SSL証明書を表示します。**証明書**タブをクリックすると、証明書名と合計ヒット数が表示されます。
  - **プロトコル** – 合計SSLプロトコルを表示します。**プロトコル**タブをクリックすると、SSL/TSLプロトコルと合計ヒット数の詳細が表示されます。
  - **暗号** – 合計暗号を表示します。**暗号**タブをクリックすると、各暗号スイート名と合計ヒット数の詳細が表示されます。
  - **鍵強度** – SSL証明書で使用されている合計鍵強度を表示します。**鍵強度**タブをクリックすると、各鍵強度と合計ヒット数の詳細が表示されます。

## メトリックの詳細をグラフィカル形式で表示

各メトリックについて、**詳細を表示**オプションをクリックすると、グラフィカル形式で詳細を表示できます。**>**をクリックすると、グラフィカル形式で詳細が表示されます。



**詳細を表示**オプションをクリックすると、各メトリックについて以下の詳細を表示できます。

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

| インサイト名 | メトリック | 説明 |
| --- | --- | --- |
| **クライアント** | クライアント | クライアントリストを示します。 |
| | レンダリング時間 (平均) | クライアントがサーバー応答をレンダリングするのにかかった平均時間を示します。 |
| | クライアントネットワーク遅延 (平均) | クライアントからNetScalerインスタンスへの平均ネットワーク遅延を示します。 |
| | リクエスト | クライアントからの合計リクエスト数を示します。 |
| **サーバー** | サーバー | サーバーリストを示します。 |
| | サーバー処理時間 (平均) | サーバーがリクエストを処理するのにかかった平均時間を示します。 |
| | サーバーネットワーク遅延 (平均) | サーバーからNetScalerインスタンスへの平均ネットワーク遅延を示します。 |
| | ヒット数 | サーバーが受信した合計ヒット数を示します。 |
| **地理的位置** | 位置 | クライアントの位置を示します。 |
| | 応答時間 | クライアントの位置からの合計応答時間を示します。 |
| | 帯域幅 | その場所から消費された合計帯域幅を示します。 |
| | リクエスト | その場所からの合計リクエスト数を示します。 |

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

| インサイト名 | メトリック | 説明 |
| --- | --- | --- |
| **URL** | レンダリング時間 (平均) | サーバーからページをロードするのにかかった平均時間を示します。 |
| | ロード時間 (平均) | URLがレンダリングされて表示されるまでにかかった平均時間を示します。 |
| | ヒット数 | URLからの合計ヒット数を示します |
| **HTTP応答ステータス** | 名前 | OK、Not found、Internal Server Errorなどの応答ステータス名を示します |
| | 応答ステータス | 200、400、500などのサーバーから受信した応答ステータスコードを示します |
| | ヒット数 | 応答コードからの合計ヒット数を示します |
| | 帯域幅 | 消費された合計帯域幅を示します |
| **オペレーティングシステム** | オペレーティングシステム | Windows、MACなどのオペレーティングシステム名を示します |
| | ロード時間 | オペレーティングシステムがサーバーからロードされるまでにかかった合計時間を示します |
| | 帯域幅 | オペレーティングシステムによって消費された合計帯域幅を示します |
| | リクエスト | オペレーティングシステムからの合計リクエスト数を示します |

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

| インサイト名 | メトリック | 説明 |
| --- | --- | --- |
| **ブラウザ** | ブラウザ | Mozilla Firefox、Chromeなどのブラウザ名を示します |
| | ロード時間 | ブラウザがサーバーからロードされるまでにかかった合計時間を示します |
| | 帯域幅 | ブラウザによって消費された合計帯域幅を示します |
| | リクエスト | ブラウザからの合計リクエスト数を示します |
| **SSLエラー** | SSL障害タイプ | CLIENTAUTH FAILUREなどのエラー名を示します。 |
| | 発生回数 | SSLエラーの総発生回数を示します。 |
| **SSL使用状況** | SSL使用状況 | TLS、SSLなどのプロトコル名とバージョンを示します。 |
| | ヒット数 | プロトコルからの総ヒット数を示します。 |

## Web Insightの問題をトラブルシューティングする

詳細については、トラブルシューティングドキュメント「Web Insightの問題をトラブルシューティングする」を参照してください。

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

# A+ SSL評価分析

**注：**

準拠していないSSL証明書の一括アップグレードには、**タスクのSSL A+評価アップグレード**を使用できます。

アプリケーションは、SSLトランザクションに安全な暗号とプロトコルを使用する必要があります。そうしないと、アプリケーションにアクセスするユーザーのプライバシー、データの整合性、およびセキュリティに影響を与える可能性があります。NetScaler Consoleは、NetScalerのセキュアなフロントエンドプロファイルを使用して、アプリケーションの仮想サーバーSSL設定をレビューします。A+評価に必要な設定は、セキュアなフロントエンドプロファイルにプリロードされています。

アプリケーション所有者は、自分のアプリケーションが**A+**評価であるかどうかを評価できます。また、アプリケーションのプロトコルと暗号スイートのスコアを表示することもできます。アプリケーションが**A+**評価でない場合は、**A+**評価にアップグレードできます。

アプリケーションのSSL評価を表示するには、次の手順を実行します。

1. **アプリケーション > ダッシュボード**に移動します。
2. SSL評価に基づいてアプリケーションをフィルタリングします。

   評価がないアプリケーションは、**NA**に分類されます。
3. GUIから必要なアプリケーショングリッドを選択します。
4. **SSL**タブを選択します。このタブには、アプリケーションのSSL評価が表示されます。

**SSL**タブには、アプリケーションの評価を変更またはアップグレードするための次のいずれかのオプションが用意されています。

- A+ SSL評価にアップグレード
- 「SSLレーティングをロールバック」(#roll-back-ssl-rating)

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

# A+ SSLレーティングにアップグレード

アプリケーションをA+ SSLレーティングにアップグレードすると、NetScalerインスタンス上のデフォルトSSLプロファイルのステータスに応じて、以下の変更が発生します。

- デフォルトのSSLプロファイルが無効になっている場合、NetScaler ConsoleはSSL仮想サーバー上の推奨SSL設定に変更します。
- デフォルトのSSLプロファイルが有効になっている場合、NetScaler Consoleはセキュアプロファイルに基づいて、推奨されるA+設定を持つ新しいSSLプロファイルを作成します。

「**A+**」レーティングのないアプリケーションは、「**SSL**」タブに影響を受ける仮想サーバーの詳細を表示します。

「A+ではない」(/en-us/netscaler-application-delivery-management-software/media/ssl-rating-not-a-plus.png)

「**App Details**」では、セキュアなフロントエンドプロファイルに準拠していない仮想サーバーの詳細を確認できます。また、「**Recommendation**」列には修復策が表示されます。これらの対策は、アプリケーションをセキュアなフロントエンドプロファイルに準拠させるために提供されます。

この例では、仮想サーバーにいくつかのセキュリティ問題があります。「**Protocol TLSv1.0 enabled**」もその1つです。「**App Details**」セクションでは、この問題を解決するための適切なアクションが推奨されています。それぞれの推奨事項に従って、これらの問題をすべて解決するには、次の手順を実行します。

1. 「**A+レーティングにアップグレード**」をクリックします。

   「A+アップグレードの確認」(/en-us/netscaler-application-delivery-management-software/media/ssl-rating-upgrade-to-a-plus.png)

   確認メッセージには、仮想サーバーで実行されるコマンドが表示されます。これらのコマンドは、アプリケーションのトラフィックに影響を与える可能性があります。
2. コマンドを確認し、「**Confirm**」をクリックします。

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

# SSLレーティングをロールバック

「

**注:**

」:

アプリケーションをA+ SSL評価にアップグレードした場合、アップグレード後7日以内であれば元の評価に戻すことができます。

アプリケーションをA+評価にアップグレードした後、SSL insightで受信トラフィックを分析できます。このページには、SSLトランザクションがネゴシエートされる暗号とプロトコルが表示されます。

ただし、正当なトラフィックの一部がドロップされていることに気付いた場合は、アプリケーションに構成されているセキュアなフロントエンドプロファイルをロールバックできます。この操作により、SSL評価が以前の評価に戻ります。

SSL評価をロールバックするには：

1. **ロールバック**をクリックします。

   確認メッセージには、仮想サーバーで実行されるコマンドが表示されます。
2. コマンドを確認し、**確認**をクリックします。

# アプリケーショントラフィックに対するSSL評価の影響を判断する

SSL評価をアップグレードすると、アプリケーションのトラフィックに影響が出る可能性があります。**SSLメトリクス**で、アップグレード後に接続が切断されたかどうかを確認できます。この情報に基づいて、SSL評価を継続するかロールバックするかを決定できます。

次のグラフの例では、SSL評価を**A+**にアップグレードした後、一部の接続が切断されています。

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

# Web Insight ダッシュボード

**注:**

リリース 14.1 ビルド 51.x 以降、IPv6 アドレスで構成された仮想サーバーに対して Web Insight 分析が表示されます。

改善された Web Insight 機能は拡張され、Web アプリケーション、クライアント、および NetScaler インスタンスの詳細なメトリックに対する可視性を提供します。この改善された Web Insight により、パフォーマンスと使用状況の両方の観点から、アプリケーション全体を評価および視覚化できます。管理者として、Web Insight を次の目的で表示できます。

- アプリケーション。**アプリケーション > ダッシュボード**に移動し、アプリケーションをクリックして、**Web Insight** タブを選択すると、詳細なメトリックが表示されます。詳細については、「アプリケーション使用状況分析」を参照してください。
- すべてのアプリケーション。**アプリケーション > Web Insight** に移動し、各タブ（アプリケーション、クライアント、インスタンス）をクリックして、次のメトリックを表示します。

| アプリケーション | クライアント | インスタンス |
|---|---|---|
| アプリケーション | クライアント | インスタンスメトリック |
| サーバー | 地理的位置 | アプリケーション |
| ドメイン | HTTPリクエストメソッド | ドメイン |
| 地域 | HTTP応答ステータス | URL |
| URL | URL | HTTPリクエストメソッド |
| HTTPリクエストメソッド | オペレーティングシステム | HTTP応答ステータス |
| HTTP応答ステータス | ブラウザ | クライアント |
| SSLエラー | SSLエラー | サーバー |
| SSL使用状況 | SSL使用状況 | オペレーティングシステム |

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

| アプリケーション | クライアント | インスタンス |
| --- | --- | --- |
| | | ブラウザ |

ウェブインサイト(/en-us/netscaler-application-delivery-management-software/media/web-insight-app.png)

各メトリックで、上位5つの結果を表示できます。クリックしてさらにドリルダウンし、問題を分析してトラブルシューティングアクションをより迅速に実行できます。

**注:**

- **14.1-4.x**リリース以降、メトリックをドリルダウンすると、時系列グラフの分析ビューには、選択した期間のnil値（たとえば、0ミリ秒と0リクエスト）が表示されます。以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、分析ビューはこれらのnil値をスキップしてグラフを表示していました。
- 一部のシナリオでは、NetScalerが一部のトランザクションのRTT値を計算できない場合があります。そのようなトランザクションの場合、NetScaler ConsoleはRTT値を次のように表示します。
  - **NA** – NetScalerインスタンスがRTTを計算できない場合に表示されます。
  - **< 1ms** – NetScalerインスタンスが0ミリ秒から1ミリ秒の間の小数でRTTを計算する場合に表示されます。たとえば、0.22ミリ秒。

たとえば、1ヶ月間のサーバーネットワーク遅延を分析し、本番環境をスケールアップまたはスケールダウンするかどうかを決定したいとします。これを分析するには、次の手順を実行します。

1. リストから「Last 1 Month」を選択し、**Applications**タブから**Servers**までスクロールして、サーバーをクリックします。

   アプリ ウェブインサイト(/en-us/netscaler-application-delivery-management-software/media/app-wi-server.png)

   選択したサーバーのメトリック詳細が表示されます。
2. レイテンシーを分析するには、**Server Network Latency** タブを選択します。

   サーバーネットワークレイテンシー(/en-us/netscaler-application-delivery-management-software/media/app-wi-serverlatency.png)

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

平均レイテンシーは10.01秒を示しており、グラフから、過去1か月のサーバーネットワークレイテンシーが高いことが分析できます。管理者として、本番環境をスケールアップする決定を下すことができます。

## 統合キャッシュリクエスト

統合キャッシュは、NetScalerアプライアンス上にインメモリストレージを提供し、オリジンサーバーへのラウンドトリップを必要とせずに、Webコンテンツをユーザーに提供します。

統合キャッシュリクエストは現在、NetScaler仮想サーバーのIPアドレスの横にIC通知とともに**Servers**の下に表示されます。その他のすべてのリクエストは、オリジンサーバーのIPアドレスとともに表示されます。

統合キャッシュ(/en-us/netscaler-application-delivery-management-software/media/web-insight-integrated-cache.png)

サーバーをドリルダウンして詳細を表示すると、**Server Metrics** に統合キャッシュのヒットとミスのタブが表示されます。

グラフビュー：

- **Integrated Cache Hits** タブでは、NetScalerアプライアンスがキャッシュから提供する合計応答数を表示できます。

  統合キャッシュヒット(/en-us/netscaler-application-delivery-management-software/media/web-insight-server-integrated-cache.png)
- **Integrated Cache Misses** タブでは、NetScalerアプライアンスがオリジンサーバーから提供する合計応答数を表示できます。

  統合キャッシュミス(/en-us/netscaler-application-delivery-management-software/media/web-insight-server-integrated-miss.png)

## Web Insight の問題のトラブルシューティング

詳細については、トラブルシューティングドキュメント「Web Insight の問題のトラブルシューティング」(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/web-insight-troubleshooting.html)を参照してください。

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

# アプリケーションの遅延の根本原因を表示する

アプリケーションの応答速度の低下は、ビジネスへの影響や生産性の低下につながるため、どの組織にとっても大きな懸念事項です。 > で、 という新しいメトリックを表示できるようになりました。このメトリックを使用すると、管理者として、アプリケーションの遅延が以下の原因から生じているかどうかを分析できます。

- クライアントネットワークの遅延
- サーバーネットワークの遅延
- サーバー処理時間

NetScaler Consoleは1時間ごとに異常チェックを実行し、特定の前提条件に基づいて過去1時間のトラフィックの異常を報告します。たとえば、誤検知を避けるため、応答時間が1ミリ秒未満の場合、その結果に対する異常チェックはスキップされます。

> ページでは、選択した期間の応答時間異常のあるアプリケーションを表示できます。 メトリックには、合計異常数に基づいて上位5つのアプリケーションが表示されます。すべてのアプリケーションを表示するには、 をクリックします。

アプリケーション応答時間の異常(/en-us/netscaler-application-delivery-management-software/media/app-anomalies.png)

- **アプリケーション** – アプリケーション名を示します。
- **合計異常と寄与要因** – アプリケーションからの合計異常を示します。マウスポインターを合わせると、クライアントネットワークの遅延、サーバーネットワークの遅延、およびサーバー処理時間からそれぞれ発生した合計異常を表示できます。
- **応答時間範囲** – アプリケーションからの予想される応答時間範囲を示します。
- **最大異常応答時間** – アプリケーションからの最高の応答時間を示します。
- **最大異常寄与要因** – アプリケーションの最大異常数が、クライアントネットワークの遅延、サーバーネットワークの遅延、またはサーバー処理時間のいずれに起因するかを示します。

## アプリケーションのドリルダウン

アプリケーションをクリックすると、選択した期間の**アプリケーションメトリック**の詳細が表示されます。

**アプリケーションメトリック**では、以下を表示できます。

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

- **概要** – 応答時間、リクエスト、帯域幅など、アプリケーションのパフォーマンスを視覚化するための概要。
- **リクエスト** – アプリケーションが受信した合計リクエスト。合計リクエスト数に基づいて、上位5つのクライアントからのリクエストも表示できます。
- **帯域幅** – アプリケーションによって処理された合計帯域幅。合計帯域幅消費量に基づいて、上位5つのサーバーからの帯域幅消費量も表示できます。
- **応答時間** – クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間を同じグラフで視覚化するための概要。
- **クライアントネットワーク遅延** – 平均クライアントネットワーク遅延 (クライアントからNetScalerまで)。
- **サーバーネットワーク遅延** – 平均サーバーネットワーク遅延 (NetScalerからサーバーまで)。
- **サーバー処理時間** – 平均サーバー処理時間 (サーバーからNetScalerまで)。

アプリケーションに異常がある場合、その異常がクライアントネットワーク遅延、サーバーネットワーク遅延、またはサーバー処理時間のいずれに起因するかを確認できます。各タブをクリックして詳細を表示します。

**クライアントネットワーク遅延**タブと**サーバーネットワーク遅延**タブでは、以下を表示できます。

- **検索バー** - 検索バーをクリックすると、すべてのクライアント (クライアントネットワーク遅延内) およびサーバー (サーバーネットワーク遅延内) のIPアドレスが表示されます。IPアドレスを選択して結果をフィルタリングできます。
- **エクスポートオプション** - **CSVをダウンロード**をクリックして、詳細をCSV形式でエクスポートします。

### 応答時間

「**異常の詳細**」の下で、応答時間の寄与要因（クライアントからサーバーまで）の詳細を表示するにはクリックします。次の例では、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間の異常があります。予想される範囲と、その範囲を超えて発生した違反も表示できます。

「**推奨されるアクション**」は、異常に対する考えられる解決策を提案します。

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

同様に、「**クライアントネットワーク遅延**」、「**サーバーネットワーク遅延**」、および「**サーバー処理時間**」タブをクリックして、以下を表示できます。

- 予想される範囲を超えた異常。
- 考えられる解決策を提案する推奨されるアクション。

アプリケーションが正常に動作している場合、アプリケーションメトリックを異常なしとして表示できます。



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

# サービスグラフ

NetScaler Consoleのサービスグラフ機能を使用すると、すべてのサービスをグラフィカルな表現で監視できます。この機能により、サービスの詳細な分析と実用的なメトリックを表示することもできます。サービスグラフは以下に対して表示できます。

- すべてのNetScalerインスタンスにわたって構成されたアプリケーション
- Kubernetesアプリケーション
- 3層Webアプリケーション

## すべてのNetScalerインスタンスにわたるアプリケーションのサービスグラフ

グローバルサービスグラフ機能を使用すると、`clients to infrastructure to application`ビューの全体的な視覚化を行うことができます。このシングルペインのサービスグラフビューから、管理者として次のことができます。

- ユーザーが特定のアプリケーション（3層Webアプリおよびマイクロサービスアプリ）にどの地域からアクセスしているかを理解する
- クライアント要求が処理されるインフラストラクチャ（NetScalerインスタンス）ビューを視覚化する
- 問題がクライアント、インフラストラクチャ、またはアプリケーションのいずれから発生しているかを理解する
- さらにドリルダウンして問題をトラブルシューティングする

**アプリケーション > サービスグラフ**に移動し、**グローバル**タブをクリックして以下を表示します。

- クライアントからバックエンドサーバーに接続されているすべてのアプリケーションのエンドツーエンドの詳細
- それぞれのデータセンターに接続されているすべてのNetScalerインスタンス

> **注**
>
> GSLBアプリがある場合にのみ、データセンターを表示できます。

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

- クライアントメトリクス情報
- NetScalerメトリクス情報
- 個別のアプリケーション、カスタムアプリケーション、および個別のマイクロサービスアプリケーションを持つすべてのNetScalerインスタンス
- カスタムアプリ、個別アプリ、マイクロサービスアプリに属するスコアの低い上位4つのアプリケーション
- スコアの低い上位4つの仮想サーバーのメトリクス情報
- アプリケーション（個別アプリ、カスタムアプリ、マイクロサービスアプリ）のステータス（**Critical**、**Review**、**Good**、**Not Applicable**など）。

詳細については、「サービスグラフにおけるアプリケーションの全体像」(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/holistic-view-sg.html)を参照してください。

## Kubernetesアプリケーションのサービスグラフ

**Applications > Service Graph** に移動し、**Microservices** タブをクリックして表示します。

- エンドツーエンドのアプリケーション全体のパフォーマンスを確保する
- アプリケーションの異なるコンポーネント間の相互依存性によって生じるボトルネックを特定する
- アプリケーションの異なるコンポーネント間の依存関係に関する洞察を収集する
- Kubernetesクラスター内のサービスを監視する
- どのサービスに問題があるかを監視する
- 性能問題の原因となっている要因を確認する
- サービスHTTPトランザクションの詳細な可視性を表示する
- HTTP、TCP、およびSSLメトリックを分析する

NetScaler Consoleでこれらのメトリックを視覚化することで、問題の根本原因を分析し、必要なトラブルシューティングアクションをより迅速に実行できます。サービスグラフは、アプリケーションをさまざまなコンポーネントサービスに表示します。Kubernetesクラスター内で実行されているこれらのサービスは、アプリケーション内外のさまざまなコンポーネントと通信できます。開始するには、「サービスグラフの設定」を参照してください。

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

# 3層Webアプリケーションのサービスグラフ

**Applications > Service Graph** に移動し、**Web Apps** タブをクリックして以下を表示します。

- アプリケーションがどのように構成されているか（コンテンツスイッチング仮想サーバーと負荷分散仮想サーバーを使用）に関する詳細

  GSLBアプリケーションの場合、データセンター、NetScalerインスタンス、CS、およびLB仮想サーバーを表示できます。
- クライアントからサービスへのエンドツーエンドのトランザクション
- クライアントがアプリケーションにアクセスしている場所
- クライアント要求が処理されるデータセンター名と、関連するデータセンターNetScalerメトリック（GSLBアプリケーションのみ）
- クライアント、サービス、および仮想サーバーのメトリック詳細
- エラーがクライアントからのものか、サービスからのものか
- **Critical**、**Review**、**Good** などのサービスステータス。NetScaler Consoleは、サービス応答時間とエラー数に基づいてサービスステータスを表示します。
  - **Critical (赤)** - 平均サービス応答時間 > 200 ms かつエラー数 > 0 の場合に示されます。
  - **Review (orange)** - 平均サービス応答時間 > 200 ミリ秒またはエラー数 > 0 の場合に示されます。
  - **Good (green)** - エラーがなく、平均サービス応答時間 < 200 ミリ秒の場合に示されます。
- クライアントのステータス (**Critical**、**Review**、**Good** など)。NetScaler Console は、クライアントのネットワーク遅延とエラー数に基づいてクライアントのステータスを表示します。
  - **Critical (red)**- 平均クライアントネットワーク遅延 > 200 ミリ秒かつエラー数 > 0 の場合に示されます。
  - **Review (orange)** - 平均クライアントネットワーク遅延 > 200 ミリ秒またはエラー数 > 0 の場合に示されます。
  - **Good (green)** - エラーがなく、平均クライアントネットワーク遅延 < 200 ミリ秒の場合に示されます。
- 仮想サーバーのステータス (**Critical**、**Review**、**Good** など)。NetScaler Console は、アプリスコアに基づいて仮想サーバーのステータスを表示します。
  - **Critical (red)** - アプリスコア < 40 の場合に示されます。
  - **Review (orange)** - アプリスコアが 40 から 75 の間に示されます。

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

- **Good (green)** - アプリスコア > 75 の場合に示されます。

**注意点:**

- サービスグラフには、負荷分散、コンテンツスイッチング、GSLB 仮想サーバーのみが表示されます。
- カスタムアプリケーションに仮想サーバーがバインドされていない場合、そのアプリケーションの詳細はサービスグラフに表示されません。
- 仮想サーバーと Web アプリケーション間でアクティブなトランザクションが発生している場合にのみ、サービスグラフでクライアントとサービスのメトリックを表示できます。
- 仮想サーバーと Web アプリケーション間でアクティブなトランザクションがない場合でも、負荷分散、コンテンツスイッチング、GSLB 仮想サーバー、サービスなどの構成データに基づいて、サービスグラフで詳細を表示できます。
- アプリケーション構成に変更があった場合、サービスグラフに反映されるまでに10分かかる場合があります。

詳細については、アプリケーションのサービスグラフを参照してください。

# Kubernetesアプリ向けサービスグラフ

Kubernetesアプリのサービスグラフを使用して、Kubernetesクラスター内のマイクロサービスを視覚化、監視、トラブルシューティングします。以下のトピックは、サービスグラフのセットアップ、表示、分析に役立ちます。

- サービスグラフのセットアップ(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/service-graph-begin.html)
- サービスグラフでの詳細表示(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/service-graph-begin-details.html)
- サービスグラフでのしきい値の設定(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/configure-thresholds-sg.html)
- サービス詳細の表示(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/view-service-details-service-graph.html)

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

- トラブルシューティングのためのイングレス詳細の表示(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/ingress-details.html)
- 分散トレース(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/service-graph-trace.html)
- 診断の表示(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/serviceability-sg.html)

## サービスグラフのセットアップ

### ソフトウェア要件

| KUBERNETESディストリビューション | KUBERNETESバージョン | コンテナネットワークインターフェース(CNI) | CPXバージョン | CICバージョン | NETSCALER CONSOLEバージョン | NETSCALERエージェントバージョン |
|---|---|---|---|---|---|---|
| オープンソース | v1.16.3 | フラネル、カリコ、またはカナル | 13.0–41.28以降 | 1.5.25以降 | 13.0–47.22以降 | 13.0–47.22 以降 |

Kubernetesクラスターは、さまざまなデプロイメントトポロジで構成でき、サービスグラフでサポートされているトポロジを次の表に示します。

| トポロジ | サービスグラフでサポート |
|---|---|
| 単一ティアまたは統合インGRESS | はい |
| デュアルティア | はい |
| クラウド | はい、ただしクラウドロードバランサーはグラフに表示されません |
| サービスメッシュライト | はい |
| サービスメッシュ | はい |
| LoadBalancerタイプのサービス | いいえ |

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

| トポロジ | サービスグラフでサポート |
| --- | --- |
| NodePortタイプのサービス | いいえ |

NetScaler Consoleでサービスグラフの設定を完了するには、Kubernetesクラスター用に構成したトポロジタイプをクリックし、記載されている手順を完了してください。

- シングルティアまたは統合イングレストポロジ
- デュアルティアまたはサービスメッシュライトトポロジ
- サービスメッシュトポロジ

**注**

デュアルティアおよびサービスメッシュライトトポロジのサービスグラフ設定手順は同じです。

### 始める前に

以下のシナリオでサービスグラフを表示できます。

- NetScaler ConsoleとKubernetesクラスターが同じネットワーク上にある場合（例：NetScaler ConsoleとKubernetesクラスターが同じCitrix Hypervisorでホストされている場合）。
- NetScaler ConsoleとKubernetesクラスターが異なるネットワーク上にある場合。このシナリオでは、オンプレミスエージェントを構成し、Kubernetesクラスターがホストされているネットワークにエージェントを登録する必要があります。

### シングルティアまたは統合イングレストポロジ

以下を確認してください。

- 単一ティアまたは統合イングレストポロジでKubernetesクラスターを構成済み。
- NetScaler ConsoleにVPX、MPX、SDX、BLXインスタンスを追加し、**Web Insight**を有効にしました。
- NetScaler ConsoleにKubernetesクラスターを追加しました。

### デュアルティアまたはService Mesh Liteトポロジ

以下を確認してください。

- サポートされているいずれかのトポロジでKubernetesクラスターを構成済み。

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

- NetScaler ConsoleとNetScaler CPX間の通信を有効にするために、NetScaler Consoleで静的ルートを構成済み。

  **注**

  NetScaler Consoleを同じクラスター内のマイクロサービスとして展開している場合は、この手順を無視できます。

- GitHubリポジトリからサンプル展開ファイルをダウンロード済み。
- NetScaler ConsoleへのCPXの登録を成功させるために、CPX YAMLファイルに必要なパラメーターを追加済み。
- NetScaler ConsoleにVPX、MPX、SDX、またはBLXインスタンスを追加しました。
- NetScaler ConsoleにKubernetesクラスターを追加しました。
- サンプルマイクロサービスアプリケーションを展開済み。
- NetScaler CPXを展開し、CPXをNetScaler Consoleに登録しました（2層アーキテクチャにのみ適用）。
- 仮想サーバーをライセンスするために、仮想サーバーの自動選択を有効にしました。
- NetScalerエージェントがHTTPおよびTCPトランザクションを取得できるように、WebトランザクションおよびTCPトランザクション設定を**すべて**に有効にしました。
- マイクロサービスにトラフィックを送信しました。

### サービスメッシュトポロジ

以下を確認してください。

- 以下のいずれかのサービスメッシュトポロジでKubernetesクラスターバージョン`1.14.0`を構成しました。
  - IstioのサイドカープロキシとしてのNetScaler CPX
  - Istioのイングレスゲートウェイとしての NetScaler
- `admissionregistration.k8s.io/v1beta1` APIを有効にしました。APIは以下を使用して確認できます。

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  以下の出力は、APIが有効になっていることを示しています。

  ```
  admissionregistration.k8s.io/v1beta1
  ```

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

- Istio `istio v.1.3.0`をインストールしました。
- Helmバージョン3.xをインストールしました。
- NetScaler ConsoleとNetScaler CPX間の通信を有効にするために、NetScaler Consoleで静的ルートを構成しました。

> **注**
>
> 同じクラスターにNetScalerエージェントをマイクロサービスとして展開している場合は、この手順を無視できます。

- サービスメッシュトポロジデータを入力するために、必要なパラメータを設定しました。
- サンプルアプリケーションを展開しました。
- NetScaler ConsoleにKubernetesクラスターを追加しました。
- 仮想サーバーをライセンスするために、仮想サーバーの自動選択を有効にしました。

> **注**
>
> サービスメッシュ展開でCPXがサイドカープロキシとして展開されている場合、仮想サーバーはIPアドレスがCPX NS IPと一致する場合にのみライセンスされます。

- NetScalerエージェントがHTTPおよびTCPトランザクションを取得できるように、Webトランザクションおよび TCPトランザクション設定を**すべて**に設定しました。
- マイクロサービスにトラフィックを送信しました。

## サービスグラフで詳細を表示

NetScaler Consoleで、**Applications > Service Graphs > Kubernetes service graph** に移動し、リストから期間を選択してサービスグラフの詳細を表示します。

| 2層/SERVICE MESH LITE トポロジ | 単層/UNIFIED INGRESS トポロジ |
| --- | --- |
|  |  |

- **Tier 1 ingress** – Kubernetesクラスター内部で動作するNetScaler Ingress Controllerが、Kubernetesクラスター外部にあるNetScalerインスタンス（VPX/MPX/SDX/BLX）を設定します。

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

- **Tier 2 ingress** – Kubernetesクラスター内でNetScaler CPXインスタンスとともにサイドカーとして実行されているNetScaler Ingress Controller。
- **Ingress** – 他のすべての展開トポロジに対して表示されます。

### サービスグラフダッシュボード



**1** - コンポーネントサービスがどのように通信しているかを示す、アプリケーションのエンドツーエンドネットワークマップ

**2** – 特定の期間のヒット数とエラー数を示すグラフ

**3** – サービスを検索するための検索バー

**4** – 期間を選択するためのタイムリスト

**5** - サービスを表示するためのフィルターを適用します。

**6** – 設定アイコン

**7** – ズームインおよびズームアウト表示

**8** – グラフ表示または表形式表示

選択した期間に基づいて、サービスグラフを表示できます。

| サービスアイコン | 説明 |
| --- | --- |
|  | エッジの幅はヒット数を示します。エッジの幅が広いほど、ヒット数が多いことを示します。 |
|  | 警告アイコンが付いたサービスは、そのサービスにエラーがあることを示します。 |
|  | ストップウォッチアイコンが付いたサービスは、そのサービスに遅延または応答時間の問題があることを示します。 |
|  | ストップウォッチアイコンと警告アイコンの両方が付いたサービスは、そのサービスにエラーと遅延/応答時間の両方の問題があることを示します。 |

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

**注**

サービスに警告アイコンまたはストップウォッチアイコンがない場合、そのサービスに異常があるか、ヒット数のしきい値を超えていることを示します。

選択した期間に基づいて、サービスグラフを表示できます。ヒット数を示すグラフから期間を選択し、さらに詳細な情報をドリルダウンできます。

**注**

NetScaler Consoleでアクティブなトランザクションが受信されない場合、NetScalerインスタンスによって負荷分散されているサービスのみを表示できます。サービスにマウスポインターを合わせると、すべてのメトリックが0として表示されます。

サービスグラフには、サービスが使用するプロトコルが表示されます。次の画像に示すように、Kubernetesクラスターで次のサービスが実行されているとします。

注

**Orchestration** > **Kubernetes** > **Clusters** に複数のクラスターを追加している場合、各クラスターに関連付けられたサービスを表示できます。

サービスについて、次のステータスを表示できます。

- **重大 (赤)** - 平均サービス応答時間 > 200 ms かつ エラー数 > 0 の場合に示されます。
- **レビュー (オレンジ)** - 平均サービス応答時間 > 200 ms または エラー数 > 0 の場合に示されます。
- **良好 (緑)** - エラーがなく、平均サービス応答時間が200ミリ秒未満であることを示します

以下は、サービスが使用するプロトコルを識別できるプロトコルです。

- **TCP** – サービスがTCPプロトコルを使用していることを示します。
- **SSL, HTTP** – サービスがSSL over HTTPプロトコルを使用していることを示します。
- **SSL, TCP** – サービスがSSL over TCPプロトコルを使用していることを示します。

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

**注**

プロトコルがないサービスは、HTTPプロトコルを使用していることを示します。

### 表形式ビューを使用して主要メトリックの傾向を表示する

表形式ビューを使用すると、以下を確認できます。

- サービスの主要メトリック
- ソースサービスから宛先サービス間の主要メトリック

管理者として、これらの主要メトリックを使用して、選択した期間のゴールデンシグナルの傾向を分析できます。

### クライアントメトリックを表示する

クライアントがどの場所からサービスにアクセスしているかを確認できます。管理者として、クライアントメトリックを視覚化し、クライアントから発生する問題を分析できます。

クライアント領域にマウス ポインターを合わせると、メトリックが表示されます。

クライアントメトリック(/en-us/netscaler-application-delivery-management-software/media/client-metrics1.png)

- **ヒット数** - クライアントが受信した合計ヒット数を示します。
- **クライアントネットワーク遅延** - 平均クライアントネットワーク遅延を示します。
- **クライアント 4xx エラー** - クライアントの合計 4xx エラーを示します。
- **クライアント SSL エラー** - クライアントの合計 SSL エラーを示します。

**NetScaler Console の IP ブロック** - クライアントがパブリック IP アドレスを使用している場合、NetScaler Console はクライアントの場所を認識できます。NetScaler Console には、クライアント IP アドレス範囲に基づいて場所を照合する組み込みの場所 CSV ファイルがあります。

NetScaler Console は、プライベート IP アドレスが NetScaler Console サーバーに追加されている場合にのみ、プライベート IP アドレスを持つクライアントの場所を認識できます。たとえば、クライアント IP アドレスが都市 A に関連付けられたプライベート IP アドレス範囲内にある場合、NetScaler Console は、このクライアントのトラフィックが都市 A から発信されていると認識します。

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

### プライベート IP ブロックを作成する

NetScaler Console は、クライアントのプライベート IP アドレスが NetScaler Console サーバーに追加されている場合に、クライアントの場所を認識できます。たとえば、クライアントの IP アドレスが都市 A に関連付けられたプライベート IP アドレスブロックの範囲内にある場合、NetScaler Console は、このクライアントのトラフィックが都市 A から発信されていると認識します。

IP ブロックを作成するには：

1. NetScaler Console で、**設定** > **分析設定** > **IP ブロック** に移動し、**追加** をクリックします。
2. **IP ブロックの作成** ページで、次のパラメーターを指定します。
   - **名前**。プライベート IP ブロックの名前を指定します。
   - **開始 IP アドレス**。IP ブロックの最小 IP アドレス範囲を指定します。
   - **終了IPアドレス**。IPブロックの最大IPアドレス範囲を指定します。
   - **国**。リストから国を選択します。
   - **地域**。国に基づいて地域が自動入力されますが、独自の地域を選択できます。
   - **都市**。地域に基づいて都市が自動入力されますが、独自の都市を選択できます。
   - **都市の緯度**と**都市の経度**。選択した都市に基づいて、緯度と経度が自動入力されます。
3. **作成**をクリックして完了します。

### パブリックIPブロック

NetScaler Consoleは、クライアントがパブリックIPアドレスを使用している場合、クライアントの場所を認識することもできます。NetScaler Consoleには、クライアントIPアドレス範囲に基づいて場所を照合する組み込みの場所CSVファイルがあります。パブリックIPブロックを使用するための唯一の要件は、**Configure Insight**ページから**地理データ収集を有効にする**ことです。

注

> NetScaler Consoleは、特定の地理的位置のジオマップを表示するためにインターネット接続を必要とします。GeoMapを.pdf、.png、または.jpg形式でエクスポートするためにもインターネット接続が必要です。

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

### イングレスメトリクスの表示

Kubernetesクラスターで使用されているイングレスの種類を表示できます。



- NetScaler IPアドレスとそのスコア
- **現在の状態** – NetScalerインスタンスがUp、Down、またはOut of Statusのいずれであるかを示します
- **最大寄与** – インスタンススコアに影響を与えている問題を示します

シングルティアトポロジの場合、単一の**Ingress**のみを表示できます。

詳細を確認するには、**Ingress**をクリックしてさらにドリルダウンします。詳細については、「問題トラブルシューティングのためのイングレス詳細の表示」を参照してください。

## TCPおよびSSLメトリックの表示

TCPおよびSSLメトリックを使用すると、次のことができます。

- サービス間のTCP接続の詳細を表示する
- TCP関連の問題が送信元サービスまたは宛先サービスのどちらに起因するかを判断する
- SSLエラーが送信元サービスまたは宛先サービスのどちらに起因するかを表示する
- SSLサービスで使用されているSSLプロトコルバージョンを表示する

### TCPメトリック

TCPサービスまたはそれに関連付けられた受信サービスにマウスポインターを合わせると、TCPメトリックが表示されます。



- **TCP接続** – サービス間で確立された合計接続数
- **データ量** – サービスによって処理された合計データ
- **TCPサーバーリセット** – サーバーから開始された合計TCPリセット

### SSLメトリクス

SSLプロトコルを使用するサービスにマウスポインターを合わせると、SSLメトリクスが表示されます。



- **SSLサーバーエラー** – サーバーからの合計SSLエラーを示します。(例: SSL証明書不明)
- **SSLプロトコル** – サービスによって使用されるSSLプロトコルバージョンを示します

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

- **SSLクライアントエラー** – クライアントからの合計SSLエラーを示します。(例: SSLクライアント認証エラー)

### サービスの詳細を表示

サービスをクリックし、**詳細の表示**を選択してサービスの詳細を表示します。詳細については、「サービスの詳細を表示」を参照してください。

### フィルターを適用

特定のサービス情報を表示するためにフィルターを適用できます。フィルターオプションを取得するには、**フィルターなし**リストをクリックします。

たとえば、レイテンシーが150ミリ秒未満のサービスを表示したい場合は、**サービス応答時間**の下にある棒グラフをクリックして結果を表示します。

「**サービス情報**」をクリックして、次のフィルターを選択して適用します。

- **クラスター** – 選択したクラスターまたは複数のクラスターに適用可能なすべてのサービスを表示します。
- **名前空間** – 選択した名前空間に適用可能なすべてのサービスを表示します。

  注

  > Kubernetesサービス定義YAMLでサービスに設定されているラベルに応じて、さらに多くのフィルターオプションを表示できる場合があります。

「**すべてクリア**」をクリックして、すべてのフィルターをクリアします。

または、検索テキストボックスを使用してサービス名を入力し、サービスグラフに結果を表示することもできます。

### 設定オプションの使用

**1** – 設定アイコン

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

**2** – サービスグラフをデフォルト、レイヤーベース、または強制指向ビューとして表示するオプション

**3** – リストからオプションを選択して、カテゴリに基づいてサービスを表示します。リストからカテゴリを選択したら、グラフ上の「**+**」をクリックしてすべてのサービスを表示します。



**4** – サービスの表示方法を選択するオプションを有効にします。

**5** - 設定を保存するか、デフォルトにリセットするオプション。

### エラーを分析する

エラーを示しているサービスにマウスポインターを合わせます。

| エラー | 説明 |
| --- | --- |
|  | **TCPサーバーリセット**は、サーバーから開始されたTCPリセットの合計数を示します。 |
|  | **TCPクライアントリセット**は、クライアントによって開始されたTCPリセットの合計数を示します。 |
|  | SSLクライアントエラーは、クライアントからのSSLエラーの合計数を示します。（例：SSLクライアント認証エラー）. |
| | SSLサーバーエラーは、サーバーからのSSLエラーの合計数を示します。（例：SSL証明書不明） |

**注**

- クライアントエラー数が**1以上**の場合、プロトコルタイプに関係なく、任意のサービスでクライアントエラー数が表示されます。
- 任意のサービスに表示されるクライアントエラー数は、エラーがクライアント側からのものであることを示します。

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

### HTTPトランザクションの詳細を表示

**注**

エラーのあるサービスにマウスポインターを合わせ、問題の数をクリックすると、エラーを表示できます。

画像に示されている例によると、コンポーネントサービスがどのように通信しているかを示す、アプリケーションのエンドツーエンドのネットワークマップを表示できます。

**Ecommerce-Service**にマウスポインターを合わせると、**Ecommerce-Service**のメトリック詳細を表示できます。

NetScaler Consoleでは、Ingressとサービス間のトランザクション詳細も表示できます。マウスポインターを合わせると、Ingressとサービス間の合計エラー数、平均サービス応答時間などの詳細が表示されます。

**ヒット数** – サービスが受信したヒットの総数を示します。

**サービス応答時間** – サービスがTime To First Byte (TTFB) に応答するまでにかかる平均応答時間を示します。

**エラー** – 4xx、5xxなどの合計エラー数を示します。

**データ量** – サービスによって処理されたデータの総量を示します。

**SSLプロトコル** – SSLプロトコルバージョンを示します。

詳細なトランザクションを表示するには、**Ingress** と **service** の間の矢印をクリックします。

詳細については、Webトランザクションの分析を表示を参照してください。

## サービスグラフでしきい値を設定する

管理者として、Kubernetesサービスにしきい値を設定できます。NetScaler Consoleは、サービス応答時間とエラー数に基づいてサービスステータス（重大、レビュー、良好）を表示します。デフォルトでは、すべてのサービスに適用される**デフォルトしきい値**（サービス応答時間 = 200ミリ秒、エラー数 = 0）を表示できます。

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

**注**

デフォルトしきい値を削除することはできません。

新しいしきい値を設定するには：

サービスグラフで：

1. 設定アイコンをクリックし、**しきい値**タブを選択します。
2. 新しいしきい値を設定するには、**新しいしきい値**をクリックします。

   しきい値の設定(/en-us/netscaler-application-delivery-management-software/media/sg-new-threshold.png)

   **新しいしきい値**ページが表示されます。
3. 次のパラメータを設定します。

   a. **名前** – しきい値の名前を指定します。

   b. **マイクロサービス**で、しきい値を適用するサービスを選択します。

   c. **しきい値**で、高応答時間と高エラーに対して**単一**または**二重**を選択します。

   d. しきい値を指定します。

   **注記**

   二重しきい値を選択する場合は、以下を確認してください。

   - しきい値1の値はしきい値2の値よりも小さいこと。たとえば、しきい値1を250ミリ秒に設定した場合、しきい値2は251ミリ秒以上である必要があります。
   - しきい値1の値はしきい値2の値と同じであってはなりません。
4. **保存**をクリックします。

   しきい値が正常に作成されました。しきい値の詳細は、**しきい値**ページで確認できます。

### 単一しきい値

単一しきい値を構成すると、NetScaler Consoleは次のようになります。

- 現在の値を構成されたしきい値と比較します

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

- 超過したしきい値に基づいて合計ペナルティを計算します
- ペナルティ計算に基づいてサービススコアとサービスステータスを表示します

### 二重しきい値

二重しきい値を構成すると、NetScaler Consoleは次のようになります。

- 現在の値を構成されたしきい値と比較します
- 現在の値が以下であるかどうかを確認します。
  - しきい値1より小さい
  - しきい値1と2の間
  - しきい値2より大きい
- 超過したしきい値に基づいて合計ペナルティを計算します
- ペナルティ計算に基づいてサービススコアとサービスステータスを表示します

## サービスの詳細を表示

サービスをクリックし、**詳細を表示**を選択します。

サービス詳細オプション(/en-us/netscaler-application-delivery-management-software/media/sg-details.png)

サービス詳細ページでは、以下を表示できます。

- サービスがホストされているクラスター名 (1)
- サービスのネームスペースとサービスラベル (2) (4)
- 選択したサービスに接続されているすべての関連する受信および送信サービス (3)
- ヒット数、応答時間、エラー、データ量、SSLフロントエンドエラー、TCPフロントエンドエラーなどのグラフ形式のサービス主要メトリック (5)。
- サービスに関連付けられているバックエンドポッド (6)。

  サービス詳細(/en-us/netscaler-application-delivery-management-software/media/sg-details-more.png)

これらの主要メトリックの傾向を使用して、特定の期間におけるサービスのパフォーマンスを分析できます。

**応答時間**メトリックでは、以下を表示できます。

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

- **99パーセンタイル** – 選択した期間のリクエストの99%が32ミリ秒未満であることを示します（例の画像による）。
- **平均** – サービスからの平均応答時間を示します
- **99.9パーセンタイル** – サービスからの最高の応答時間を示します

### メトリックの詳細

| メトリック | 説明 |
|---|---|
| ヒット数 | サービスが受信したリクエストの総数 |
| エラー | サービスからのHTTPエラーの総数 |
| サービス応答時間 | サービスがTime To First Byte (TTFB) に応答するまでにかかった平均応答時間。 |
| データ量 | サービスによって処理されたデータ総量 |
| SSLフロントエンドエラー | サービスからのSSLフロントエンドエラーの総数。例: SSL CLIENTAUTH FAILURE |
| SSLバックエンドエラー | サービスからのSSLバックエンドエラーの総数。例: SSL Client Errors |
| TCP バックエンドエラー | サービスからのTCPバックエンドエラーの合計。例: TCPサーバーリセット |
| TCP フロントエンドエラー | サービスからのTCPフロントエンドエラーの合計。例: TCPクライアントリセット |

### バックエンドPodの詳細を表示

**Pod**タブをクリックして、サービスに関連付けられているバックエンドPodを表示します。

バックエンドPod(/en-us/netscaler-application-delivery-management-software/media/backend-pod-details.png)

- **Pod名** – Pod名を示します
- **ステータス** – Podが実行中（UP）か、そうでないか（DOWN）を示します。
- **IPアドレス** – PodのIPアドレスを示します

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

**「今すぐポーリング」オプションを使用してPodステータスを取得する**

**今すぐポーリング**オプションは、クラスターから最新のPodステータスを取得します。

今すぐポーリング(/en-us/netscaler-application-delivery-management-software/media/sg-poll-now.png)

## トラブルシューティングのためのイングレスの詳細を表示

サービスグラフで、イングレスをクリックし、**詳細の表示**を選択して、Kubernetesクラスター用に構成されたNetScalerインスタンスの詳細を視覚化します。

イングレスの詳細(/en-us/netscaler-application-delivery-management-software/media/ingress-details.png)

**インスタンスの詳細**をクリックして、詳細を表示します。

インスタンスの詳細(/en-us/netscaler-application-delivery-management-software/media/instanceinfo-ingress.png)

次の詳細が表示されます。

- **情報** - インスタンスタイプ、展開タイプ、バージョン、モデルなどのインスタンスの詳細。

  情報(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instanceinfo.png)
- **機能** – デフォルトでは、ライセンスされていない機能が表示されます。**ライセンスされた機能**をクリックして、ライセンスされている機能を表示します。

  機能(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instancefeature.png)
- **モード** – デフォルトでは、インスタンスで無効になっているすべてのモードが表示されます。**有効なモードの表示**をクリックして、インスタンスで有効になっているモードを表示します。

  モード(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instancemodes.png)

インスタンスダッシュボードには、次の詳細を確認できるインスタンスの概要が表示されます。

- **インスタンススコア**

  インスタンススコア(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instancescore.png)

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

**1** – 選択した期間の現在のNetScalerインスタンススコアを示します。最終スコアは**100から合計ペナルティを引いた値**として計算されます。グラフには、選択した期間のスコア範囲が表示されます。

**2** – NetScalerインスタンスの現在のステータス（**Up**、**Down**、**Out of Service**など）を示します。

**3** – NetScalerインスタンスが稼働している期間を示します。

**4** – インスタンスで有効または無効になっているネットワークインターフェイスの合計数を示します。クリックすると、ネットワークインターフェイス名やステータス（有効または無効）などの詳細が表示されます。

**5** – リストから期間を選択して、インスタンスの詳細を表示します。

**6** – NetScalerインスタンスの合計問題数と問題カテゴリを表示します。

- **主要メトリック**

  各タブをクリックして詳細を表示します。各メトリックでは、選択した期間の平均値と差分値を表示できます。

  次の画像はHTTPS Req/Secの例で、選択された期間は過去1か月です。値**692**は過去1か月のHTTPS Req/Secの平均値であり、値**20**は差分値です。グラフでは、最初の値が**139**で、最後の値が**119**です。差分値は**139 – 119 = 20**です。

  

  選択した期間のインスタンスメトリックをグラフ形式で表示できます。

  - **CPU使用率** – 選択した期間におけるインスタンスの平均CPU使用率（パケットCPUと管理CPUの両方に表示されます）。
  - **メモリ使用率** – 選択した期間におけるインスタンスの平均メモリ使用率。
  - **ディスク使用率** – 選択した期間におけるインスタンスの平均ディスクスペース使用率。
  - **スループット** – 選択した期間におけるインスタンスによって処理された平均ネットワークスループット。
  - **HTTPS request/sec** – 選択した期間にインスタンスが受信したHTTPSリクエストの平均。
  - **TCP connections** – 選択した期間にクライアントとサーバーによって確立されたTCP接続の平均。
  - **SSL transactions** – 選択した期間にインスタンスによって処理されたSSLトランザクションの平均。

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

- **問題**

  NetScalerインスタンスで発生する以下の問題を表示できます。

| 問題カテゴリ | 説明 | 問題 |
|---|---|---|
| システムリソース | CPU、メモリ、ディスク使用量など、NetScalerシステムリソースに関連するすべての問題を表示します。 | - 高いCPU使用率 |
| | | - 高いメモリ使用率 |
| | | - 高いディスク使用率 |
| | | - SSLカード障害 |
| | | - 電源障害 |
| | | - ディスクエラー |
| | | - フラッシュエラー |
| | | - NIC破棄 |
| SSL設定 | NetScalerインスタンス上のSSL設定に関連するすべての問題を表示します。 | - SSL証明書の期限切れ |
| | | - 推奨されない発行者 |
| | | - 推奨されないアルゴリズム |
| | | - 推奨されない鍵強度 |
| 設定の逸脱 | NetScalerインスタンスに適用された設定ジョブに関連するすべての問題を表示します。 | - 設定ドリフト |
| | | - 実行中とテンプレートの比較 |

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

| 問題カテゴリ | 説明 | 問題 |
| --- | --- | --- |
| 容量の問題 | NetScalerの容量の問題を表示します。NetScaler Consoleは、NetScalerインスタンスから5分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンターの増分が存在する場合に表示します。問題は、以下の容量パラメータに基づいて分類されます。 | - スループット制限に達しました |
| | | - PE CPU制限に達しました |
| | | - PPS制限に達しました |
| | | - SSLスループットレート制限 |
| | | - SSL TPSレート制限 |
| ネットワーク | インスタンスで発生する運用上の問題を表示します。 | 詳細については、「新しいインジケーターによる強化されたインフラストラクチャ分析」を参照してください。 |

各タブをクリックして、問題を分析し、トラブルシューティングを行います。たとえば、選択した期間にインスタンスに次のエラーが発生したとします。

- **Current** タブには、インスタンススコアに影響を与えている現在のNetScalerの運用上の問題が表示されます。
- **All** タブには、選択した期間に検出されたすべてのインフラストラクチャの問題が表示されます。

## 分散トレース

サービスグラフでは、分散トレースビューを使用して、次のことができます。

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

- サービス全体のパフォーマンスを分析します。
- 選択したサービスとその相互依存サービス間の通信フローを視覚化します。
- どのサービスがエラーを示しているかを特定し、エラーのあるサービスをトラブルシューティングします。
- 選択したサービスとその各相互依存サービス間のトランザクションの詳細を表示します。

### 前提条件

サービスのトレース情報を表示するには、次の操作を行う必要があります。

- アプリケーションが東西トラフィックを送信する際に、次のトレースヘッダーを維持していることを確認します。

  ☐

- **CICビルド1.7.23以前**の場合、CPX YAMLファイルを`NS_DISTRIBUTED_TRACING`と値`yes`で更新します。

  ☐

- **CICビルド1.7.23以降**の場合、ConfigMapを使用する必要があります。

  ConfigMapを使用すると、構成をポッドから分離し、ワークロードをポータブルにすることができます。ConfigMapを使用すると、ワークロードの構成を簡単に変更および管理でき、構成データをポッド仕様にハードコードする必要がなくなります。

  ConfigMapのサポートにより、NetScaler Ingress Controllerポッドを実行したまま、構成を自動的に更新できます。更新後にポッドを再起動する必要はありません。詳細については、イングレスコントローラーのConfigMapサポートを参照してください。

  ConfigMapを使用して、分散トレース、イベント、監査ログなどを有効または無効にできます。ConfigMapを使用するには：

  a. 必要なパラメータを使用してYAMLファイルを作成します。

     次のYAMLファイルの例では、分散トレースが有効になっており、監査ログ、イベント、トランザクションなどの他の変数は無効になっています。

     ```
     apiVersion: v1

     kind: ConfigMap

     metadata:
     ```

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

```
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <Console-AgentIP> / <Console-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
```

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

```
    transactions:

      enable: 'false'

      port: 5557
```

注

`Samplingrate` の値は0から100の間で指定できます。NetScaler Consoleは、指定された数のトレーストランザクションを表示します。

b. ConfigMapをデプロイするには、以下を使用します。

`kubectl create -f <configmap-yaml>.yaml`

c. CPX YAMLファイルを編集し、`envFrom` または `args` のいずれかを使用して次の引数を指定します。

```
envFrom:

 - configMapRef:

     name: cic-configmap
```

または

d. いずれかの変数の値を変更したい場合は、ConfigMapの値を編集します。この例では、他のすべての変数が `false` から `true` に変更されています。

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default
```

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

```
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <Console-AgentIP> / <Console-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
```

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

```
      port: 5557
```

e. 次のコマンドを使用してConfigMapを再適用します。

```
kubectl apply -f <yaml-file>.yaml
```

### サービス追跡の詳細を表示

サービスグラフでサービスをクリックし、**Trace Info** を選択します。

選択したサービスに対して、トレースサマリーページが表示されます。

**トレースサマリー**には以下が表示されます。

- 提案と演算子を使用してトランザクションを検索できる高度な検索 (1)。詳細については、高度な検索を参照してください。
- 1時間、12時間、1日、1週間、1か月、カスタム時間などの時間期間を選択できる時間期間リスト (2)。
- 特定の時間期間の結果を表示するためにドラッグして選択できるタイムライン詳細グラフ (3)。
- 各メトリックからオプションを選択できるフィルターパネル (4)。
- 選択したサービスに関するトランザクションの詳細 (5)。

### トランザクションの詳細を表示する

詳細情報を表示するには、トランザクションをクリックします。選択したサービスに関するトランザクションの詳細を次のように表示できます。

- 開始時刻
- 終了時刻
- SSLメトリック
- 相互依存サービスとの通信 (各サービスのエラーと応答時間を含む)。

以下の例は`catalogue-store-service`からのエラーを示しています。詳細については、 をクリックしてください。

トレースの詳細ページが表示されます。

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

**1** – トランザクションの開始時刻、応答時間、合計サービス、および合計スパンを表示します。

**2** – 相互依存サービスと通信した選択されたサービスの詳細を表示します。各トランザクションをクリックして詳細を表示できます。

**3** – 各サービスのトランザクションの詳細を表示します。

例の画像によると、`catalogue-store-service`はエラーを示しています。`catalogue-store-service`で利用可能なトランザクションをクリックしてください。

`product-catalogue-service`と`catalogue-store-service`間のトランザクションの詳細は、HTTP応答が500であることを示しています。これらの詳細により、管理者として、エラーのあるサービスを分析し、解決策として`product-catalogue-service`をトラブルシューティングできます。

パネルの下にある各メトリックからオプションを選択して、結果をフィルターすることもできます。たとえば、すべての5xxトランザクションを表示したい場合は、 をクリックして を選択します。

- **クライアントRTT**: パケットがクライアントから移動する時間。
- **サーバーRTT**: パケットがサーバーから移動する時間。
- **アプリ応答時間**: アプリケーションの平均応答時間
- **データ転送時間**: サービスとの間で転送が発生する可能性のあるデータ転送サイズと転送速度。
- **ロケーション**: クライアントのロケーション
- **ブラウザ**: クライアントが使用するブラウザの種類。例: Chrome、Firefox。
- **クライアントOS**: ブラウザのユーザーエージェントの詳細に基づくクライアントOS。
- **デバイス**: ブラウザのユーザーエージェントの詳細に基づくデバイス。例: タブレット、モバイル。
- **リクエストタイプ**: トランザクションのリクエストタイプ。例: GET。
- **レスポンスコード**: サーバーから受信したレスポンスコード。例: 501、404、200。
- **レスポンスコンテンツタイプ**: トランザクションのコンテンツタイプ。クライアントのリクエストがtext/htmlの場合、サーバーからのレスポンスもtext/htmlである必要があります。
- **SSLプロトコル**: クライアントが使用するSSLプロトコルバージョン。例: SSLv3。

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

- **SSL暗号強度**: 高、中、低などのSSL証明書キーサイズに基づく暗号強度。
- **SSLキー強度**: SSL暗号強度はSSL証明書キーサイズから計算されます。キー長はSSLアルゴリズムのセキュリティを定義します。例: 2048
- **SSLフロントエンド障害理由**: フロントエンドのSSLハンドシェイクエラーメッセージ。例: SSL CLIENTAUTH FAILURE

## サービスグラフの部分データまたはデータなしの診断詳細を表示する

必要なサービスグラフ構成を完了し、NetScaler ConsoleにKubernetesクラスターを追加すると、サービスグラフにデータが入力され始めます。場合によっては、サービスグラフが部分的なデータまたはデータを表示しないことがあります。サービスグラフに部分的なデータまたはデータがない場合の考えられる理由の一部は次のとおりです。

- 静的ルートが構成されていません
- Kubernetesクラスターのステータスがダウンしています
- CPXの登録に失敗しました
- CPX仮想サーバーはライセンスされていません
- サービスグラフがすべてのデータをロードするのを妨げる必要な分析構成が設定されていません

管理者として、サービスグラフが部分的なデータまたはデータを表示しない場合、その理由を分析するのは難しいと感じるかもしれません。サービスグラフページの診断情報により、部分的なデータまたはデータなしの問題をトラブルシューティングするための考えられる理由と必要なアクションを確認できます。

NetScaler Consoleで、**Applications** > **Service Graph** に移動し、**Microservices** タブをクリックします。

### データなしの診断

サービスグラフにデータが表示されない場合、次の診断メッセージが表示されます。

詳細を表示するには **>** をクリックします。サービスグラフにデータが表示されない考えられる理由を確認できます。次の画像は、サービスグラフにデータがない場合の例です。

問題の詳細を表示するには、**See More** をクリックします。

詳細を見る(/en-us/netscaler-application-delivery-management-software/media/more-details.png)

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

- **問題の種類** – 設定、分析設定、またはライセンスから発生する問題かどうかを示します。
- **メッセージ** – 問題の原因を示します。
- **アクション** – 問題のトラブルシューティングのために実行する必要があるアクションを示します。

### 部分的なデータに関する診断

サービスグラフが部分的なデータのみで表示される場合は、**診断の表示**ボタンをクリックして診断情報を表示します。

次の例は、TCPトランザクションが無効になっていることを示しています。

部分的なデータ(/en-us/netscaler-application-delivery-management-software/media/partial-data.png)

この例では、**設定 > 分析設定**に移動して、**TCPトランザクション設定**を**すべて**に有効にする必要があります。

### トラブルシューティング

管理者として、これらの診断メッセージを使用して、これらの問題を検証し、トラブルシューティングを試みることができます。トラブルシューティング後、NetScaler Consoleは定期的に自動で診断チェックを実行します。診断チェックが完了すると、サービスグラフの部分的なデータまたはデータなしの問題が解決されます。

また、**診断の実行**をクリックし、**CPXインスタンス**を選択して、**診断の実行**をクリックすることもできます。

トラブルシューティング(/en-us/netscaler-application-delivery-management-software/media/troubleshooting.png)

その他のトラブルシューティングシナリオについては、FAQを参照してください。

## アプリケーションのサービスグラフ

アプリケーションのサービスグラフを表示するには：

1. **Applications** > **Dashboard** に移動します。
2. アプリケーションを選択します。

   アプリケーションの詳細ページが表示されます。
3. 期間を選択し、**Service Graph** をクリックします。

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

選択したアプリケーションのサービスグラフページが表示されます。

サービスグラフは、**Application View** または **Network Functions View** で表示できます。

ヒット数とエラーをドラッグして選択し、結果を変更することもできます。

## アプリケーションビュー

アプリケーション構成の概要が表示されます。このビューでは、クライアント、NetScaler、およびWebアプリケーション間の通信を視覚化できます。

## ネットワーク機能ビュー

アプリケーションに関連付けられている仮想サーバーを表示します。このビューでは、NetScalerが以下と通信しているかどうかを視覚化できます。

- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバー
- アプリケーションにアクセスするための負荷分散仮想サーバー
- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバーと負荷分散仮想サーバーの両方

GSLBアプリケーションの場合、データセンターとNetScalerとともに詳細が表示されます。

## アクティブなトランザクションがない場合のサービスグラフビュー

NetScalerとWebアプリケーション間でアクティブなトランザクションが発生しない場合、サービスグラフはアプリケーションの基本構成（クライアントとNetScalerなし）のみを表示します。

サービスまたは仮想サーバーにマウスポインターを合わせると、トランザクションがないため、すべてのメトリックの詳細が0として表示されます。

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

# メトリックの分析

各サービスにマウスポインターを合わせると、アプリケーションビューまたはネットワーク機能ビューでメトリックの詳細を表示できます。

## クライアントメトリクス

クライアントにマウスポインターを合わせると、クライアントメトリクスが表示されます。

クライアントメトリクス(/en-us/netscaler-application-delivery-management-software/media/ga-sg-clientmetrics.png)

- **クライアントネットワーク遅延** – クライアントからのネットワーク遅延を示します。
- **クライアント4xxエラー** – クライアントから発生した4xxエラーの合計数を示します。
- **クライアントSSLエラー** – クライアントからのSSLエラーの合計数を示します。

## ネットワーク機能メトリクス

ロードバランシングまたはコンテンツスイッチングサービスにマウスポインターを合わせると、メトリクスの詳細が表示されます。

ネットワーク機能メトリクス(/en-us/netscaler-application-delivery-management-software/media/ga-sg-networkmetrics.png)

- **ヒット数** – 仮想サーバーが受信したヒットの合計数を示します。
- **NetScaler処理時間** – NetScalerインスタンスによる平均処理時間を示します。
- **データ量** – 仮想サーバーによって処理されたデータ総量を示します。
- **ヘルススコア** – アプリケーションスコアを示します。
- **現在の状態** – 仮想サーバーの現在のステータスを示します。

## サービスメトリクス

サービス（Webアプリケーション）にマウスポインターを合わせると、メトリックが表示されます。

サービスメトリック(/en-us/netscaler-application-delivery-management-software/media/ga-sg-servicemetrics.png)

- **ヒット数** – サービスが受信したヒットの総数を示します。
- **サービス応答時間** – サービスからの平均応答時間を示します。
- **エラー** – サービスで発生したエラーの総数を示します。

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

- **データ量** – サービスによって処理されたデータの総量を示します。

### NetScalerメトリック（GSLBアプリケーションのみ）

NetScalerにマウスポインターを合わせると、メトリックが表示されます。

NetScalerメトリック(/en-us/netscaler-application-delivery-management-software/media/adc-metrics-gslb.png)

- ホスト名と現在のNetScalerスコアが表示されます。このスコアは、NetScalerのさまざまな潜在的な問題に基づいて計算されます。詳細については、「インスタンススコア」を参照してください。
- **IPアドレス** – NetScalerのIPアドレスを示します。
- **現在の状態** – NetScalerのステータス（Up、Down、Out of serviceなど）を示します。
- **NetScaler処理時間** – NetScalerインスタンスによる平均処理時間を示します。

**注**

ホスト名がNetScalerに割り当てられていない場合：

NetScaler IPアドレスがホスト名の代わりに表示されます。
メトリクスでは、NetScaler IPアドレス情報は表示されません。
ホスト名(/en-us/netscaler-application-delivery-management-software/media/hostname-gslb.png)

## サービスグラフ内のすべてのアプリケーションの全体像

**Applications** > **Service Graph** に移動し、**Global** をクリックします。

グローバルサービスグラフ(/en-us/netscaler-application-delivery-management-software/media/global-sg-view.png)

サービスグラフには、選択した期間について以下が表示されます。

- ユーザーが特定のアプリケーションにアクセスする地域

NetScalerインスタンスがホストされているデータセンター

- すべてのNetScalerインスタンスからの合計個別アプリケーション

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

**注**

NetScalerインスタンスに個別のアプリケーションがない場合、NetScalerインスタンスから個別仮想サーバーへの矢印エッジは表示されません。

- すべてのNetScalerインスタンスからの合計カスタムアプリケーション
- NetScaler CPXインスタンスからの合計マイクロサービスアプリケーション

## クライアントメトリクスの表示

クライアント領域にマウスポインターを合わせると、メトリクスが表示されます。

クライアントメトリクス(/en-us/netscaler-application-delivery-management-software/media/client-metrics.png)

- **クライアントネットワーク遅延** - 平均クライアントネットワーク遅延を示します。
- **クライアント4xxエラー** - 総クライアント4xxエラーを示します。
- **クライアントSSLエラー** - 総クライアントSSLエラーを示します。

## NetScalerの詳細を表示

サービスグラフを使用すると、以下を表示できます。

- データセンターとその合計NetScalerインスタンスがグループ化されています
- 各データセンターからのスコアの低い上位4つのNetScalerインスタンスのみ

**その他のADC**をクリックして、それぞれのステータス（重大、レビュー、良好、該当なし）タブを選択し、すべてのNetScalerインスタンスを表示します。

NetScalerインスタンスにマウスポインターを合わせると、メトリックが表示されます。

以下を表示できます。

- NetScalerインスタンスのIPアドレスとスコア
- **ホスト名** – NetScalerインスタンスに割り当てられているホスト名を示します
- **現在の状態** – NetScalerインスタンスの現在のステータス（稼働中、停止中、サービス停止中など）を示します。

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

- **主要な問題** – 現在のNetScalerスコアに影響を与える主要な問題を示します

**NetScalerインスタンス**をクリックして、インスタンススコア、主要メトリック、NetScalerインスタンスに関連する問題などのインスタンスの詳細を表示します。詳細については、インフラストラクチャ分析でインスタンスの詳細を表示するを参照してください。

## 個別のアプリケーションを表示

サービスグラフには、スコアの低い上位4つの個別のアプリケーションが表示されます。

以下の個別のアプリケーションがあるとします。

| アプリ名 | NETSCALER | アプリスコア | アプリステータス |
|---|---|---|---|
| App1 | 10.102.29.50 | 35 (クリティカル) | 稼働中 |
| App2 | 10.102.29.90 | 100 (良好) | ダウン |
| App 3 | 10.102.32.40 | 49 (確認) | アップ |
| App4 | 10.102.113.208 | 92 (良好) | ダウン |
| App5 | 10.102.25.25 | 86 (良好) | アップ |
| App6 | 10.102.29.41 | 77 (良好) | 稼働中 |
| App7 | 10.102.29.102 | 41 (要確認) | 稼働中 |

このシナリオでは、App1、App3、App6、App7をサービスグラフで上位4つの低スコアアプリケーションとして表示できます。

同様に、**カスタム**および**マイクロサービス**アプリケーションについても、上位4つの低スコアアプリケーションを表示することもできます。

サービスにマウスポインターを合わせると、メトリック情報を表示できます。

アプリケーションメトリック(/en-us/netscaler-application-delivery-management-software/media/app-metrics.png)

以下を表示できます:

- アプリケーション名とスコア
- **現在の状態** – アプリケーションの現在のステータス (稼働中または停止中など) を示します

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

- **問題** – アプリケーションに適用される問題の総数を示します
- **上位の問題** – アプリケーション全体のスコアに影響を与える上位の問題を示します

**その他** をクリックすると、すべての個別のアプリケーションが表示されます。次の図に示すように、個別の仮想サーバーページが表示されます。

すべてのアプリ(/en-us/netscaler-application-delivery-management-software/media/all-apps.png)

仮想サーバーはステータスに応じて表示されます。

- **合計** – 個別のアプリケーションの総数
- **重大** – アプリケーションスコアが0から40未満の場合
- **レビュー** – アプリケーションスコアが40から75未満の場合
- **良好** – アプリケーションスコアが75を超える場合
- **該当なし** – アプリケーションがどの仮想サーバーにもバインドされていない場合

各タブをクリックして仮想サーバーを表示できます。アプリケーションをクリックすると、選択したアプリケーションのサービスグラフが表示されます。

アプリのサービスグラフ(/en-us/netscaler-application-delivery-management-software/media/app-sg.png)

詳細については、「」(/ja-jp/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/service-graph-global-application.html#application-view) を参照してください。

## マイクロサービスアプリケーションを表示する

サービスグラフには、Kubernetesクラスターに属するすべてのマイクロサービスアプリケーションも表示されます。サービスにマウスポインターを合わせると、メトリックの詳細が表示されます。

表示できる項目は次のとおりです。

- サービス名
- サービスが使用するプロトコル（SSL、HTTP、TCP、SSL over HTTPなど）
- **ヒット数** – サービスが受信したヒットの総数
- **サービス応答時間** – サービスからの平均応答時間。

  （応答時間 = クライアントRTT + リクエスト最終バイト – リクエスト初回バイト）

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

- **エラー** – 4xx、5xxなどのエラーの総数
- **データ量** – サービスによって処理されたデータの総量
- **名前空間** – サービスの名前空間
- **クラスター名** – サービスがホストされているクラスター名
- **SSLサーバーエラー** – サービスからのSSLエラーの総数

サービスをクリックすると、選択したサービスのKubernetesサービスグラフが、サービスの名前空間とクラスター名のフィルターが適用された状態で表示されます。

Kubernetesサービス(/en-us/netscaler-application-delivery-management-software/media/k8s-service.png)

すべてのサービスを含むKubernetesサービスグラフを表示するには、**詳細**をクリックします。Kubernetesサービスグラフの詳細については、「クラウドネイティブアプリケーションのサービスグラフ」を参照してください。

Kubernetesのすべてのアプリ(/en-us/netscaler-application-delivery-management-software/media/k8s-all.png)

## 検索バーで結果をフィルタリング

検索バーを使用して結果をフィルタリングできます。管理者として、次のような場合に、この検索バーを使用すると、特定のインスタンス/クライアント/アプリケーション/データセンターにすばやく絞り込むことができます。

- 多数のデータセンターを持つ大規模なエンタープライズ
- 各データセンターに多数のNetScalerインスタンスを設定している
- 各NetScalerインスタンスを介して展開またはアクセスされる多数のアプリケーションを設定している
- 異なる場所からアプリケーションにアクセスするクライアント

検索バーにマウスポインターを置き、フィルタを作成したいカテゴリを選択します。

検索バー(/en-us/netscaler-application-delivery-management-software/media/search-bar-gsg.png)

例えば、特定のNetScalerインスタンスを表示したい場合は、検索バーから**インスタンス**を選択し、インスタンスのIPアドレスを選択します。グローバルサービスグラフには、選択したインスタンスと、それに関連するアプリケーション、データセンター、クライアントの場所が表示されます。

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

検索結果(/en-us/netscaler-application-delivery-management-software/media/search-results-gsg.png)

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

# StyleBooks

StyleBooksは、アプリケーションの複雑なNetScaler構成を管理するタスクを簡素化します。StyleBookは、NetScaler構成を作成および管理するために使用できるテンプレートです。NetScalerの特定の機能を構成するためのStyleBookを作成することも、Microsoft ExchangeやLyncなどのエンタープライズアプリケーション展開用の構成を作成するためにStyleBookを設計することもできます。

StyleBooksは、DevOpsチームが実践するInfrastructure-as-codeの原則によく適合します。そこでは、構成は宣言型であり、バージョン管理されています。構成は繰り返し使用され、全体として展開されます。StyleBooksには次の利点があります。

- **宣言型**: StyleBooksは、命令型ではなく宣言型の構文で記述されています。StyleBooksを使用すると、特定のNetScalerインスタンスで構成を実現するための段階的な手順ではなく、構成の結果または「望ましい状態」を記述することに集中できます。NetScaler Consoleは、NetScaler上の既存の状態と指定した望ましい状態との差分を計算し、インフラストラクチャに必要な編集を行います。StyleBooksはYAMLで記述された宣言型構文を使用するため、StyleBookのコンポーネントは任意の順序で指定でき、NetScaler Consoleは計算された依存関係に基づいて正しい順序を決定します。
- **アトミック**: StyleBooksを使用して構成を展開する場合、完全な構成が展開されるか、まったく展開されないかのいずれかであり、これによりインフラストラクチャは常に一貫した状態に保たれます。
- **バージョン管理**: StyleBookには、システム内の他のStyleBookと一意に区別する名前、名前空間、およびバージョン番号があります。StyleBookを変更するには、この一意性を維持するためにバージョン番号（または名前または名前空間）の更新が必要です。バージョン更新により、同じStyleBookの複数のバージョンを維持することもできます。
- **構成可能**: StyleBookが定義されると、そのStyleBookは他のStyleBookを構築するための単位として使用できます。構成の一般的なパターンを繰り返すことを避けることができます。また、組織内で標準的な構成要素を確立することもできます。StyleBooksはバージョン管理されているため、既存のStyleBooksへの変更は新しいStyleBooksを生み出し、その結果、依存するStyleBooksが意図せず破損することはありません。
- **アプリケーション中心**: StyleBooksは、完全なアプリケーションのNetScaler構成を定義するために使用できます。アプリケーションの構成は、パラメータを使用することで抽象化できます。したがって、StyleBookから構成を作成するユーザーは、いくつかのパラメータを入力するだけで、複雑なNetScaler構成を作成できるシンプルなインターフェイスを操作できます。

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

StyleBooksから作成された構成は、インフラストラクチャに縛られません。したがって、単一の構成を1つまたは複数のNetScalerに展開したり、インスタンス間で移動したりできます。

- **自動生成UI**: NetScaler Console GUIを使用して構成を行う場合、NetScaler ConsoleはStyleBookのパラメータを入力するために使用されるUIフォームを自動生成します。StyleBookの作成者は、新しいGUI言語を学習したり、UIページやフォームを個別に作成したりする必要はありません。
- **API駆動**: すべての構成操作は、NetScaler Console GUIまたはREST APIを使用してサポートされます。APIは同期モードまたは非同期モードで使用できます。構成タスクに加えて、StyleBooks APIを使用すると、実行時に任意のStyleBookのスキーマ（パラメータ記述）を検出することもできます。

1つのStyleBookを使用して複数の構成を作成できます。各構成はconfig packとして保存されます。たとえば、一般的なHTTP負荷分散アプリケーション構成を定義するStyleBookがあるとします。負荷分散エンティティの値を持つ構成を作成し、NetScalerインスタンスで実行できます。この構成はconfig packとして保存されます。同じStyleBookを使用して、異なる値を持つ別の構成を作成し、同じまたは異なるNetScalerインスタンスで実行できます。この構成のために新しいconfig packが作成されます。config packは、NetScaler Consoleと、構成が実行されたNetScalerインスタンスの両方に保存されます。

NetScaler Consoleに付属のデフォルトのStyleBooksを使用して展開用の構成を作成することも、独自のStyleBooksを設計してNetScaler Consoleにインポートすることもできます。StyleBooksを使用して構成を作成するには、NetScaler Console GUIを使用するか、APIを使用します。

このドキュメントには、次の情報が含まれています。

- StyleBookの表示方法
- デフォルトのStyleBook
- ビジネスアプリケーション向けに開発されたStyleBook(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/business-application-stylebooks.html)
- カスタムStyleBook(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks.html)
- StyleBookにおけるAPI(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks.html)
- StyleBookの文法(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar.html)

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

# StyleBookのカテゴリ

NetScaler Consoleには、デフォルトのStyleBookとカスタムStyleBookの2つのStyleBookカテゴリがあります。StyleBookは、デフォルトかカスタムかに関わらず、パブリックまたはプライベートのStyleBookのいずれかです。NetScaler Consoleでは、種類や表示ステータスに関係なく、システムに存在するすべてのStyleBookを表示できます。また、StyleBookが互いにどのように接続されているかをグラフィカルに表示することもできます。

このドキュメントでは、さまざまな種類のStyleBookについて説明します。また、NetScaler ConsoleからStyleBookに対して実行できる次のアクションについても説明します。

- カスタムStyleBookをダウンロードして変更を加えるか、既存のStyleBookに基づいてStyleBookを作成します。
- デフォルトのStyleBookを非表示にします。
- NetScaler Consoleからカスタム StyleBookを削除します。
- StyleBookにタグを追加します。

## デフォルトおよびカスタムStyleBook

- **デフォルトのStyleBook**は、NetScaler Consoleに付属しているStyleBookであり、NetScalerインスタンスに展開できる構成を作成できます。デフォルトのStyleBookを削除することはできませんが、NetScaler Console GUIから非表示にすることができます。
- **カスタムStyleBook**は、NetScaler Consoleにインポートした独自のStyleBookです。

デフォルトのStyleBookとカスタムStyleBookはどちらも、パブリックまたはプライベートにすることができます。

## パブリックおよびプライベートStyleBook

設定パックを作成できるStyleBookは、**パブリック**StyleBookとして分類できます。つまり、NetScaler Console GUIおよびAPIから構成を作成するために、すべて直接使用できます。

しかし、一部のStyleBookは他のStyleBookの構成要素として使用されます。このようなStyleBookは**プライベート**としてマークされます。プライベートStyleBookは、NetScaler Console GUIから設定パックを直接作成するために使用することはできません。ただし、これらのStyleBookをNetScaler Consoleに表示して確認することはできます。カスタムStyleBookのいずれかを**プライベート**としてマークするには、StyleBookのプライベート属性を**true**に設定します。プライベートStyleBookは、NetScaler Console APIを使用して設定パックを作成するために引き続き使用できます。

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

### プライベートとしてマークされたStyleBookの例

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

private: true
```

## StyleBookの表示

NetScaler Consoleでは、デフォルトとプライベートの両方のStyleBookの数が増加しています。アクセスしたい特定のStyleBookを検索したい場合があります。また、両方のタイプのStyleBookを個別に表示したい場合もあります。

NetScaler Consoleで、**Applications** > **StyleBooks** に移動すると、システムに存在するStyleBookのリストを表示できます。

デフォルトのパブリックStyleBookには、そのパネルに次のアイコンがあります。



一方、デフォルトのプライベートStyleBookには、それがプライベートStyleBookであることを示すアイコンがあります。



プライベートStyleBookの定義と依存関係は表示できますが、GUIを使用してプライベートStyleBookから構成パックを作成することはできません。プライベートStyleBookの主な目的は、別のStyleBookの構成要素として使用することです。構成要素となるStyleBookを使用することで、一般的な構成パターンを再利用できます。

カスタムのパブリックStyleBookには、次の図に示すように異なるアイコンがあります。



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

一方、カスタムのプライベートStyleBookは、このアイコンで表示されます。

ページの右上には、表示するStyleBookのタイプを選択するオプションがあります。「すべて」、「パブリック」、または「プライベート」の3つのオプションがあります。いずれかのオプションをクリックします。

検索アイコンをクリックして、特定のStyleBookを検索することもできます。名前、名前空間、バージョン属性、またはこれらのオプションの組み合わせで検索できます。検索操作では大文字と小文字は区別されません。

## カスタムStyleBookをダウンロード

NetScaler ConsoleからカスタムStyleBookをダウンロードするには、**Applications** > **StyleBooks** > **Configurations**の順に移動します。右側のパネルに表示されるStyleBookのリストで、カスタム定義のStyleBookをダウンロードするオプションをオンにします。**Download**をクリックします。StyleBookに依存するカスタムStyleBookがある場合は、依存するStyleBookをダウンロードしたバンドルに含めることができます。

**注:**

パブリックまたはプライベートとしてマークされているカスタムStyleBookをダウンロードできます。

**注:**

デフォルトのStyleBookはダウンロードできません。それらの定義と依存関係を表示できます。これを行うには、StyleBookパネルの**View Definition**および**View Dependencies**リンクをクリックします。

## カスタムStyleBookを更新

NetScaler Console GUI自体からカスタムStyleBookの定義を更新できます。これにより、バージョンを変更せずにStyleBookに変更を加えることができます。StyleBookバンドルからインポートされた定義を更新することもできます。

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

**重要:**

- NetScaler Console GUIからStyleBook定義を更新する前に、StyleBook定義に依存するStyleBookがないことを確認してください。
- 設定パックを持つStyleBook定義を更新できます。
- StyleBook定義が下位互換性があることを確認してください。既存のStyleBookのすべてのパラメータは更新されたStyleBookに保持され、追加されたパラメータはオプションとして表示されます。

1. **Applications > Configuration > StyleBooks**の順に移動します。
2. 「**カスタムStyleBook**」タブを選択します。
3. 更新するStyleBookで「**定義の更新**」を選択します。
4. 必要に応じて定義を更新し、「**更新**」をクリックします。

   カスタムStyleBookを更新(/en-us/netscaler-application-delivery-management-software/media/update-stylebook-definition-inline.gif)
5. ページを更新して最新の変更を確認します。

## カスタムStyleBookを削除する

「**削除**」ボタンをクリックして、カスタムStyleBookを削除することもできます。ポップアップウィンドウが表示され、NetScaler ConsoleからStyleBookを削除するかどうかを確認するメッセージが表示されます。StyleBookが他のカスタムStyleBookを使用している場合は、チェックボックスをオンにして、それらのStyleBookを削除することを選択できます。

StyleBookを削除(/en-us/netscaler-application-delivery-management-software/media/mas-delete-custom-stylebooks-new.png)

「

**注:**

」:

NetScaler Consoleに依存するStyleBookがある場合は、カスタムStyleBookを削除しないでください。削除すると、既存のStyleBookが破損します。

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

## StyleBookの依存関係を表示する

StyleBookの重要かつ強力な機能の1つは、他のStyleBookの構成要素として使用できることです。あるStyleBookを別のStyleBookにインポートできます。インポートされたStyleBookはタイプとして宣言され、2番目のStyleBookのコンポーネントまたはパラメータによって使用されます。NetScaler Consoleの既存のデフォルトStyleBookを調べて、あるStyleBookが別のStyleBookの上にどのように構築できるかを学ぶことができます。

NetScaler Consoleでは、StyleBookが互いにどのように接続されているかをグラフィカルに表示できます。この表現は、他のStyleBookを構成要素として使用して構築された複雑なStyleBookにとって特に役立ちます。依存関係グラフを見ることで、複数のStyleBook間の関係と依存関係を確認できます。

他のStyleBookで使用されているStyleBookは、既存のStyleBookを破損させるため、システムから削除できません。依存関係グラフ表示を使用すると、どのStyleBookがStyleBookの削除を妨げているかを特定できます。

### StyleBookの依存関係を表示するには

NetScaler Consoleで、**Applications** > **StyleBooks**に移動します。StyleBooksページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、目的のStyleBookを見つけます。**StyleBook**タイルには、構成の作成、StyleBook定義の表示、およびStyleBookの依存関係の表示へのリンクが表示されます。**View Dependencies**をクリックします。

## 順方向の依存関係

**Forward Dependencies**タブでは、お使いのStyleBookが使用しているさまざまなデフォルトのStyleBookを表示できます。矢印をたどって、StyleBookが使用しているStyleBookを見つけます。いずれかの矢印にマウスを合わせると、その矢印と相互に接続されているStyleBookが強調表示されます。StyleBook名をクリックして、そのStyleBookの定義を表示することもできます。

順方向の依存関係(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebooks-forward-dependencies.png)

## 逆方向の依存関係

**Reverse Dependencies**タブでは、お使いのStyleBookを使用しているStyleBookをグラフィカルに表示できます。矢印をたどると、表示されているすべてのStyleBookがお使いのStyleBookを指していることがわかります。一部のStyleBookは直接StyleBookを使用している場合があり、一部のStyleBookは別のStyleBookを介してStyleBookを使用している場合があります。

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

逆方向の依存関係(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebooks-reverse-dependencies.png)

## 設定パックに対するNetScaler構成の監査

StyleBook設定パックによって行われた変更を、現在のNetScaler構成と比較できます。この比較により、次のことができます。

- StyleBook設定パックとNetScaler構成間の設定ドリフトを検出します。
- 設定パックによって行われた変更を反映していない、NetScaler上の変更済みおよび削除済みオブジェクトを特定します。

設定パックの変更をNetScaler構成と比較するには、次の手順を実行します。

1. **Applications** > **StyleBooks** > **Configurations**に移動します。
2. **Configuration Audit**をクリックします。

   **Configuration Audit**ページには、作成および監査されたオブジェクトが表示されます。

   構成パックに対するNetScaler構成の監査(/en-us/netscaler-application-delivery-management-software/media/configuration-audit-configpack.png)

## 構成パックのサポートバンドルをダウンロードする

構成パックのサポートバンドルは、NetScaler®テクニカルサポートチームが構成パックの問題を表示、分析、トラブルシューティングするのに役立ちます。

1. **Applications > Configuration > Config Packs > Support Bundles**で、構成パックを選択します。**Download**をクリックします。
2. **Download Support Bundle**ページで、以下を指定します。
   - **パスフレーズを使用して構成データを暗号化する** - バンドルファイルを暗号化するためのパスフレーズを指定する場合は、このオプションを選択します。
   - **パスフレーズ** - エクスポートバンドルを暗号化するためのパスフレーズを指定します。このパスフレーズは、構成パックの機密データを保護します。パスフレーズは20文字以上である必要があります。
   - **圧縮ファイルタイプ** - バンドルをZIPまたはTGZファイル形式で圧縮できます。
3. **Download**をクリックします。

サポートバンドル(/en-us/netscaler-application-delivery-management-software/media/support-bundle-configpack.png)

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

## StyleBookのタグを作成する

NetScaler Consoleの任意のStyleBookにタグを追加できます。タグは、さまざまな基準を使用してStyleBookをグループ化できるキーと値のペアです。NetScaler ConsoleでStyleBookを検索またはフィルタリングする際に、これらのタグを使用できます。

StyleBookにタグを追加するには：

1. **Applications** > **StyleBooks**に移動します。
2. タグを追加したいStyleBookで**Tags**を選択します。

   すべての種類のStyleBookにタグを追加できます。
3. StyleBookのフィルタリングに役立つ、必要な**キー**と**値**の情報を指定します。

   例えば、Key=team と Value=bizdata

   さらにタグを追加するには、**+**をクリックします。
4. **作成**をクリックします。

検索バーでタグを使用してStyleBookをフィルタリングするには、**タグ**をクリックし、リストからキーと値を選択します。指定されたタグに一致するStyleBookが表示されます。

以下は、`key=team`および`value=bizdata`のタグを持つStyleBookの検索例です。

StyleBookタグをそのconfig packに関連付けることができます。そのため、StyleBookタグ自体を使用してconfig packを検索できます。

config packを作成する際は、**タグ関連付け**セクションで以下のいずれかのオプションを使用します。

- **現在および将来のすべてのStyleBookタグを構成に関連付ける** – このオプションは、すべてのStyleBookタグをconfig packに関連付けます。また、将来StyleBookに追加する可能性のある新しいタグも関連付けられるようにします。
- **タグを選択** – このオプションは、選択したStyleBookのタグを表示します。必要なStyleBookタグを選択し、config packに関連付けることができます。

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

## CLIコマンドを使用してStyleBookを設定するには

CLIコマンドを使用してStyleBookを設定する場合は、次の手順を実行します。

- NetScalerで`show ns runningConfig`コマンドを実行します。
- NetScaler Consoleで、デフォルトのStyleBook、ビジネスアプリケーションのStyleBook、またはカスタムのStyleBookのいずれかを使用して構成を作成します。
- NetScalerで`show ns runningConfig`コマンドを再度実行します。

2つの出力の差分は、NetScaler CLIを使用してStyleBookを設定するために使用できるCLIコマンドを表示します。

## StyleBookをクローンする

管理者は、StyleBookとその依存StyleBookの複製を作成できます。このバンドルは、`parameters`セクションと`components`セクションの更新などのカスタマイズに使用できます。

StyleBookをクローンするには：

1. **Applications > Configuration > StyleBooks** に移動します。
2. 複製したいデフォルトまたはカスタムのStyleBookで、**Clone** を選択します。

   
3. **Clone StyleBook** ページで、StyleBookと依存StyleBookのネームスペースとバージョンを入力します。推奨されるネームスペースとバージョンを選択することもできます。

   

   **注：**

   クローンされたStyleBookとその依存するStyleBookは、既存のStyleBookと区別するために、異なる名前空間とバージョンを持つ必要があります。クローンされたStyleBookに対して、予約済みのNetScaler Console名前空間を使用することはできません。
4. 「**クローン**」をクリックします。クローンされたStyleBookパッケージはNetScaler Consoleにインポートされ、「**StyleBooks**」ページに表示されます。

# 外部リポジトリからStyleBookをインポートして同期する

開発にCI/CDプロセスを使用しているシナリオ、またはすべてのアプリケーションソースコードとデプロイオブジェクトをGitHub/GitLabで管理しているシナリオを検討してください。

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

GitHub/GitLabリポジトリでは、NetScaler構成をデプロイし、これらのStyleBookを管理するためにいくつかのStyleBookを作成している場合があります。これらのStyleBookはNetScaler Consoleでも必要です。これで、これらのStyleBookをNetScaler Consoleに直接インポートできます。GitHub/GitLabから手動でコピーしてNetScaler Consoleにアップロードしたり、NetScaler ConsoleとGitHub/GitLabの両方でファイルを手動で同期したりする必要はありません。

StyleBookと構成パックをインポートするには、GitHub/GitLabリポジトリを表すリポジトリをNetScaler Consoleで定義します。GitHub/GitLabリポジトリのURLと、GitHub/GitLabで作成したユーザー名とAPIまたは個人アクセストークン (PA) を指定します。つまり、GitHub/GitLabで有効なアカウントを持つ承認済みユーザーのみがStyleBookをインポートおよび同期できます。

次のタイプのリポジトリをインポートおよび同期できます。

- **公開アクセス可能なリポジトリ** - 一般に公開されており、インターネット経由でアクセスできるリポジトリ。
- **オンプレミスまたはプライベートなGitLab/GitHubリポジトリ** - プライベートにホストされており、通常は企業のイントラネット内でのみアクセスできるリポジトリ。これらのリポジトリの場合、登録プロセス中にNetScalerエージェントを選択する必要があります。NetScalerエージェントは、企業のイントラネット内のリポジトリにアクセスするためのプロキシとして機能します。

リポジトリを作成した後、NetScaler ConsoleをGitHub/GitLabリポジトリと同期できます。NetScaler ConsoleはGitHub/GitLabに接続し、そのリポジトリで見つかったStyleBookをインポートします。その後、NetScaler ConsoleはStyleBookを検証し、NetScaler ConsoleのStyleBookリストに追加します。検証に失敗したStyleBookはNetScaler Consoleに追加されません。エラーを修正し、更新されたバージョンをGitHub/GitLabリポジトリにコミットしてください。後で、それらをNetScaler Consoleに再度インポートまたは同期を試すことができます。

**注**

- StyleBookファイルは、GitHub/GitLabリポジトリの任意のブランチからインポートおよび同期できます。
- 依存するStyleBookが関連付けられているStyleBookもインポートおよび同期できます。
- The synchronization of StyleBooks from a GitHub/GitLab repository must be initiated manually from the NetScaler Console GUI or API. That is, currently, importing and syncing of StyleBooks does not happen automatically based on GitHub/GitLab commit activity.

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

## リポジトリを追加し、外部リポジトリからStyleBookをインポートする

開始する前に、GitHub/GitLabで有効なアカウントを持っていることを確認してください。

GitHub/GitLabリポジトリ内の任意のフォルダーからNetScaler ConsoleにStyleBookファイルをインポートできます。

1. NetScaler Consoleで、**Applications** > **StyleBooks** > **Repositories** に移動します。
2. **Add** をクリックします。**Add Repository** ウィンドウで、次のパラメータを入力します。
   - **名前**。リポジトリの名前を入力します。この名前は、GitHub/GitLabのリポジトリ名と同じでも、異なるものでも構いません。
   - **リポジトリURL** - GitHub/GitLabリポジトリのURLを入力します。

     GitHub/GitLabエンタープライズURLを指定できます。これにより、GitHub/GitLabエンタープライズアカウントからStyleBookと設定パックをインポートまたは同期できます。
   - **プライベートURLですか？** - リポジトリがオンプレミスまたはプライベートのGitLab/GitHubリポジトリである場合は、このチェックボックスを選択し、**Agent** を選択します。
   - **ユーザー名とパスワード**。GitHub/GitLabアカウントにアクセスするためのユーザー名とパスワードを入力します。

   **注**

   パスワードの代わりにAPIトークンを指定することもできます。APIトークンは、HTTPS経由でGitHub/GitLabのパスワードの代わりに使用できます。GitHub/GitLabリポジトリのAPI/PAトークンの作成方法については、個人アクセストークンの作成に関するGitHub/GitLabのドキュメントを参照してください。
3. **Create** をクリックします。

   リポジトリがNetScaler Consoleに作成されます。
4. StyleBookをインポートまたは同期するには、**Repositories** ページでリポジトリを選択し、**Sync** をクリックします。

ここで使用できるその他のアクションは次のとおりです。

- **編集**。リポジトリのURL、ユーザー名、パスワード（またはAPIトークン）を編集できます。

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

- **削除**。NetScaler Consoleに存在する、以前そのGitHub/GitLabリポジトリからインポートされたすべてのStyleBookとともに、リポジトリを削除できます。

  **注**

  関連付けられたConfigPackを持つStyleBookが存在する場合、NetScaler Consoleからリポジトリを削除することはできません。まず、これらのStyleBookのすべてのConfigPackを削除してください。その後、NetScaler Consoleからリポジトリを削除して、そのリポジトリからStyleBookをクリーンアップできます。

- **リセット**。NetScaler Consoleからリポジトリのエントリを実際に削除することなく、そのリポジトリから同期されたNetScaler Console内のすべてのStyleBookを削除できます。
- **ファイルの一覧表示**。GitHub/GitLabリポジトリから取得された、NetScaler Consoleに存在するすべてのStyleBookのリストを表示できます。

### GitHub/GitLabからStyleBookとConfigPackをインポートする手順

前提条件を完了したら、以下の手順に従ってGitHub/GitLabリポジトリからStyleBookとConfigPackをインポートします。

1. オプション: リポジトリを追加していない場合は追加します。
2. 「リポジトリ」ページでリポジトリを選択します。
3. **同期**をクリックします。

## デフォルトのStyleBookを使用する

NetScaler Consoleには、一連のデフォルトのStyleBookが用意されています。デフォルトのStyleBookを使用する場合、そのStyleBook内のパラメータの値を指定し、構成を実行したいNetScalerインスタンスのIPアドレスを選択する必要があります。構成を送信すると、NetScaler Consoleは指定されたパラメータ値を検証し、構成のグラフを作成し、NetScalerインスタンスに接続して、インスタンス上で構成を実行します。

### デフォルトのスタイルブックから構成を作成するには

1. 「**Applications** > **Configurations > StyleBooks**」に移動します。スタイルブックページには、NetScaler Console内のすべてのスタイルブックが表示されます。このリストには、デフォルトのスタイルブックとカスタムのスタイルブックの両方が含まれます。検索フィールドにスタイルブックの名前を入力し、**Enter**キーを押すことができます。または、リストをスクロールしてスタイルブックを見つけることもできます。

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

2. **Create Configuration** をクリックします。パラメータに必要な値を指定します。

   **注:**

   構成パラメータと値は、選択したスタイルブックによって異なる場合があります。

3. 「**Target Instances**」で、構成を実行するNetScalerインスタンスのIPアドレスをクリックして選択します。この構成を複数のインスタンスで実行する場合は、「+」をクリックしてインスタンスを追加します。

   **NetScaler Console** > **Settings > Change System Settings** > **Modify System Settings** で **Prompt Credentials for Instance Login** オプションが有効になっている場合、選択したNetScalerインスタンスで構成を実行する際に、NetScalerインスタンスの資格情報の入力を求められます。それ以外の場合、NetScaler Consoleはインスタンスプロファイルに保存されているインスタンス資格情報を使用してインスタンスにログインします。

   **Prompt credentials for StyleBook Operations** を有効にするには、次の手順に従います。

   a. **Settings > Administration** に移動します。
   b. 「**システム管理**」ページで、「**システム設定**」の下にある「**システム、タイムゾーン、許可されたURL、およびエージェント設定**」を選択します。
   c. 「**システム構成**」ページで、「**システム設定**」の下にある「**インスタンスログインの資格情報を要求**」と「**StyleBook操作の資格情報を要求**」を選択します。
   d. **Save** をクリックします。

   システム設定(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebooks-user-credentials-instance-2.png)

   リリース 14.1 ビルド 25.x 以降、選択したすべてのNetScalerインスタンスの資格情報を指定できます。

   2つ以上のNetScalerインスタンスを選択し、「**すべてのインスタンスに同じ資格情報を使用**」を選択すると、選択したNetScalerインスタンスに同じ資格情報を適用できます。

   インスタンスの資格情報(/en-us/netscaler-application-delivery-management-software/media/instance_login.png)

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

NetScalerインスタンスで設定を実行する前にテストまたは検証したい場合は、「**ドライラン**」を選択し、「**作成**」をクリックします。設定が有効な場合、指定した値に基づいて作成されたオブジェクトが表示されます。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/stylebooks_objects_added.png)

4. 「**ドライラン**」チェックボックスをオフにし、「**作成**」をクリックして、設定を作成し、NetScalerインスタンスで設定を実行します。作成したStyleBook設定は、以下に示すように設定リストに表示されます。

> **注:**
>
> 更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスをこのウィンドウの利用可能なインスタンスリストに追加することもできます。

NetScaler Consoleを使用して、この設定パックを検査、更新、または削除できます。

## WebアプリケーションファイアウォールStyleBook

NetScaler Web App Firewallは、Webアプリケーションとサイトを、既知および未知の攻撃、すべてのアプリケーション層およびゼロデイの脅威から保護するWebアプリケーションファイアウォール (WAF) です。

NetScaler Consoleでは、NetScalerインスタンス上でアプリケーションファイアウォール構成をより便利に作成できるデフォルトのStyleBookが提供されるようになりました。

### アプリケーションファイアウォール構成の展開

以下のタスクは、ビジネスネットワーク内のNetScalerインスタンスに、アプリケーションファイアウォールおよびIPレピュテーションポリシーとともに負荷分散構成を展開するのに役立ちます。

**アプリケーションファイアウォール設定でLB構成を作成するには：**

1. NetScaler Consoleで、**Applications** > **Configurations** > **StyleBooks**に移動します。StyleBooksページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、アプリケーションファイアウォールポリシーとIPレピュテーションポリシーを含むHTTP/SSL負荷分散StyleBookを見つけます。名前を`lb-appfw`と入力してStyleBookを検索することもできます。**Create Configuration**をクリックします。

   StyleBookはユーザーインターフェイスページとして開き、このStyleBookで定義されているすべてのパラメーターの値を入力できます。

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

2. 以下のパラメーターの値を入力します。

   - **Load Balanced Application Name**。ネットワークに展開するアプリケーションファイアウォール付きの負荷分散構成の名前。
   - **Load balanced App Virtual IP address**。NetScalerインスタンスがクライアント要求を受信する仮想IPアドレス。
   - **Load Balanced App Virtual Port**。ユーザーが負荷分散されたアプリケーションにアクセスする際に使用するTCPポート。
   - **Load Balanced App Protocol**。リストからフロントエンドプロトコルを選択します。
   - **Application Server Protocol**。アプリケーションサーバーのプロトコルを選択します。

   ☐

3. オプションとして、**Advanced Load Balancer Settings** を有効にして構成できます。

   高度なロードバランサー設定を指定する (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-2.png)

4. オプションで、ロードバランシング仮想サーバーのトラフィックを認証するための認証サーバーを設定することもできます。

   オプション、高度なロードバランサー仮想サーバー (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-3.png)

5. サーバーIPとポートのセクションで「+」をクリックして、アプリケーションサーバーとアクセス可能なポートを作成します。

   IPとポートの詳細を指定する (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-4.png)

6. アプリケーションサーバーのFQDN名を作成することもできます。

   アプリケーションサーバーのFQDN名を作成する (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-5.png)

7. SSL証明書の詳細を指定することもできます。

   アプリケーションサーバーにSSL証明書の詳細を指定する (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-6.png)

8. ターゲットのNetScalerインスタンスでモニターを作成することもできます。

   ターゲットインスタンスでモニターを作成する (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-7.png)

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

9. 仮想サーバーでアプリケーションファイアウォールを構成するには、WAF設定を有効にします。

   アプリケーションファイアウォール設定をそのVIP上のすべてのトラフィックに適用したい場合は、アプリケーションファイアウォールポリシー規則がtrueであることを確認してください。そうでない場合は、アプリケーションファイアウォール設定を適用するリクエストのサブセットを選択するためにNetScalerポリシー規則を指定します。次に、適用するプロファイルの種類（HTMLまたはXML）を選択します。

   WAF設定を有効にする (/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-8.png)

10. オプションで、アプリケーションファイアウォールプロファイル設定チェックボックスを有効にすることで、詳細なアプリケーションファイアウォールプロファイル設定を構成できます。
11. オプションで、アプリケーションファイアウォール署名を設定する場合は、仮想サーバーが展開されるNetScalerインスタンスで作成された署名オブジェクトの名前を入力します。

    **注:**

    このStyleBookを使用して署名オブジェクトを作成することはできません。

12. 次に、StartURL設定、DenyURL設定などの他のアプリケーションファイアウォールプロファイル設定も構成できます。

    アプリケーションファイアウォールと構成設定の詳細については、「Application Firewall」を参照してください。

13. **ターゲットインスタンス**セクションで、アプリケーションファイアウォールを使用して負荷分散仮想サーバーを展開するNetScalerインスタンスを選択します。

    **注:**

    更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを、このウィンドウで使用可能なインスタンスのリストに追加することもできます。

14. また、不要なリクエストを送信しているIPアドレスを特定するために、**IPレピュテーションチェック**を有効にすることもできます。IPレピュテーションリストを使用して、評判の悪いIPからのリクエストを事前に拒否できます。
15. **作成**をクリックして、選択したNetScalerインスタンスに構成を作成します。

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

**ヒント**

インスタンスで実際の構成を実行する前に、ターゲットインスタンスで作成する必要がある構成オブジェクトを確認するために、**ドライラン**を選択することをお勧めします。

構成が正常に作成されると、StyleBookは必要な負荷分散仮想サーバー、アプリケーションサーバー、サービス、サービスグループ、アプリケーションファイアウォールラベル、アプリケーションファイアウォールポリシーを作成し、それらを負荷分散仮想サーバーにバインドします。

以下の図は、各サーバーで作成されたオブジェクトを示しています。



16. NetScaler Consoleで作成されたConfigPackを表示するには、**Applications** > **Configurations** に移動します。



## すべてのデフォルトStyleBookを非表示にする

NetScaler Consoleは、NetScaler Consoleフォルダーシステムに存在するすべてのStyleBookを一覧表示します。StyleBookのリストには、プライベートとパブリックの両方になり得るデフォルトおよびカスタムのStyleBookが含まれます。管理者として、すべてのデフォルトStyleBookを非表示にしたい場合があります。ユーザーには、作成者またはユーザーが作成したカスタムStyleBookのみを表示およびアクセスさせることができます。

NetScaler Consoleでは、カスタムStyleBookを表示し、NetScaler Consoleに付属するすべてのデフォルトStyleBookを非表示にすることができます。すべてのデフォルトStyleBookを非表示にできる新しいGUIオプションが提供されています。

**すべてのデフォルトStyleBookを非表示にするには**:

1. NetScaler Consoleで、**Applications** > **Configurations > Settings** の順に移動します。
2. **Settings** ページには、デフォルトStyleBookがユーザーに表示されるかどうかに関する情報が表示されます。
3. デフォルトStyleBookを非表示にするには、右上にある編集アイコンをクリックします。
4. **Configure StyleBook Settings** ページで、**Hide Default StyleBooks** オプションを選択します。
5. **OK** をクリックします。

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



RBAC機能を使用してページを非表示にすることを選択していない場合、**Configure StyleBook Settings** ページは引き続きユーザーに表示されます。ユーザーは、デフォルトStyleBookを再表示するオプションをまだ持っている可能性があります。

**Configure StyleBook Settings** ページを非表示にするには、ポリシーを作成し、そのポリシーをデフォルトStyleBookを表示すべきではないユーザーに割り当てる必要があります。

**RBACポリシーを作成するには**:

1. NetScaler Consoleで、**Account** \> **User Administration** \> **Access Policies** の順に移動します。
2. **Add** をクリックしてポリシーを作成します。
3. ポリシー名を入力します。
4. 「**権限**」セクションで、「**すべて**」>「**アプリケーション**」>「**構成**」>「**設定**」が選択されていないことを確認し、「**OK**」をクリックします。

ポリシーを作成したら、ロールを作成し、各ロールを1つ以上のポリシーにバインドし、ユーザーグループにロールを割り当てる必要があります。ポリシーをユーザーに関連付ける方法の詳細については、「ロールベースのアクセス制御の構成」を参照してください。

## PrometheusアナリティクスStyleBook

NetScalerでアナリティクスプロファイルを作成し、スキーマファイルを指定することで、NetScalerからPrometheusにメトリクスをエクスポートできます。StyleBookでは、`Prometheus TimeSeries Analytics Configuration` StyleBookを使用して、すべての管理対象インスタンスに構成を実行できます。

### 前提条件

管理対象のNetScalerインスタンスが**13.1 build 39-27以降**であることを確認してください。

`Prometheus TimeSeries Analytics Configuration` StyleBookを使用して構成するには：

1. **Applications** > **Configurations** > **StyleBooks** に移動し、`Prometheus TimeSeries Analytics Configuration` と名前を入力してStyleBookを検索し、**Create Configuration** をクリックします。
2. **構成パックの詳細**で：
   a. アナリティクスプロファイル名を指定します。詳細については、「メトリクスコレクターの構成」を参照してください。

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

b. **カウンター・スキーマ・ファイル：**

- デフォルトのスキーマを続行する場合は、この手順をスキップできます。
- カスタムスキーマを続行する場合は、パラメータを変更したスキーマファイルをアップロードします。NetScalerでは、サポートされているすべてのカウンターを含む参照ファイル `reference_schema.json` がパス `/var/metrics_conf/` の下にあります。FTPクライアントを使用して、ファイルをローカルにコピーできます。

3. **Target Instances** で、構成を実行するインスタンスまたはインスタンスグループを選択します。
4. **Tag Association** で、現在および将来のすべてのStyleBookタグを構成に関連付けます。

   このオプションは、すべてのStyleBookタグを構成パックに関連付けます。また、将来StyleBookに追加する可能性のある新しいタグも関連付けられるようにします。

   **注記：**

   NetScaler®インスタンスから作成、変更、または削除される結果を表示するには、「**ドライラン**」をクリックします。

5. 構成を実行するには、「**作成**」をクリックします。

# StyleBooks Configuration Builderを使用したNetScaler®アプリケーション構成の移行

StyleBooks Configuration Builderは、既存のNetScaler構成からアプリケーション構成StyleBookを作成するために使用されます。この機能は、アプリケーション構成をあるNetScalerインスタンスから別のインスタンスへ移行する作業も自動化します。

Configuration Builderを使用すると、StyleBookの文法や構成要素に関する深い理解がなくても、カスタマイズされたStyleBookの作成プロセスを効率化できます。そうでない場合、StyleBookを作成するには、StyleBookの文法と構成要素に精通している必要があります。

Configuration Builderは、あるNetScalerインスタンスの構成を別のNetScalerインスタンスに複製できる構成パックも作成します。初期構成ソースは、次のいずれかになります。

- **NetScalerインスタンス:** 複製したいアプリケーション構成が利用可能なインスタンスを指定します。

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

ターゲットインスタンスを指定しない場合でも、Configuration BuilderはNetScaler構成をStyleBookと構成パックに変換します。後でこの構成パックを使用して、NetScaler構成を他のNetScalerインスタンスに移行できます。

- **CLIコマンドのセット:** `ns.conf` または `Application config` から構成を貼り付けます。
- **構成ファイルのアップロード:** ローカルマシンから構成をアップロードします。

Configuration Builderは、ソース構成に埋め込まれた個別のアプリケーションのリストを識別します。関心のあるアプリケーション構成を選択すると、Configuration Builderは選択したアプリケーションのCLIコマンドのセットを抽出します。これらのCLIコマンドはソース構成から抽出されます。また、入力が必要となる可能性のある展開属性と構成属性も識別します。

- **アプリケーション展開情報** - 仮想サーバー、サービス、サービスグループメンバーのIPアドレスとポートを元の構成から表示および編集できます。仮想サーバーの状態とARPも表示および編集できます。
- **構成属性** - これらの属性は、ソース構成で指定されたパスワードまたは証明書である場合があります。

必要な情報を指定した後、ターゲットのNetScalerインスタンスでアプリケーション構成の移行または複製を開始します。

アプリケーションの作成と移行が完了すると、対応するStyleBookとともに構成パックがNetScaler Consoleに作成されます。この構成パックは、ターゲットのNetScalerインスタンス上のアプリケーション構成を表します。作成された構成パックを表示するには、**Applications** > **StyleBooks** > **Configurations** に移動します。

## 移行された構成間での構成エンティティの共有

Config Migrationユーティリティを使用して構成を移行する際に、構成エンティティを再利用できます。その後の移行では、既存の構成エンティティが正常に再利用されます。以前は、一部の構成エンティティを共有する2つの構成を移行する際に、**Resource already exists**というエラーで構成の移行が失敗していました。このオプションにより、複数の構成で構成エンティティが使用されるシナリオで構成エンティティの再利用が可能になり、移行ワークフローが効率化されます。

## サポートされているNetScaler機能

StyleBook Configuration Builderは、ソース構成で以下のNetScaler機能を認識し、サポートしています。

- アナリティクス

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

- AppFlow®
- アプリケーションレベルのQuality of Experience構成 (AppQoE)
- 認証と承認
- 監査
- ボット管理
- キャッシュリダイレクト
- コンテンツスイッチング
- DNS
- フロントエンド最適化
- HTTP圧縮
- 統合キャッシュ
- ロードバランシング
- モニタリング
- QUICプロトコル
- レート制限
- レスポンダー
- リライト
- SSLオフロード
- スピルオーバー
- トラフィック管理
- URL変換
- Webアプリケーションファイアウォール (WAF)

## NetScalerアプリケーション構成を移行するためのStyleBookを作成する

NetScaler ConsoleでNetScalerアプリケーション構成を移行するStyleBookを作成する手順は次のとおりです。

1. **アプリケーション** > **構成** > **Config Packs** の順に移動します。
2. **NetScaler構成の移行** をクリックします。
3. 「**開始**」をクリックします。

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

4. 「**構成の指定**」で、次の構成ソースのいずれかを選択します。

   - 「**NetScalerからインポート**」:
     - 「**ソースNetScalerインスタンス**」 - アプリケーション構成を移行または複製するNetScalerインスタンスを選択します。「**OK**」をクリックします。
   - 「**CLIコマンドを使用してインポート**」 - 構成ファイルから構成を貼り付けます。
   - 「**構成ファイルのアップロード**」 - 「**参照**」をクリックして、ローカルマシンから構成ファイルを選択します。

   「**ターゲットインスタンス**」 - アプリケーション構成を移行または複製するNetScalerインスタンスまたはオートスケールグループのいずれかを選択します。「**OK**」をクリックします。

   「**次へ**」をクリックします。

5. 「**高度なポリシー構成**」で、構成に応じて、次のシナリオが発生します。

   - 構成内の既存のすべてのクラシックポリシーは、エラーなしで高度なポリシーに正常に変換されます。更新された構成を確認し、確認を選択します。「**次へ**」をクリックします。
   - 構成内の既存のすべてのクラシックポリシーは、エラーを伴って高度なポリシーに正常に変換されます。エラーを確認して修正します。「**戻る**」をクリックします。
   - クラシックポリシーがない場合、構成は更新されません。「**OK**」をクリックして続行します。

6. 「**アプリケーションの定義**」で、,

   a. 「**アプリケーション名**」で、アプリケーションの名前を指定します。
   b. 移行する仮想サーバーを選択します。
   c. 「**次へ**」をクリックします。

7. 「**アプリケーション構成**」で、アプリケーションのコマンドを確認します。これらのコマンドは、選択したアプリケーション構成に固有のものです。

   「**ビジュアライザー**」を有効にして、アプリケーション構成とそれに関連付けられたエンティティを表示します。ビジュアライザーを使用すると、さまざまなコンポーネントがどのように接続されているかを確認でき、移行プロセス中の理解と意思決定に役立ちます。

   仮想サーバー設定を編集(/en-us/netscaler-application-delivery-management-software/media/application-configuration-visualizer.png)

   ビジュアライザーを使用すると、次のことができます。

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

- サーバーに関連付けられているアクションとポリシーの階層を表示します
- サーバーにカーソルを合わせると、サーバーにバインドされているポリシーやアクションを含む、サーバーの詳細な説明が表示されます
- ズームスライダーを使用して表示を拡大および縮小します
- エンティティのマイナス記号(-)またはプラス記号(+)をクリックして、階層を折りたたむか展開します

「**次へ**」をクリックします。

8. 「**アプリケーション展開情報**」で、仮想サーバー、サービス、およびサービスグループメンバーのIPアドレス、ポート、状態、ARPを表示および編集できます。

   仮想サーバー設定を編集(/en-us/netscaler-application-delivery-management-software/media/edit-state-and-arp-attributes.png)

   「**詳細**」ページで、NSIPエンティティのIPアドレス、ポート、状態、およびARPステータスを編集できます。

   状態とARPステータスを編集(/en-us/netscaler-application-delivery-management-software/media/edit-state-arp-lbv.png)

   「

   **注:**

   」:

   - 仮想サーバーIPのNSIPエンティティの状態が、ARPの初期状態を決定します。
   - 仮想サーバーIPのNSIPエンティティがターゲットのNetScalerにすでに構成されている場合、仮想サーバーのARPステータスを変更することはできません。
   - 仮想サーバーのARP状態を変更すると、同じIPアドレスを持つすべての仮想サーバーのARP状態が変更されます。仮想サーバーの状態を変更しても、関連付けられた仮想サーバーのみに影響します。
   - ARPは、IPパターンベースの仮想サーバーには適用されません。
   - ソース構成で仮想サーバーIPのNSIP状態が無効になっている場合、ARPも自動的に無効になり、ARPを変更することはできません。

   ソースインスタンスとターゲットインスタンスが同じ場合、**Application Deployment Info**タブは表示されません。

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

9. **Authentication/Networking Deployment Info**では、利用可能な場合、認証サーバーとネットプロファイルの属性を表示および編集できます。

   a. **Authentication Deployment Info**で、必要な認証サーバーを選択し、サーバーのIPアドレス、サーバーIP、サーバー名、およびポート番号を編集します。

   b. **NetProfile Info**で、必要なネットプロファイルを選択し、**NetProfile**と**IPSET**の詳細を編集します。

   > **注:**
   >
   > このステップで行われたNSIPアドレスの変更は最終的な移行に考慮され、以前のステップでの構成は変更を反映するように更新されます。

10. 「**リソースファイル/シークレット**」で、パスワードと証明書を復号化するための証明書とキーをアップロードします。「**次へ**」をクリックします。
11. **Global Configuration**で、ソースとターゲット間のグローバル構成設定の違いを表示します。ターゲットに適用される構成を確認し、確認応答を選択します。**Next**をクリックします。
12. **Migrate**で、StyleBookの詳細を表示します。**Migrate**をクリックします。

> **注:**
>
> デフォルトでは、NetScaler Console は、アプリケーションまたは仮想サーバーを NetScaler に移行する際に作成される設定パックを管理します。結果として得られる設定に設定パックを関連付けたくない場合は、**NetScaler Console を介して設定を管理する** チェックボックスをオフにしてください。

13. **サポートされていない構成**で、見落とされた構成またはサポートされていない構成を表示します。これらの構成を正常に移行するには、見落とされた構成またはサポートされていない構成をターゲットインスタンスに個別に適用する必要があります。**次へ**をクリックします。

## 制限事項

- ソースインスタンスで言及されている名前付き式と `responderhtmlpages` は識別されません。移行前に、ターゲットインスタンスで名前付き式と `responderhtmlpages` を構成してください。
- ソースに `servicegroup` とモニターバインディングの構成が次のようにある場合：

```
bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
```

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

次のエラーが表示されます：

```
CLI Command conversion failed: 100 - No such command [{ "errorcode":
1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
```

このエラーは、NetScaler がサービスグループとモニター間のバインディングを無効な形式で保存するため発生します。この問題は、NetScaler 12.1.52.15 ビルド以降で修正されています。

# ビジネスアプリケーションのStyleBook

NetScaler Consoleは、特定のビジネスアプリケーション向けにNetScaler構成を展開するのに役立つStyleBookを提供します。これらのStyleBookの詳細については、次のトピックを参照してください。

- SSO Google Apps スタイルブック
- SSO Office 365 スタイルブック
- Microsoft Skype for Business スタイルブック
- Microsoft Exchange スタイルブック
- Microsoft SharePoint スタイルブック
- Microsoft ADFS プロキシ スタイルブック
- Oracle e-business スタイルブック

## SSO Google Apps スタイルブック

Google Appsは、Googleが開発したクラウドコンピューティング、生産性向上、コラボレーションツール、ソフトウェア、製品のコレクションです。シングルサインオン (SSO) を使用すると、ユーザーはエンタープライズ資格情報を使用してすべてのサービスに1回サインインするだけで、管理者による管理コンソールへのサインインを含むすべてのエンタープライズクラウドアプリケーションにアクセスできます。

NetScaler Console SSO Google Apps StyleBookを使用すると、NetScalerインスタンスを介してGoogle AppsのSSOを有効にできます。このStyleBookは、NetScalerインスタンスを、Google Appsにアクセスするユーザーを認証するためのSAML IDプロバイダーとして構成します。

このStyleBookを使用してNetScalerインスタンスでGoogle AppsのSSOを有効にすると、次の手順が実行されます。

1. 認証仮想サーバーの構成

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

2. SAML IdPポリシーとプロファイルの構成
3. ポリシーとプロファイルを認証仮想サーバーにバインドする
4. インスタンスでのLDAP認証サーバーとポリシーの構成
5. LDAP認証サーバーとポリシーを、インスタンスで構成された認証仮想サーバーにバインドする

**構成の詳細**:

以下の表に、この統合が正常に機能するために必要な最小ソフトウェアバージョンを示します。統合プロセスは、それらの上位バージョンもサポートします。

| 製品 | 最小要件バージョン |
| --- | --- |
| NetScaler | リリース 11.0、Advanced/Premium ライセンス |

以下の手順は、認証要求をNetScalerが監視するIPアドレスにルーティングするために、適切な外部または内部DNSエントリをすでに作成していることを前提としています。

**SSO GoogleアプリStyleBook構成の展開**:

以下のタスクは、ビジネスネットワークにMicrosoft SSO Google Apps StyleBookを展開するのに役立ちます。

### SSO GoogleアプリStyleBookを展開するには

1. NetScaler Consoleで、**Applications** > **Configurations** > **StyleBooks** に移動します。StyleBooksページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、**SSO Google Apps StyleBook** を見つけます。**Create Configuration** をクリックします。
2. StyleBookは、このStyleBookで定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして開きます。
3. 以下のパラメーターの値を入力します。

    a. **アプリケーション名**。ネットワークに展開するSSO Googleアプリ構成の名前。

    b. **認証仮想IPアドレス**。認証、承認、監査仮想サーバーがGoogleアプリSAML IdPポリシーにバインドするために使用する仮想IPアドレス。

    c. **SAMLルール式**。デフォルトでは、以下のNetScalerポリシー（PI）式が使用されます: HTTP.REQ.HEADER("Referrer").CONTAINS("google")。要件が異なる場合は、このフィー

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

ルドを別の式で更新してください。このポリシー式は、これらのSAML SSO設定が適用されるトラフィックと一致し、ReferrerヘッダーがGoogleドメインから来ていることを確認します。

4. SAML IdP設定セクションでは、ステップ3で作成された認証、承認、監査仮想サーバーによって使用されるSAML IdPプロファイルとポリシーを作成することにより、NetScalerインスタンスをSAML IDプロバイダーとして構成できます。

   a. **SAML発行者名**。このフィールドに、認証仮想サーバーのパブリックFQDNを入力します。例: `https://<NetScaler Auth VIP>/saml/login`

   b. **SAMLサービスプロバイダー（SP）ID**。（オプション）NetScaler IDプロバイダーは、このIDと一致する発行者名からのSAML認証要求を受け入れます。

   c. **アサーションコンシューマーサービスURL**。NetScaler IDプロバイダーがユーザー認証成功後にSAMLアサーションを送信する必要があるサービスプロバイダーのURLを入力します。アサーションコンシューマーサービスURLは、IDプロバイダーサーバーサイトまたはサービスプロバイダーサイトで開始できます。

   d. このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。

      i. SAMLバインディングプロファイル（デフォルトは「POST」プロファイル）。

      ii. SAMLリクエスト/レスポンスを検証/署名するための署名アルゴリズム（デフォルトは「RSA-SHA1」）。

      iii. SAMLリクエスト/レスポンスのハッシュをダイジェストする方法（デフォルトは「SHA-1」）。

      iv. 暗号化アルゴリズム（デフォルトはAES256）、およびその他の設定。

      **注**

      これらの設定はGoogle Appsとの互換性がテスト済みであるため、デフォルト設定を維持することをお勧めします。

   e. ユーザー属性チェックボックスを有効にして、次のようなユーザー詳細を入力することもできます。

      i. ユーザー属性の名前

      ii. 属性の値を抽出するために評価されるNetScaler PI式

      iii. 属性のユーザーフレンドリーな名前

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

iv. ユーザー属性の形式を選択します。

これらの値は発行されたSAMLアサーションに含まれます。このStyleBookを使用してNetScalerによって発行されるアサーションには、最大5セットのユーザー属性を含めることができます。

5. LDAP設定セクションで、Google Appsユーザーを認証するために以下の詳細を入力します。ドメインユーザーが会社のメールアドレスを使用してNetScalerインスタンスにログオンできるようにするには、以下を設定する必要があります。

   a. **LDAP (Active Directory) ベース**。認証を許可したいActive Directory (AD) 内にユーザーアカウントが存在するドメインのベースドメイン名を入力します。例: `dc=netscaler`、`dc=com`

   b. **LDAP (Active Directory) Bind DN**。ADツリーを参照する権限を持つドメインアカウント（設定を容易にするためにメールアドレスを使用）を追加します。例: `cn=Manager,dc=netscaler,dc=com`

   c. **LDAP (Active Directory) Bind DN Password**。認証用のドメインアカウントのパスワードを入力します。

   d. このセクションで入力する必要があるその他のフィールドは次のとおりです。

      i. NetScalerがユーザー認証のために接続するLDAPサーバーのIPアドレス

      ii. LDAPサーバーのFQDN名

      > **注**
      >
      > 上記の2つのうち、LDAPサーバーのIPアドレスまたはFQDN名の少なくともいずれか1つを指定する必要があります。

      iii. NetScalerがユーザー認証のために接続するLDAPサーバーポート（デフォルトは389）.

      iv. LDAPホスト名。これは、検証がオンになっている場合（デフォルトではオフ）、LDAP証明書を検証するために使用されます。

      v. LDAPログイン名属性。ログイン名を抽出するために使用されるデフォルトの属性は「sAMAccountName」です。

      vi. その他のオプションのLDAP設定

6. SAML IdP SSL証明書セクションでは、SSL証明書の詳細を指定できます。

   a. **Certificate Name**。SSL証明書の名前を入力します。

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

b. **Certificate File**。ローカルシステムまたはNetScaler Consoleのディレクトリから SSL証明書ファイルを選択します。

c. **CertKey Format**。ドロップダウンリストボックスから、証明書と秘密鍵ファイルの形式を選択します。サポートされている形式は.pemおよび.der拡張子です。

d. **Certificate Key Name**。証明書秘密鍵の名前を入力します。

e. **証明書キーファイル**。ローカルシステムまたはNetScaler Consoleから、証明書の秘密鍵を含むファイルを選択します。

f. **秘密鍵パスワード**。秘密鍵ファイルがパスフレーズで保護されている場合は、このフィールドに入力します。

g. また、「詳細証明書設定」チェックボックスを有効にして、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力することもできます。

7. オプションで、上記で入力したSAML IdP証明書がNetScalerにCA公開証明書をインストールする必要がある場合、IdP SSL CA証明書を選択できます。詳細設定で「CA証明書である」を選択していることを確認してください。
8. オプションで、SAML SP SSL証明書を選択して、Google Apps (SAML SP) からの認証要求を検証するために使用されるGoogle SSL証明書 (公開鍵) を指定できます。
9. **ターゲットインスタンス**をクリックし、このGoogle Apps SSO構成を展開するNetScalerインスタンスを選択します。**作成**をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

**注**

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを、このウィンドウの利用可能なインスタンスリストに追加することもできます。

また、,

**ヒント**

実際の構成を実行する前に、**ドライラン**を選択して、StyleBookによってターゲットNetScalerインスタンスに作成される構成オブジェクトを視覚的に確認することをお勧めします。

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

## SSO Office 365 スタイルブック

Microsoft Office 365は、Microsoftがサブスクリプションベースで提供する、クラウドベースの生産性およびコラボレーションアプリケーションのスイートです。これには、Exchange、SharePoint、Office、Skype for BusinessなどのMicrosoftの人気のあるサーバーベースのアプリケーションが含まれます。シングルサインオン (SSO) により、ユーザーはすべてのエンタープライズクラウドアプリケーションにアクセスできます。

- 管理コンソールにサインインする管理者を含む
- 企業の資格情報を使用して、すべてのMicrosoft Office 365サービスに1回サインオンします。

SSO Office 365 StyleBookを使用すると、NetScalerインスタンスを介してMicrosoft Office 365のSSOを有効にできます。NetScalerをSAML IDプロバイダー (IdP) として、Microsoft Office 365をSAMLサービスプロバイダーとしてSAML認証を構成できるようになりました。

このStyleBookを使用してNetScalerインスタンスでMicrosoft Office 365のSSOを有効にするには、次の手順が必要です。

1. 認証仮想サーバーの構成
2. SAML IDPポリシーとプロファイルの構成
3. ポリシーとプロファイルを認証仮想サーバーにバインドする
4. インスタンス上のLDAP認証サーバーとポリシーの構成
5. インスタンスで構成された認証仮想サーバーにLDAP認証サーバーとポリシーをバインドする。

この統合が正常に機能するために必要な最小ソフトウェアバージョンを次の表に示します。統合プロセスは、それ以降のバージョンでも機能するはずです。

| PRODUCT | MINIMUM REQUIRED VERSION |
| --- | --- |
| NetScaler | 11.0, Advanced/Premium License |

以下の手順は、適切な外部および内部DNSエントリをすでに作成していることを前提としています。これらのエントリは、認証要求をNetScalerが監視するIPアドレスにルーティングするために不可欠です。

以下の手順は、ビジネスネットワークでSSO Office 365 StyleBookを実装するのに役立ちます。

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

### SSO Microsoft Office 365 StyleBookを展開するには

1. NetScaler Consoleで、**Applications** > **StyleBooks** に移動します。**StyleBooks** ページには、NetScaler Console で使用できるすべてのStyleBookが表示されます。下にスクロールして、**SSO Office 365 StyleBook** を見つけます。**Create Configuration** をクリックします。
2. StyleBookは、このStyleBookで定義されているすべてのパラメータの値を入力できるユーザーインターフェイスページとして開きます。
3. 次のパラメータの値を入力します。

   a. **アプリケーション名**。ネットワークに展開するSSO Microsoft Office 365構成の名前。

   b. **認証仮想IPアドレス**。Microsoft Office 365 SAML IdPポリシーがバインドされているAAA仮想サーバーで使用される仮想IPアドレス。

   

4. **SSL Certificates Settings**セクションで、SSL証明書と証明書キーの名前を入力します。

   **注**

   これはOffice 365サービスプロバイダー証明書ではありません。このSSL証明書は、NetScalerインスタンス上の仮想認証サーバーにバインドされます。

5. ローカルストレージフォルダーから該当するファイルを選択します。PEM形式の暗号化された秘密キーをロードするために、秘密キーパスワードを入力することもできます。

   

6. **詳細証明書設定**チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力できます。
7. オプションで、SSL証明書がNetScalerにCA公開証明書をインストールする必要がある場合は、**認証仮想IP用のSSL CA証明書**チェックボックスを選択できます。上記の**詳細証明書設定**セクションで「CA証明書である」を選択していることを確認してください。
8. **SSO Office 365のLDAP設定**セクションで、Office 365ユーザーを認証するために次の詳細を入力します。ドメインユーザーが会社のメールアドレスを使用してNetScalerインスタンスにログオンできるようにするには、次を構成します。

   - **LDAP (Active Directory) ベース**。認証を許可するために、Active Directory (AD) 内にユーザーアカウントが存在するドメインのベースドメイン名を入力します。例: dc=netscaler®,dc=com

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

- **LDAP (Active Directory) Bind DN**。ADツリーを参照する権限を持つドメインアカウント（設定を容易にするためにメールアドレスを使用）を追加します。例：cn=Manager,dc=netscaler,dc=com
- **LDAP (Active Directory) Bind DN パスワード**。認証用のドメインアカウントのパスワードを入力します。
- このセクションで入力する必要があるその他のフィールドは次のとおりです。
  - ユーザー認証のためにNetScalerが接続するLDAPサーバーのIPアドレス。
  - LDAPサーバーのFQDN名。

    **注**

    上記2つのうち、LDAPサーバーのIPアドレスまたはFQDN名のいずれかを少なくとも1つ指定する必要があります。

  - ユーザー認証のためにNetScalerが接続するLDAPサーバーポート（デフォルトは389）。LDAPSは636を使用します。
  - LDAPホスト名。ホスト名は、検証がオンになっている場合（デフォルトではオフ）、LDAP証明書を検証するために使用されます。
  - LDAPログイン名属性。ログイン名を抽出するために使用されるデフォルトの属性は「samAccountname」です。
  - その他のオプションのLDAP設定。

9. **SAML IdP証明書**セクションでは、SAMLアサーションに使用されるSSL証明書の詳細を指定できます。
   - **証明書名**。SSL証明書の名前を入力します。
   - **証明書ファイル**。ローカルシステムのディレクトリからSSL証明書ファイルを選択します。
   - **CertKey Format**。ドロップダウンリストボックスから、証明書と秘密鍵ファイルの形式を選択します。サポートされている形式は、.pemおよび.derファイル拡張子です。
   - **Certificate Key Name**。証明書秘密鍵の名前を入力します。
   - **Certificate Key File**。ローカルシステムから証明書の秘密鍵を含むファイルを選択します。
   - **Private Key Password**。秘密鍵ファイルを保護するパスフレーズを入力します。

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

**Advanced Certificate Settings**チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力できます。



10. オプションで、上記で入力したSAML IdP証明書にNetScalerにインストールするCA公開証明書が必要な場合は、**SAML IdP CA Certificate**を選択できます。上記の**Advanced Certificate Settings**セクションで**Is a CA Certificate**が選択されていることを確認してください。
11. **SAML SP Certificate**セクションで、Office 365 SSL公開証明書の以下の詳細を入力します。この証明書は、NetScalerインスタンスが受信SAML認証要求を検証するために使用されます。

    - **Certificate Name**。SSL証明書の名前を入力します。
    - **Certificate File**。ローカルシステムのディレクトリからSSL証明書ファイルを選択します。
    - **CertKey Format**。ドロップダウンリストボックスから、証明書と秘密鍵ファイルの形式を選択します。サポートされている形式は、.pemおよび.derファイル拡張子です。
    - **Advanced Certificate Settings**チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力できます。

    

12. **SAML Idp Settings**セクションでは、ステップ3で作成されたAAA仮想サーバーによって使用されるSAML IDPプロファイルとポリシーを作成することにより、NetScalerインスタンスをSAML IDプロバイダーとして構成できます。

    - **SAML Issuer Name**。このフィールドに、認証仮想サーバーのパブリックFQDNを入力します。例: `https://<NetScaler Auth VIP>/saml/login`
    - **Name Identifier Expression**。SAMLアサーションで送信されるSAML NameIdentifierを抽出するために評価されるNetScaler式を入力します。例: `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - **署名アルゴリズム**: SAMLリクエスト/レスポンスを検証/署名するアルゴリズムを選択します（デフォルトは「RSA-SHA256」）。
    - **ダイジェストメソッド**。SAMLリクエスト/レスポンスのハッシュをダイジェストする方法を選択します（デフォルトは「SHA256」）。
    - **オーディエンス名**。サービスプロバイダー（Microsoft Office 365）を表すエンティティ名またはURLを入力します。

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

- **SAMLサービスプロバイダー（SP）ID**。（オプション）NetScaler IDプロバイダーは、このIDと一致する発行者名からのSAML認証リクエストを受け入れます。
- **アサーションコンシューマーサービスURL**。ユーザー認証が成功した後、NetScaler IDプロバイダーがSAMLアサーションを送信する必要があるサービスプロバイダーのURLを入力します。アサーションコンシューマーサービスURLは、IDプロバイダーサーバーサイトまたはサービスプロバイダーサイトで開始できます。
- このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。
  - **SAML属性名**。SAMLアサーションで送信されるユーザー属性の名前。
  - **SAML属性フレンドリ名**。SAMLアサーションで送信されるユーザー属性のフレンドリ名。
  - **SAML属性のPI式**。デフォルトでは、次のNetScalerポリシー（PI）式が使用されます: HTTP.REQ.USER.ATTRIBUTE(1)。このフィールドは、LDAPサーバーから送信される最初のユーザー属性（メール）をSAML認証属性として指定します。
  - ユーザー属性の形式を選択します。

  これらの値は、発行されたSAMLアサーションに含まれます。

  **ヒント**

  これらの設定はMicrosoft Office 365アプリで動作することがテストされているため、デフォルト設定を維持することをお勧めします。

13. **ターゲットインスタンス**をクリックし、このMicrosoft Office 365 SSO構成を展開するNetScalerインスタンスを選択します。**作成**をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

    **ヒント**

    実際の構成を実行する前に、**ドライラン**を選択して、StyleBookによってターゲットのNetScalerインスタンス上に作成される構成オブジェクトを表示することをお勧めします。

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

# マイクロソフト スカイプ for ビジネス スタイルブック

Skype for Business 2015アプリケーションは、機能するためにいくつかの外部コンポーネントに依存しています。Skype for Businessネットワークは、サーバーとそのオペレーティングシステム、データベース、認証および認可システム、ネットワークシステムとインフラストラクチャ、電話PBXシステムなど、さまざまなシステムで構成されています。Skype for Business Server 2015には、Standard EditionとEnterprise Editionの2つのバージョンがあります。主な違いは、Enterprise Editionにのみ含まれる高可用性機能のサポートです。高可用性を実装するには、複数のフロントエンドサーバーをプールに展開し、SQLサーバーをミラーリングする必要があります。

Enterprise Editionの展開により、異なる役割を持つ複数のサーバーを作成できます。

## 主要コンポーネント

Skype for Business 2015アプリケーションの主要コンポーネントは次のとおりです。

- フロントエンドサーバー
- エッジサーバー
- ディレクターサーバー
- データベース (SQL) サーバー

### フロントエンドサーバー

Skype for Businessアプリケーションでは、フロントエンドサーバーはネットワークのコアサーバーです。ユーザー認証、登録、プレゼンス、アドレス帳、A/V会議、アプリケーション共有、インスタントメッセージング、Web会議のリンクとサービスを提供します。Skype for Business 2015 Enterprise Editionを展開する場合、トポロジは通常、Skype for Businessデータベースを保持するSQL Serverインスタンスをホストするデータベースサーバーを備えたフロントエンドプールで負荷分散された少なくとも2つのフロントエンドサーバーで構成されます。

### エッジサーバー

組織の内部ネットワークにログインしていない外部ユーザーが内部ユーザーと対話できるようにする必要がある場合、Skype for Business用のエッジサーバーの展開が必要です。これらの外部ユーザーは、認証された匿名のリモートユーザー、フェデレーションパートナー、またはその他のモバイルクライアントである可能性があります。

Skype For Business Edgeサーバーには4種類の役割があります。

- アクセスエッジ。これはSIPトラフィックを処理し、外部接続を認証し、リモート接続とフェデレーション接続を許可します。

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

- Web会議。データ会議パケットを処理し、外部ユーザーがSkype for Businessにアクセスできるようにします。
- A/V会議。A/V会議パケットを処理し、オーディオとビデオ、アプリ共有、ファイル転送を外部ユーザーに拡張します。
- XMPPプロキシ。XMPPパケットを処理し、XMPPベースのサーバーまたはクライアントがSkype for Businessに接続できるようにします。

### ディレクターサーバー

Skype for Business 2015におけるディレクターサーバーの主な機能は、エンドポイントを認証し、ユーザーをアカウントを含むプールに「誘導」することです。Skype for Business 2015では、ディレクターはスタンドアロンサーバー上の完全に専用かつ特定の役割ですが、オプションのサーバーです。これにより、構成の展開や削除が容易になり、セキュリティが向上します。

ディレクターは、複数のプールが存在する場合に最も役立ちます。これは、エンドポイントを認証するための単一の接点を提供するからです。また、リモートユーザーの場合、ディレクターはエッジプールとフロントエンドプールの間の追加のホップとして機能し、攻撃に対する保護層を追加します。

次の図は、ネットワークにおけるSkypeサーバーの展開を図式的に表しています。



## 企業におけるNetScalerインスタンスの構成

次の表は、以下の手順に含まれるサンプル構成で使用されているIPアドレスを示しています。

| スカイプ フォー ビジネス サーバー | 仮想IPアドレス | サーバーIPアドレス | NETSCALERインスタンス |
|---|---|---|---|
| エッジサーバー | 外部VIP - 192.20.20.20 | 192.20.20.21; 192.20.20.22 | 10.102.29.141 |
| | 内部VIP - 10.10.10.20 | 10.10.10.21; 10.10.10.22 | |
| フロントエンドサーバー | 10.10.10.10 | 10.10.10.11; 10.10.10.12 | 10.102.29.60 |
| ディレクターサーバー | 10.10.10.30 | 10.10.10.31; 10.10.10.32 | 10.102.29.93 |

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

### フロントエンドサーバーを構成するには

1. NetScaler Consoleで、**Applications** > **Configuration** に移動し、**Create New** をクリックします。**Choose StyleBook** ページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、**Microsoft Skype for Business 2015 StyleBook** を選択します。StyleBookはユーザーインターフェイスページとして開き、このStyleBookで定義されているすべてのパラメーターの値を入力できます。
2. 「**Edge Server**」セクションで、ネットワーク内のすべてのEdgeサーバーの仮想IP（VIP）アドレスとIPアドレスを入力します。
    a. Access Edge、Web会議Edge、およびA/V Edgeに使用されるEdgeサーバーの外部VIPアドレスとIPアドレス。
    b. 内部ネットワークに接続されるEdgeサーバーの内部VIPアドレスとIPアドレス。
    c. ネットワーク内の2つの外部Edgeサーバーと2つの内部Edgeサーバー。
3. 「**Front-End Server**」セクションで、Skype for Business Front-Endサーバー用に作成される仮想Front-Endサーバー（VIP）のIPアドレスを入力します。また、ネットワーク内のすべてのSkype for Business Front-EndサーバーのIPアドレスを入力します。
4. 「**Director Server**」セクションで、Skype for Businessアプリケーション用に作成されるDirectorサーバーの仮想IPアドレス（VIP）を入力します。また、ネットワーク内のすべてのSkype for Business DirectorサーバーのIPアドレスを入力します。高可用性のために、少なくとも2つのDirectorサーバーを作成します。
5. 「**Advanced Settings**」セクションには、3つのSkypeサーバー用にNetScalerインスタンスで構成されているすべてのデフォルトポートが一覧表示されます。

次の表に、すべてのデフォルトポートとプロトコルの一覧を示します。

| ラベル | ポート | プロトコル | 説明 |
|---|---|---|---|
| HTTPポート | 80 | HTTP | HTTPSが使用されていない場合に、フロントエンドサーバーからWebファームFQDNへの通信に使用されます。 |
| HTTPSポート | 443 | HTTPS | フロントエンドサーバーからWebファームFQDNへの通信に使用されます。 |

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

| ラベル | ポート | プロトコル | 説明 |
| --- | --- | --- | --- |
| AutoDiscover内部ポート | 4443 | HTTPS | AutoDiscoverサインインのためのHTTPS（リバースプロキシから）およびHTTPSフロントエンドのプール間通信。 |
| RPCポート | 135 | DCOMおよびリモートプロシージャコール（RPC） | ユーザーの移動、ユーザーレプリケーターの同期、アドレス帳の同期などのDCOMベースの操作に使用されます。 |
| SIPポート | 5061 | TCP (TLS) | すべての内部SIP通信にフロントエンドサーバーによって使用されます。 |
| SIPフォーカスポート | 444 | HTTPS、TCP | フォーカス（Skype会議の状態を管理するコンポーネント）と個々のサーバー間のHTTPS通信に使用されます。 |
| SIPグループポート | 5071 | TCP | 応答グループアプリケーションの受信SIPリクエストに使用されます。 |
| SIP AppSharingポート | 5065 | TCP | アプリケーション共有の受信SIPリスニングリクエストに使用されます。 |
| SIPアテンダントポート | 5072 | TCP | アテンダントへの着信SIPリクエストに使用されます (つまり、ダイヤルイン会議用です)。 |

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

| ラベル | ポート | プロトコル | 説明 |
| --- | --- | --- | --- |
| SIP会議アナウンスポート | 5073 | TCP | Skype for Business サーバー会議アナウンスサービスへの着信SIPリクエストに使用されます (つまり、ダイヤルイン会議用です)。 |
| SIPコールパークポート | 5075 | TCP | CallParkアプリケーションへの着信SIPリクエストに使用されます。 |
| SIPコールアドミッションポート | 448 | TCP | Skype for Business サーバー帯域幅ポリシーサービスによるコールアドミッションコントロールに使用されます。 |
| SIPコール受付TURNポート | 5080 | TCP | オーディオ/ビデオエッジTURNトラフィックの帯域幅ポリシーサービスによるコール受付制御に使用されます。 |
| SIPオーディオテストポート | 5076 | TCP | オーディオテストサービスへの着信SIPリクエストに使用されます。 |
| HTTPS外部ポート | 443 | HTTPS | リモートユーザーアクセス、内部Web会議へのアクセス、および内部メディアとA/Vセッションへのアクセス用のSTUN/TCPインバウンドおよびアウトバウンドメディア通信のため |

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

| ラベル | ポート | プロトコル | 説明 |
| --- | --- | --- | --- |
| | | | のSIP/TLS通信の外部ポートに使用されます。 |
| HTTPS内部ポート | 443 | HTTPS | リモートユーザーアクセス、内部Web会議へのアクセス、および内部メディアとA/Vセッションへのアクセス用のSTUN/TCPインバウンドおよびアウトバウンドメディア通信のためのSIP/TLS通信用の内部ポートに使用されます。 |
| SIP外部リモートアクセスポート | 5061 | TCP | リモートユーザーアクセスまたはフェデレーションのためのSIP/MTLS通信用の外部ポートに使用されます。 |
| SIP内部リモートアクセスポート | 5061 | TCP | リモートユーザーアクセスまたはフェデレーションのためのSIP/MTLS通信用の内部ポートに使用されます。 |
| SIP外部STUN UDPポート | 3478 | UDP | STUN/UDPインバウンドおよびアウトバウンドメディア通信用の外部ポートに使用されます。 |
| SIP内部STUN UDPポート | 3478 | UDP | STUN/UDPのインバウンドおよびアウトバウンドメディア通 |

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

| ラベル | ポート | プロトコル | 説明 |
| --- | --- | --- | --- |
| | | | 信用の内部ポートに使用されます。 |
| SIP内部IMポート | 5062 | | 内部ファイアウォールを介して外部に流れるIM通信のSIP/MTLS認証用の内部ポートに使用されます。 |
| HTTPポート | 80 | TCP | ディレクターからWebファームのFQDNへの初期通信に使用されます。 |
| HTTPSポート | 443 | HTTPS | ディレクターからWebファームのFQDNへの通信に使用されます。 |
| AutoDiscover内部ポート | 4443 | HTTPS | HTTPS（リバースプロキシから）およびAutoDiscoverサインイン用のHTTPSディレクターのプール間通信に使用されます。 |
| SIP内部ポート | 5061 | TCP | サーバー間の内部通信およびクライアント接続に使用されます。 |

6. **ターゲットインスタンス**セクションで、3つのSkype for Businessサーバーを展開する3つの異なるNetScalerインスタンスを選択します。

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

**注**

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスをこのウィンドウの利用可能なインスタンスリストに追加することもできます。

「**作成**」をクリックして、選択したNetScalerインスタンスに構成を作成します。

**ヒント**

インスタンスで実際の構成を実行する前に、ターゲットインスタンスに作成する必要がある構成オブジェクトを確認するために**ドライラン**を選択することをお勧めします。

構成が正常に作成されると、StyleBookは25個のロードバランシング仮想サーバーを作成します。つまり、各ポートに対して1つのロードバランシング仮想サーバーが1つのサービスグループとともに定義され、そのサービスグループはロードバランシング仮想サーバーにバインドされます。構成はまた、フロントエンドサーバーをサービスグループメンバーとして追加し、それらをサービスグループにバインドします。作成されるサービスグループメンバーの数は、作成されるフロントエンドサーバーの数と同じです。

次の図は、各サーバーで作成されたオブジェクトを示しています。



## マイクロソフト エクスチェンジ StyleBook

Microsoft Exchange 2016 StyleBookを使用すると、ネットワーク内のMicrosoft Exchange 2016エンタープライズアプリケーションを最適化および保護するNetScaler構成を展開できます。Microsoft Exchange 2016は、従業員やその他の関係者に電子メール、個人情報管理、およびメッセージングサービスを提供する上で重要なエンタープライズアプリケーションです。

### Microsoft Exchange StyleBookを使用して構成されるNetScaler機能

Microsoft Exchange 2016 StyleBookは、Microsoft Exchange 2016サーバー向けに以下のNetScaler機能を有効化および構成します。

- 負荷分散 - 複数のExchangeサーバーの負荷分散を可能にする基本的な負荷分散
- コンテンツスイッチング - 単一IPアクセスと、クエリを正しい負荷分散仮想サーバーにリダイレクトすることを可能にするコンテンツスイッチング
- リライト - ユーザーをセキュアなページにリダイレクトします

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

- SSLオフロード - SSL処理をNetScalerにオフロードし、Exchangeサーバーの負荷を軽減します

次の図は、ネットワーク内のExchangeサーバーの展開を模式的に表しています。



### 前提条件

- 証明書ベースの認証の場合、ネットワーク設定の一部であるすべてのアドレス指定可能なホストは、IPアドレスだけでなく、解決可能なドメイン名を持っている必要があります。
- Microsoft Exchange 2016サーバーでSIPポートにアクセスできることを確認してください。

### マイクロソフト エクスチェンジ StyleBook の構成

NetScaler構成を展開するために、ビジネスエンタープライズでMicrosoft Exchange StyleBookを構成します。

#### NetScaler Console で Microsoft Exchange アプリケーションを構成するには

1. NetScaler Console で、**Applications** > **StyleBooks** の順に移動します。
2. **Microsoft Exchange 2016 StyleBook** を検索し、**Create Configuration** をクリックします。

   StyleBook は、この StyleBook で定義されているすべてのパラメータの値を入力できるユーザーインターフェイスフォームとして表示されます。

   Microsoft Exchange StyleBook の構成(/en-us/netscaler-application-delivery-management-software/media/microsoft-exchange-2016-create-configuration.png)
3. 次のパラメータの詳細を入力します。

   - **Exchange Application Name** - ネットワーク内の Microsoft Exchange アプリケーションの名前
   - **Exchange VIP** - Microsoft Exchange アプリケーションのクライアント要求を受信する NetScaler 上の仮想 IP アドレス
   - **Exchange Server IPs** - ネットワーク内のすべての Exchange サーバーの IP アドレス。

     IP アドレスを追加する場合は、プラス (+) アイコンをクリックします。通常、ネットワークには2台のExchangeサーバーが構成されています。
4. **Exchange Certificates** セクションで、Exchange 証明書を NetScaler Console にアップロードします。証明書ファイルとキーファイルの両方の名前を入力し、ローカルストレージから

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

アップロードします。キーファイルを暗号化するために秘密鍵パスワードを指定することもできます。

**注**

証明書ファイルが「.pem」または「.der」形式であることを確認してください。NetScaler Console は、他の形式のファイルを拒否します。

証明書の有効期限の詳細や高度な設定を指定する場合は、**Advanced Certificate Settings** を選択します。

5. **Exchange Active Directory Authentication config** セクションで、データを入力して AD 設定を構成します。

   - **Active Directory Authentication VIP** - NetScalerアプライアンスでAD (LDAP) 仮想サーバーを作成および構成するために使用される仮想IPアドレス。
   - **Active Directory Server IP** - Active Directoryドメインコントローラーの IPアドレス。
   - **Active Directory ベース文字列** - Active Directory の LDAP ベース文字列です。例: CN=Users,DC=CTXNSSFB,DC=COM。
   - **Active Directory LDAP Bind Distinguished Name (DN)** - LDAPバインド識別名 (DN) は、このオブジェクトをLDAPサーバー (AD) にバインドするために使用されます。例: 「cn=Administrator,cn=Users,dc=acme,dc=com」
   - **Active Directory LDAP Bind Distinguished Name (DN) Password** - LDAPバインド識別名 (DN) は、AD認証のパスワードです。
   - **Active Directory User Name Attribute** - ユーザー名のAD属性。NetScalerはLDAP属性を使用して外部Active Directoryサーバーを照会します。例: 「sAMAccountName」
   - **Active Directory group Attribute Name** - LDAPサーバーで構成されたLDAPグループ属性名。例: LDAPのグループ属性の「memberOf」。
   - **Active Directory Sub-Attribute Name** - LDAPサーバーで構成されたLDAPサブ属性名。例: LDAPのサブ属性の「cn」。
   - **Active Directory 認証ドメイン** - 認証に使用される AD/LDAP ドメイン名です。例: ctxnssfb.com。

6. 「**Target Instances**」セクションで、このExchange構成を展開するNetScalerインスタンスを選択します。

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

> **注**
>
> 最近検出されたNetScalerインスタンスを表示する場合は、更新アイコンをクリックします。

7. 「**Create**」をクリックして構成ファイルを作成し、選択したNetScalerインスタンスで構成を実行します。

   インスタンスで実際の構成を実行する前に、まず「**Dry Run**」を選択して、ターゲットインスタンスで作成される構成オブジェクトを確認することをお勧めします。

構成が正常に作成されると、StyleBookによってコンテンツスイッチング仮想サーバー、5つの負荷分散仮想サーバー、および1つのLDAP認証仮想サーバーにバインドされた1つのLDAPポリシーが作成されます。また、対応するサービスグループが作成され、負荷分散仮想サーバーにバインドされます。

## Microsoft SharePoint スタイルブック

Microsoft SharePoint 2016 は、主にドキュメント管理およびストレージシステムを提供する主要なエンタープライズアプリケーションであり、高度に設定可能で、すべての主要なブラウザでサポートされています。

Microsoft SharePoint 2016 StyleBook を使用して、ネットワーク内の Microsoft SharePoint 2016 エンタープライズアプリケーションを最適化および保護する NetScaler 構成を展開できます。

### 前提条件

- マイクロソフト シェアポイント 2016
- NetScaler Console バージョン 12.0 以降
- NetScaler バージョン 10.5 以降

### Microsoft SharePoint 2016 StyleBook によって構成される NetScaler 機能

Microsoft SharePoint 2016 StyleBook を使用して、Microsoft SharePoint 2016 の以下の NetScaler 機能を有効にして構成できます。

- ロードバランシング
- コンテンツスイッチング
- レスポンダー
- リライト

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

- 圧縮
- 統合キャッシュ

### ロードバランシング

NetScalerのロードバランシングは、バックエンドのSharePointサーバーにリクエストを均等に分散します。バックエンドサーバーのインテリジェントな監視により、誤動作しているサーバーにリクエストが送信されるのを防ぎます。

SharePoint StyleBookは、ドキュメント、画像、オーディオ、ビデオ、その他のファイルタイプなど、特定の種類のコンテンツのリクエストのロードバランシング専用の12個のロードバランシング仮想サーバーを設定します。

SharePoint StyleBookは、SSLベースのLB仮想サーバーを構成することで、SharePointアプリケーションのSSLモードをサポートするようになりました。フロントエンドプロトコルとしてSSLが選択されていることを確認してください。仮想ポートはデフォルトで443に設定されています。サービスグループ（SharePointアプリケーションサーバー）をターゲットのロードバランシング仮想サーバーにバインドするためにSSLを選択することもできます。バックエンドプロトコルはデフォルトでHTTPに設定されていることに注意してください。

### コンテンツスイッチング

コンテンツスイッチング機能は、特定の種類の要求されたSharePointコンテンツ（たとえば、ドキュメント、画像、オーディオまたはビデオファイル）に基づいて、複数のロードバランシング仮想サーバーにクライアントリクエストを分散するために使用されます。コンテンツスイッチングモジュールは、受信トラフィックを、その種類のコンテンツを処理できる最適なロードバランシング仮想サーバーに転送します。したがって、異なる種類のトラフィックに異なる最適化ポリシーを適用できます。たとえば、ビデオにはテキストドキュメントとは異なる圧縮ポリシーやキャッシュポリシーを使用したい場合があります。

### レスポンダー

NetScalerインスタンスのレスポンダー機能は、ユーザーをHTTPからHTTPSにシームレスにリダイレクトするために使用できます。レスポンダーは、カスタマイズされたエラーページを提供するように構成することもできます。レスポンダーポリシーは、アクションを実行する必要があるリクエスト（トラフィック）を決定し、各ポリシーをロードバランシング仮想サーバーにバインドします。SharePoint StyleBookには、ユーザーをHTTPからHTTPS URLにリダイレクトする構成が含まれています。

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

### リライト

リライトモジュールは、リクエスト/レスポンスヘッダー、URL、またはコンテンツをその場で変更するために使用されます。このモジュールはトラフィック処理と連携して動作するため、特定のユースケースに応じてトラフィックフローを変更できます。たとえば、リライトにより、ウェブサイトのサーバーに関する不要な詳細を公開することなく、要求されたコンテンツへのアクセスを提供できます。

SharePoint StyleBookでは、リライト機能を使用して、ユーザーリクエストから不要なヘッダーを削除します。

### 圧縮

NetScalerの圧縮エンジンは、圧縮可能なコンテンツを識別して圧縮します。このプロセスにより、データ転送時間が改善され、クライアントのネットワーク帯域幅要件が削減されると同時に、SharePointコンテンツサーバーのCPUサイクルが節約されます。NetScalerインスタンスは、静的データと動的に生成されたデータの両方を圧縮できます。GZIPまたはDEFLATE圧縮アルゴリズムを適用して、サーバー応答から余分な情報や反復的な情報を削除し、元の情報をよりコンパクトで効率的な形式で表現します。クライアントブラウザがデータを解凍できるかどうかは、GZIP、DEFLATE、またはその両方のうち、どのアルゴリズムをサポートしているかによって異なります。

NetScalerインスタンスは、HTML、XML、プレーンテキスト、カスケーディングスタイルシート（CSS）、およびMicrosoft Officeドキュメント内のテキストを圧縮するように構成されていますが、GIFまたはJPG形式の画像は圧縮しません。圧縮されたトラフィックの主な利点には、帯域幅コストの削減、WAN遅延の短縮、サーバーパフォーマンスの向上などがあります。

### 統合キャッシュ

NetScalerのインメモリキャッシュは、SharePointオブジェクトを保存して、頻繁に要求されるコンテンツをユーザーに迅速に配信できます。キャッシュされたコンテンツには、ダウンロードされたドキュメント、オーディオ、ビデオ、および画像ファイルが含まれます。

次の図は、NetScaler Consoleを使用してSharePoint StyleBook構成を展開するNetScalerインスタンスによってフロントエンドされたネットワークにおけるSharePointサーバーの展開を模式的に示しています。



## SharePoint StyleBook構成の展開

次のタスクは、ビジネスネットワークにMicrosoft SharePoint 2016 StyleBookを展開するのに役立ちます。

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

**Microsoft SharePoint 2016 StyleBookを展開するには：**

1. NetScaler Consoleで、**Applications** > **Administration** > **Configuration** の順に移動し、**Create New** をクリックします。

   **Choose StyleBook** ページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。

2. 下にスクロールして、**Microsoft SharePoint 2016 StyleBook** を選択します。

   **注**

   NetScaler Consoleで、**Applications** > **Configurations** > **StyleBooks** の順に移動します。下にスクロールして**Microsoft SharePoint 2016 StyleBook** を見つけ、**Create Configuration** をクリックします。

   StyleBookは、このStyleBookで定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスフォームとして開きます。

   次のパラメーターの値を入力します。

   a. **SharePointアプリケーション名**。ネットワークに展開するSharePoint構成の名前。

   b. **SharePoint仮想IP**。NetScalerインスタンスがMicrosoft SharePointアプリケーションのクライアント要求を受信する仮想IPアドレス。

   c. **SharePoint仮想ポート**。ユーザーがSharePointアプリケーションにアクセスするために使用するTCPポート。

   d. **SharePointフロントエンドプロトコル**。ドロップダウンリストからSharePointフロントエンドプロトコルを選択します。利用可能なオプションはHTTPまたはSSLです。

      **注**

      SSLを選択した場合は、このStyleBookのSharePoint詳細設定セクションでリライト構成パラメータが有効になっていることを確認してください。

   e. **SharePointサーバーIP**。ネットワーク内のすべてのSharePointサーバーのIPアドレス。

   f. **SharePointサーバーポート**。SharePointサーバーが使用するTCPポート番号。デフォルトでは80です。必要に応じてこの値を編集できますが、このポートがMicrosoft SharePoint 2016サーバーでアクセス可能であることを確認してください。

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

3. **SSL証明書設定**セクションで、+をクリックしてSSL証明書の名前、証明書キーを入力し、ローカルストレージフォルダからそれぞれのファイルを選択します。



4. 必要に応じて**詳細証明書設定**をクリックして、SSL証明書の有効期限監視を有効または無効にします。証明書の有効期限監視を有効にする場合は、証明書の有効期限が切れるまでの日数を設定すると、その日数後にNetScaler Consoleがアラームを発行します。また、OCSPチェックをオプション機能または必須機能にするオプションもあります。



5. SharePointの**詳細設定**セクションでは、NetScalerインスタンスで構成されるNetScaler機能を有効にできます。ロードバランシングとコンテンツスイッチング機能はデフォルトでインスタンスに構成されていますが、インスタンスに構成したい他の機能、つまりレスポンダー構成、リライト構成、圧縮構成、統合キャッシュ構成を選択できます。
6. **ターゲットインスタンス**をクリックし、このSharePoint構成を展開するNetScalerインスタンスを選択します。**作成**をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

**注**

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスをこのウィンドウの利用可能なインスタンスリストに追加することもできます。



**注**

実際の構成を実行する前に、**ドライラン**を選択して、ターゲットインスタンスに作成される構成オブジェクトを確認することをお勧めします。

構成が作成され、正常に展開されると、SharePoint StyleBookは1つのコンテンツスイッチング仮想サーバーと12のロードバランシング仮想サーバーを作成します。また、ポリシーとサービスグループを作成し、それらをロードバランシング仮想サーバーにバインドします。作成されるポリシーは、コンフィグパックの作成時にStyleBookで選択された機能によって異なります。

### NetScalerインスタンスで定義されたオブジェクトの表示

NetScaler Consoleでコンフィグパックが作成された後、SharePoint StyleBook用にNetScalerインスタンスで作成されたすべてのオブジェクトを表示できます。**Applications** > **Administration** >

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

**Configuration** に移動し、**View Objects Created** をクリックします。次の図は、「NetScaler ConsoleからのSharePoint StyleBook構成の展開」に示されている例で指定されたIPアドレスを持つ、作成されたオブジェクトの一部を示しています。



## Microsoft ADFS プロキシ StyleBook

Microsoft ADFS プロキシは、内部のフェデレーション対応リソースとクラウド リソースの両方にシングルサインオンアクセスを提供することで、重要な役割を果たします。クラウド リソースの一例として、Office 365 があります。ADFS プロキシ サーバーの目的は、インターネットからアクセスできない ADFS サーバーにリクエストを受信して転送することです。ADFS プロキシはリバース プロキシであり、通常、組織の境界ネットワーク (DMZ) に配置されます。ADFS プロキシは、リモート ユーザーの接続とアプリケーション アクセスにおいて重要な役割を果たします。

NetScaler は、セキュアな接続、認証、およびフェデレーション ID の処理を可能にする正確なテクノロジーを備えています。NetScaler を ADFS プロキシとして使用することで、DMZ に追加のコンポーネントをデプロイする必要がなくなります。

NetScaler Console の Microsoft ADFS プロキシ StyleBook を使用すると、NetScaler インスタンスで ADFS プロキシ サーバーを構成できます。

次の図は、NetScaler インスタンスをエンタープライズ DMZ 内の ADFS プロキシ サーバーとして展開した様子を示しています。



### NetScaler を ADFS プロキシとして使用する利点

1. ロードバランシングと ADFS プロキシの両方のニーズに対応
2. 内部および外部ユーザー アクセス シナリオの両方をサポート
3. 豊富な事前認証方法をサポート
4. ユーザーにシングルサインオン エクスペリエンスを提供
5. アクティブ プロトコルとパッシブ プロトコルの両方をサポート
    a. アクティブ プロトコル アプリの例: Microsoft Outlook、Microsoft Skype for Business
    b. パッシブ プロトコル アプリの例: Microsoft Outlook Web App、Web ブラウザ
6. DMZ ベースの展開向けに強化されたデバイス
7. 追加のNetScalerコア機能を使用することで価値を付加します。

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

a. コンテンツスイッチング
b. SSLオフロード
c. リライト
d. セキュリティ (NetScaler AAA)

アクティブなプロトコルベースのシナリオでは、Office 365に接続して資格情報を提供できます。Microsoft Federation Gatewayは、アクティブなプロトコルクライアントに代わってADFSサービス（ADFSプロキシ経由）に接続します。その後、ゲートウェイは基本認証（401）を使用して資格情報を送信します。NetScalerは、ADFSサービスへのアクセス前にクライアント認証を処理します。認証後、ADFSサービスはSAMLトークンをFederation Gatewayに提供します。Federation Gatewayは、クライアントアクセスを提供するために、そのトークンをOffice 365に送信します。

パッシブクライアントの場合、ADFSプロキシStyleBookはKerberos Constrained Delegation (KCD) ユーザーアカウントを作成します。KCDアカウントは、ADFSサーバーに接続するためのKerberos SSO認証に必要です。StyleBookは、LDAPポリシーとセッションポリシーも生成します。これらのポリシーは、パッシブクライアントの認証を処理するNetScaler AAA仮想サーバーに後でバインドされます。

StyleBookは、NetScaler上のDNSサーバーがADFS用に構成されていることも保証できます。

以下の構成セクションでは、アクティブおよびパッシブプロトコルベースのクライアント認証の両方を処理するようにNetScalerを設定する方法について説明します。

### 構成の詳細

以下の表に、この統合を正常に展開するために必要な最小ソフトウェアバージョンを示します。

| 製品 | 最小要件バージョン |
| --- | --- |
| NetScaler | 11.0、Advanced/Premiumライセンス |

以下の手順は、適切な外部および内部DNSエントリをすでに作成していることを前提としています。

### NetScaler Console から Microsoft ADFS プロキシ StyleBook 構成を展開する

以下の手順は、ビジネスネットワークで Microsoft ADFS プロキシ StyleBook を実装する際に役立ちます。

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

### Microsoft ADFS プロキシ StyleBook を展開するには

1. NetScaler Console で、**Applications** \> **StyleBooks** に移動します。**StyleBooks** ページには、NetScaler Console で使用できるすべての StyleBook が表示されます。
2. 下にスクロールして、**Microsoft ADFS proxy StyleBook** を見つけます。**Create Configuration** をクリックします。 StyleBook がユーザーインターフェイスページとして開き、この StyleBook で定義されているすべてのパラメーターの値を入力できます。
3. 次のパラメーターの値を入力します。

   a. **ADFS Proxy Deployment Name**。ネットワークに展開されている ADFS プロキシ構成の名前を選択します。

   b. **ADFS Servers FQDNs or IPs**。ネットワーク内のすべての ADFS サーバーの IP アドレスまたは FQDN (ドメイン名) を入力します。

   c. **ADFS Proxy Public VIP IP**。ADFS プロキシサーバーとして機能する NetScaler 上のパブリック仮想 IP アドレスを入力します。

   

4. **ADFS Proxy Certificates** セクションで、SSL 証明書と証明書キーの詳細を入力します。

   この SSL 証明書は、NetScaler インスタンス上に作成されたすべての仮想サーバーにバインドされます。

   ローカルストレージフォルダーからそれぞれのファイルを選択します。暗号化された秘密鍵を .pem 形式でロードするために、秘密鍵のパスワードを入力することもできます。

   

   「**Advanced Certificate Settings**」チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力できます。
5. SSL証明書にNetScalerにインストールするCA公開証明書が必要な場合は、オプションで「**SSL CA Certificate**」チェックボックスを選択できます。「**Advanced Certificate Settings**」セクションで「**Is a CA Certificate**」を選択していることを確認してください。
6. アクティブクライアントとパッシブクライアントの認証を有効にします。ユーザー認証のためにActive Directoryで使用されるDNSドメイン名を入力します。その後、アクティブクライアントまたはパッシブクライアント、あるいはその両方の認証を設定できます。
7. アクティブクライアントの認証を有効にするには、次の詳細を入力します。

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

**注**

アクティブクライアントのサポートを設定することはオプションです。

a. **ADFS Proxy Active Authentication VIP**。アクティブクライアントが認証のためにリダイレクトされるNetScalerインスタンス上の仮想認証サーバーの仮想IPアドレスを入力します。

b. **サービスアカウントのユーザー名**。NetScalerがユーザーをActive Directoryに認証するために使用するサービスアカウントのユーザー名を入力します。

c. **サービスアカウントのパスワード**。NetScalerがユーザーをActive Directoryに認証するために使用するパスワードを入力します。

8. 対応するオプションを有効にし、LDAP設定を構成することで、パッシブクライアントの認証を設定します。

**注**

パッシブクライアントのサポートを設定することはオプションです。

パッシブクライアントの認証を有効にするには、次の詳細を入力します。

a. **LDAP (Active Directory) ベース**。認証を許可するために、ユーザーアカウントがActive Directory (AD) 内に存在するドメインのベースドメイン名を入力します。例: dc=netscaler®,dc=com

b. **LDAP (Active Directory) Bind DN**。ADツリーを参照する権限を持つドメインアカウント（設定を容易にするためにメールアドレスを使用）を追加します。例: cn=Manager,dc=netscaler,dc=com

c. **LDAP (Active Directory) Bind DN Password**。認証のためにドメインアカウントのパスワードを入力します。

このセクションで値を入力する必要があるその他のフィールドは次のとおりです。

d. **LDAP Server (Active Directory) IP**。AD認証が正しく機能するように、Active Directoryサーバーの IPアドレスを入力します。

e. **LDAP Server FQDN name**。Active DirectoryサーバーのFQDN名を入力します。FQDN名はオプションです。ステップ1のようにIPアドレスまたはFQDN名を提供します。

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

f. **LDAP Server Active Directory port**。デフォルトでは、LDAPプロトコルのTCPおよびUDPポートは389ですが、セキュアLDAPのTCPポートは636です。

g. **LDAP (Active Directory) login username**。ユーザー名を「sAMAccountName」として入力します。

h. **ADFS Proxy Passive Authentication VIP**。パッシブクライアント用のADFSプロキシ仮想サーバーのIPアドレスを入力します。

**注**

「*」でマークされたフィールドは必須です。

9. オプションで、DNSサーバー用にDNS VIPを構成することもできます。

10. **ターゲットインスタンス**をクリックし、このMicrosoft ADFSプロキシ構成を展開するNetScalerインスタンスを選択します。**作成**をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

**注**

実際の構成を実行する前に、**ドライラン**を選択することをお勧めします。まず、StyleBookによってターゲットのNetScalerインスタンスに作成される構成オブジェクトを表示できます。その後、**作成**をクリックして、選択したインスタンスに構成を展開できます。

### 作成されたオブジェクト

NetScalerインスタンスにADFSプロキシ構成が展開されると、いくつかの構成オブジェクトが作成されます。次の画像は、作成されたオブジェクトのリストを示しています。

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

## Oracle e-ビジネス StyleBook

Oracle E-Business Suiteは、統合されたグローバルビジネスアプリケーションの最も包括的なスイートです。このスイートにより、組織はより良い意思決定を行い、コストを削減し、パフォーマンスを向上させることができます。以下のアプリケーションで構成されています。

- エンタープライズリソースプランニング (ERP)
- 顧客関係管理 (CRM)
- サプライチェーン管理 (SCM)

これらのコンピュータアプリケーションは、Oracleによって開発または買収されたものです。Oracle E-Business Suite 12.2 StyleBookを使用すると、選択したNetScalerインスタンスに構成を展開できます。

このStyleBookは、負荷分散仮想サーバー、サービスグループ、およびサービスリストで構成される負荷分散構成を作成します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドします。SSLを選択し、ローカルシステムからSSLファイルとキーファイルを提供することで、暗号化された通信を選択できます。

### Oracle E-Business Suite 12.2の構成を作成するには

1. NetScaler Consoleで、**Applications** > **Configuration > StyleBooks** に移動します。**StyleBooks** ページには、NetScaler Consoleで利用可能なすべてのStyleBookが表示されます。下にスクロールして、**Oracle E-Business Suite 12.2** を選択します。検索オプションを使用してStyleBookを検索することもできます。
2. StyleBookパネルで **Create Configuration** をクリックします。
3. ロードバランサー設定セクションで、ロードバランサーアプリケーションの名前と仮想IPアドレスを入力します。
4. 必要なプロトコルを選択します。ここにはHTTPとHTTPS/SSLの2つのオプションがあります。ポート番号を入力することもできます。
5. 負荷分散するネットワーク内のすべてのOracle E-Business Suiteアプリケーションサーバーの IPアドレスを入力します。**+** をクリックして、さらにサーバーIPアドレスを追加します。
6. **SSL Certificates Settings** セクションで、ローカルストレージから該当するファイルを選択します。**Advanced Certificate Settings** チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間などの詳細を設定できます。証明書の有効期限モニターを有効または無効にすることもできます。

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

構成を作成するターゲットのNetScalerインスタンスを選択し、**Create** をクリックします。



**ヒント**

このウィンドウで、最近検出されたNetScalerインスタンスをNetScaler Consoleから利用可能なインスタンスのリストに追加するには、更新アイコンをクリックすることもできます。更新アイコンは現在、NetScaler Consoleでのみ利用可能です。

## Citrix StoreFront™ スタイルブック

StoreFrontは、Citrix Virtual Apps and Desktopsサイトのアプリケーションとデスクトップを単一のストアに集約してユーザーに提供するエンタープライズアプリストアです。StoreFrontは、リソースをホストするサイトに対してユーザーを認証し、ユーザーがアクセスするアプリケーションストアとデスクトップを管理します。これは、エンタープライズアプリケーションストアをホストし、ユーザーが利用できるようにするアプリとデスクトップへのセルフサービスアクセスをユーザーに提供できます。

このStyleBookは、StoreFrontサーバーのNetScaler構成を定義します。このStyleBookを使用すると、StoreFrontサーバーを目的のNetScalerインスタンスに構成できます。SSLを選択し、ローカルシステムからSSLファイルとキーファイルを提供することで、暗号化された通信を選択できます。

### Citrix StoreFrontアプリケーションの構成を作成する

1. NetScaler Console GUIで、 **>** の順に移動します。
2. 検索バーで、 プロパティを使用して `Citrix StoreFront` を検索します。
3. Citrix StoreFront StyleBookで、 をクリックします。
4. 次の詳細を指定します。

   - **StoreFront名**: StoreFront名を指定します。StoreFront構成パックは、同じStoreFront名で作成されます。
   - **仮想IP (VIP)**: NetScalerインスタンスがクライアント要求を受信する仮想IPアドレスを指定します。
   - **StoreFrontサーバー**: NetScalerインスタンスで構成するStoreFrontサーバーのIPアドレスを指定します。
   - **HTTPSリダイレクトURL**: HTTPS要求がリダイレクトされるHTTPS URLを指定します。



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

5. セクションで、SSL証明書と証明書キーの名前を入力します。
6. ローカルストレージフォルダからそれぞれのファイルを選択します。秘密鍵のパスワードを入力して、PEM形式の暗号化された秘密鍵を指定することもできます。

   StoreFront StyleBookのSSL証明書設定を指定します(/en-us/netscaler-application-delivery-management-software/media/ssl-cert-sf-stylebooks.png)
7. 「**Advanced Certificate Settings**」チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力できます。
8. オプションで、SSL証明書がNetScalerにCA公開証明書をインストールする必要がある場合は、「**SSL CA Certificate for the authentication virtual IP**」チェックボックスを選択します。「**Advanced Certificate Settings**」セクションで「**Is a CA Certificate**」を選択していることを確認してください。
9. 「**Create**」をクリックします。
10. 「**Target Instances**」をクリックし、StoreFrontサーバーを設定するNetScalerインスタンスを選択します。
11. 「**Create**」をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

# カスタムStyleBookを作成して使用する

独自のStyleBookを作成してデプロイし、NetScaler Consoleにインポートして、構成オブジェクトを作成できます。APIを使用してStyleBookから構成を作成することもできます。

このドキュメントには、次の情報が含まれています。

## 開始する前に

StyleBookの作成を開始する前に、次の知識があることを確認してください。

- NITRO API。詳細については、Nitro APIドキュメントを参照してください。
- YAML

StyleBookファイルはYAML形式を使用します。YAML形式の詳細については、YAML構文を参照してください。

StyleBookを作成する際に注意すべきYAMLガイドラインのリストを次に示します。

- YAMLは大文字と小文字を区別します。

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

- YAMLは適切なインデントを必要とします
- 適切なインデントを作成するには、`<spacebar>`キーを使用します。`<tab>`キーは使用しないでください。`<tab>`キーを使用すると、StyleBookをMAサービスにインポートする際にコンパイルエラーが発生します。
- 文字列を引用符で囲まないでください。文字列に句読点（ダッシュ、コロンなど）が含まれている場合にのみ、文字列を引用符で囲んでください。数値を文字列として解釈したい場合は、数値を引用符で囲むか、StyleBookのstr()組み込み関数を使用してください。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off、TRUE/true/truthy/FALSE/False/false/falselyのようなリテラルはブール値と見なされ、それぞれtrueとfalseに相当します。これらを文字列として解釈するには、引用符で囲んでください。例：
  - "YES"
  - 「いいえ」
  - 「真」
  - 「偽」など。

**注**

StyleBookファイルをNetScaler Consoleにインポートする前に、ファイルがYAML形式に準拠していることを検証することをお勧めします。YAMLコンテンツを検証およびインポートするには、StyleBooksに組み込まれているYAMLバリデーターを使用することをお勧めします。

StyleBookを構成する際、**作成**および**削除**操作（POSTおよびDELETE HTTPメソッド）をサポートするNitro構成リソースのみを使用できます。詳細については、Nitro APIドキュメントを参照してください。

## StyleBookの構造

StyleBookを作成するには、StyleBookの文法、構文、および構造を理解する必要があります。標準的なStyleBookには、次のセクションがあります。

- **ヘッダー**: このセクションでは、StyleBookのIDを定義し、その機能について説明します。これは必須セクションです。
- **StyleBookのインポート**: このセクションでは、現在のStyleBookから参照する他のStyleBookを宣言します。StyleBookを作成するには、NetScaler NITRO構成StyleBookまたは他のStyleBookをインポートする必要があります。これは必須セクションです。

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

- **パラメーター**: このセクションでは、構成を作成するためにStyleBookで必要となるパラメーターを定義します。StyleBookが受け取る入力を記述します。これはオプションのセクションです。
- **コンポーネント**: このセクションでは、特定の構成のためにStyleBookによって作成されるエンティティ（構成オブジェクト）を定義します。このセクションはStyleBookの核と見なされます。コンポーネントは通常、パラメーターセクションで提供される入力を使用して、StyleBookによって生成される構成を調整します。これはオプションのセクションです。

  StyleBookには、パラメーターセクション、コンポーネントセクション、またはその両方を含めることができます。パラメーターセクションのみを持つStyleBookは、他のStyleBookで使用できるパラメーターのリストを定義するのに役立ちます。これにより、一連のStyleBook間でパラメーターグループの再利用が促進されます。コンポーネントセクションのみを持つStyleBookは、ユーザー入力を受け取るパラメーターを定義する代わりに、StyleBook内の属性の値を指定したい場合に使用できます。
- **出力**: パラメーターセクションがStyleBookの入力を定義するのに対し、このオプションのセクションはその出力を定義します。このオプションの出力セクションでは、このStyleBookから構成を作成するユーザー、およびこのStyleBookをインポートする他のStyleBookに公開したいコンポーネントを指定できます。ユーザーおよびインポートするStyleBookは、公開されたコンポーネントのプロパティを参照できます。
- **操作**: StyleBookには、StyleBookの一部である仮想サーバーでNetScaler ConsoleのAnalyticsを有効にするためのオプションセクションを含めることができます。

以下の図は、StyleBookの簡単な概要を示しています。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/stylebook-outline.png)

以下の例は、StyleBookの文法と構造、および複雑さのレベルを上げてStyleBookを作成する方法を学ぶのに役立ちます。

- 負荷分散仮想サーバーを作成するためのStyleBook(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks/create-load-balancing-virtual-server.html)
- 基本的な負荷分散構成を作成するためのStyleBook(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks/create-basic-load-balancing-configuration.html)
- 複合StyleBookを作成する(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks/create-composite-stylebook.html)

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

- GUI属性を使用してStyleBookをカスタマイズする(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks/use-gui-attributes.html)

## ロードバランシング仮想サーバーを作成するためのStyleBook

この例では、HTTPプロトコルタイプでポート80をリッスンするロードバランシング仮想サーバーを作成する基本的なStyleBookを設計します。仮想サーバー名、IPアドレス、およびロードバランシングメソッドのパラメーターは、ユーザー定義の値を受け入れます。つまり、これらがStyleBookのパラメーターとなります。

### ヘッダー

StyleBookの最初の6行はヘッダーセクションで構成されます。この例では、ヘッダーセクションは次のように記述されています。

```
name: lb-vserver

description: This StyleBook defines a load balancing virtual server
configuration.

display-name: Load Balancing Virtual Server (HTTP)

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"
```

ヘッダーセクションには、次の詳細が含まれます。

- **name**: このStyleBookの名前。
- **description**: このStyleBookが何をするかを定義する説明。この説明はNetScaler Consoleに表示されます。
- **display-name**: NetScaler Consoleに表示されるStyleBookのわかりやすい名前。
- **namespace**: 名前空間は、名前の競合を避けるためにStyleBookの一意の識別子の一部を形成します。
- **schema-version**: このリリースでは常に「1.0」の値を取ります。
- **version**: StyleBookのバージョン番号。StyleBookを更新するときにバージョン番号を変更できます。

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

**name**、**namespace**、および**version**の組み合わせは、システム内でStyleBookを一意に識別します。NetScaler Consoleでは、名前、名前空間、およびバージョンの組み合わせが同じ2つのStyleBookを持つことはできません。ただし、名前とバージョンは同じでも名前空間が異なるStyleBook、または名前空間とバージョンは同じでも名前が異なるStyleBookを持つことはできます。

**注**

StyleBookを更新し、バージョン番号も更新したとします。このStyleBookを他のStyleBookで参照している（つまりインポートしている）場合は、インポートされたStyleBookの正しいバージョンを使用するように、他のStyleBookのバージョン番号も更新してください。

### StyleBookのインポート

ヘッダーの後のセクションは「import-stylebooks」と呼ばれます。このセクションでは、現在のStyleBookで参照したい他のStyleBookのネームスペースとバージョン番号を宣言する必要があります。これにより、独自のStyleBookで同じ構成を再構築する代わりに、他のStyleBookをインポートして再利用できます。

この例では、import-stylebooksセクションは次のように記述されています。

```
import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"
```

すべてのStyleBookは、NITRO構成オブジェクトを直接使用する場合、netscaler.nitro.configネームスペースを参照する必要があります。このネームスペースには、lbvserverなどのすべてのNetScaler NITROタイプが含まれています。ソフトウェアバージョン10.5以降がサポートされているため、StyleBookを使用して、リリース10.5以降を実行している任意のNetScalerインスタンスで構成を作成および実行できます。

import-stylebooksセクションで使用されるプレフィックスは、ネームスペースとバージョンの組み合わせを参照するための短縮形です。この場合、nsはバージョン10.5のnetscaler.nitro.configを参照します。StyleBookの後のセクションでは、インポートされたStyleBookを参照するためにネー

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

ムスペースとバージョンを使用する代わりに、上記の例のように、選択したプレフィックス文字列（例：ns）を使用できます。

StyleBookで使用されるバージョンは、NetScaler NITROバージョンです。NitroバージョンXに基づいたStyleBookは、バージョンX以上の任意のNetScalerを構成するために使用できます。

**注**

StyleBookがバージョン10.5以降の任意のNetScalerインスタンスを構成できるようにするため、最大限の互換性を確保するために、Nitro組み込みStyleBookを直接使用するStyleBook（ネームスペース：netscaler.nitro.config、バージョン：10.5）にNitro 10.5ネームスペースをインポートすることをお勧めします。

他のStyleBookをインポートするStyleBookは、インポートするStyleBookと同じかそれ以上のNitroバージョンに基づいている必要があることが重要です。たとえば、Nitroバージョン10.5に基づいたStyleBookは、11.1に基づいたStyleBookに依存したり、使用したり、インポートしたりすることはできません。しかし、バージョン11.1に基づいたStyleBookは、11.1より前の任意のバージョンに基づいたStyleBookをインポートできます。

NitroネームスペースをまったくインポートしないStyleBookも可能です。つまり、StyleBookはNitroコンポーネントを直接定義する必要はありませんが、Nitroコンポーネントを定義するStyleBookをインポート（依存）できます。他のStyleBookをインポートするStyleBookは、常にその依存関係の階層で最高のNitroバージョンを取得し、したがって、そのバージョン以上のNetScalerを構成するために使用できます。

### パラメーター

パラメーターセクションでは、StyleBookで必要なすべてのパラメーターを宣言できます。StyleBook開発者として、StyleBookのユーザーに指定してもらいたい入力内容を決定する必要があります。この例では、仮想サーバーの名前、そのIPアドレス、および負荷分散方法をユーザーに提供させるようにStyleBookを構築しています。

パラメーターセクションは次のようになります。

```
parameters:

 -

  name: name

  type: string
```

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

```
  label: Application Name

  description: Name of the application configuration.

  required: true



 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: Application VIP that the clients access.

  required: true



-

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the load balancing algorithm (method) used for load
balancing client request between the application servers.

  allowed-values:

   - ROUNDROBIN

   - LEASTCONNECTION

   default: ROUNDROBIN
```

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

**注**

パラメーターのラベルを指定しない場合、NetScaler Consoleはこのパラメーターを表示する際にname属性を使用します。NetScaler Consoleでの表示方法を制御できるように、常にパラメーターのラベルを定義する必要があります。

ただし、APIを使用する場合、パラメーターはその名前で指定されます。
このセクションでは、仮想サーバー名を表す**name**、仮想サーバーのIPアドレスを表す**ip**、ロードバランシング方式を表す**lb-alg**という、**name**属性値で示される3つのパラメーターを宣言しました。

- **type**。これらのパラメーターが取りうる値のタイプ。例えば、nameとlb-algは文字列値を取ることができ、ip値はIPアドレスタイプである必要があります。StyleBookのパラメーターは、以下のいずれかの組み込みタイプにすることができます。
- **string**。文字の配列。長さが指定されていない場合、文字列値は任意の数の文字を取ることができます。ただし、min-length属性とmax-length属性を使用することで、文字列タイプの長さを制限できます。
- **number**。整数。min-value属性とmax-value属性を使用することで、このタイプが取りうる最小値と最大値を指定できます。
- **boolean**。trueまたはfalseのいずれかになります。また、すべてのリテラルはYAMLによってブール値と見なされることに注意してください（例：YesまたはNo）。
- **ipaddress**。有効なIPv4またはIPv6アドレスを表す文字列。
- **tcp-port**。TCPまたはUDPポートを表す0から65535までの数値。
- **password**。不透明な/秘密の文字列値。NetScaler Consoleがこのパラメーターの値を表示するときは、アスタリスク（*****）で表示されます。
- **certfile**。証明書ファイル。
- **keyfile**。証明書の秘密鍵ファイル。
- **file**。このタイプのパラメーターは、ユーザーがファイル（例：証明書またはキーファイル）をアップロードすることを要求します。
- **object**。複数の要素で構成され、これらの要素のそれぞれがパラメーターです。このタイプは、複数の関連するパラメーターを1つの親パラメーターの下にグループ化するために使用できます。
- **required**。パラメーターが必須かオプションかを示します。trueに設定されている場合、パラメーターは必須であり、ユーザーはこのStyleBookを使用して構成を作成する際にこのパラメーターの値を指定する必要があります。デフォルトでは、すべてのパラメーターはオプショ

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

ンです。この例では、**name**と**ip**は必須パラメーターであり、**lb-alg**はオプションパラメーターで、そのデフォルト値は「ROUNDROBIN」です。

**default**属性を使用して、オプションのパラメーターにデフォルト値を割り当てます。構成を作成する際に、ユーザーが値を指定しない場合、デフォルト値が使用されます。例えば、**lb-alg**パラメーターの場合、デフォルト値はROUNDROBINです。

**allowed-values**属性を使用して、構成を作成する際にユーザーが選択できる特定の値を定義します。この例では、**lb-alg**パラメーターにROUNDROBINとLEASTCONNECTIONの2つの値を指定しました。

StyleBookをインポートして使用すると、NetScaler Consoleにはこれら3つのパラメータを含むフォームが表示されます。nameとipに表示されるフィールドには文字列とipaddressタイプの値を入力でき、lb-algフィールドはデフォルト値としてROUNDROBINが選択されたドロップダウンリストとして表示されます。

**注**

組み込みタイプに加えて、パラメータは別のStyleBookをそのタイプとして持つことができます。これは、他のStyleBookで定義されたパラメータを再利用する方法です。

### コンポーネント

このStyleBookの最後のセクションはコンポーネントセクションと呼ばれ、StyleBookの中で最も重要なセクションと見なされます。このセクションでは、StyleBookによって作成される構成オブジェクトを定義します。

この例では、コンポーネントセクションを次のように記述する必要があります。

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: HTTP
```

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

```
    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg
```

この例には、1つのコンポーネントのみが含まれています。コンポーネントの主な属性は、name、type、およびpropertiesです。コンポーネントのタイプは、このコンポーネントが提供するプロパティを決定します。コンポーネントには次の2つのタイプがあります。

- **組み込み型**。このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITROエンティティタイプ「lbvserver」または「servicegroup」などです。この例では、組み込みコンポーネントタイプを使用しています。
- **複合型**。このタイプは、作成してNetScaler ConsoleにインポートしたStyleBook、またはNetScaler Consoleに付属しているデフォルトのStyleBookです。複合StyleBookの詳細については、「複合StyleBookの作成」を参照してください。

この例では、**lbvserver-comp**というコンポーネントを定義しました。このコンポーネントは**ns::lbvserver**（組み込みのNitroタイプ）タイプです。「ns」は、import-stylebooksセクションで指定した名前空間netscaler.nitro.configおよびバージョン10.5を参照するプレフィックスであり、「lbvserver」はこの名前空間のNitroリソースです。

ここで定義されている**properties**は、「lbvserver」リソースの属性です。利用可能なすべてのNetScaler Nitroリソースとその属性の詳細については、「NetScaler NITRO REST APIドキュメント」を参照してください。

このセクションのプロパティには、「lbvserver」リソースの必須属性が含まれており、これらの属性の値を指定できます。この例では、servicetypeとportに静的な値を指定していますが、name、ipv46、およびlbmethodプロパティは入力パラメータから値を取得します。StyleBookの残りの部分では、**$parameters.\<parameter-name\>**式（例: **$parameters.ip**）を使用して、parametersセクションで定義されたパラメータ名を参照できます。

**注**

慣例として、プレフィックス「ns」は、「import-stylebooks」セクションでNetScaler Nitro名前空間を指定するために常に使用されます。必須ではありませんが、Citrixは一貫性のために独自のStyleBookで同じ慣例を使用することを推奨しています。

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

### StyleBookを構築する

このStyleBookの必要なセクションをすべて定義したので、それらをまとめて最初のStyleBookを構築します。StyleBookの内容をテキストエディタにコピーして貼り付け、ファイルを**lb-vserver.yaml**として保存します。YAMLコンテンツを検証およびインポートするには、StyleBooksに組み込まれているYAMLバリデーターを使用することをお勧めします。

ファイルlb-vserver.yamlの全内容は以下のとおりです。

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

 -

  namespace: com.citrix.adc.stylebooks

  version: "1.0"

  prefix: stlb
```

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

```
parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION
```

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

```
components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler load balancing virtual server configuration object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
   lbmethod: $parameters.lb-alg
   servicetype: HTTP
   port: 80
```

StyleBookを使用して構成を作成するには、NetScaler Consoleにインポートしてから使用する必要があります。詳細については、「ユーザー定義StyleBookの使用方法」を参照してください。

このStyleBookを他のStyleBookにインポートすることもできます（import-stylebooksコンストラクトを使用）。または、次のセクションで説明するように、このStyleBookを修正して、より多くのパラメータとコンポーネントを含めることもできます。

## 基本的なロードバランシング構成を作成するためのStyleBook

前の例では、ロードバランシング仮想サーバーを作成するための基本的なStyleBookを構築しました。このStyleBookを別の名前で保存し、その後、基本的なロードバランシング構成のための追加のパラメーターとコンポーネントを含めるように更新できます。このStyleBookファイルを**basic-lb-config.yaml**として保存します。

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

このセクションでは、ロードバランシング仮想サーバー、サービスグループ、およびサービスリストで構成されるロードバランシング構成を作成する新しいStyleBookを設計します。また、サービスをサービスグループにバインドし、サービスグループを仮想サーバーにバインドします。

### ヘッダー

このStyleBookを構築するには、ヘッダーセクションを更新することから始める必要があります。このセクションは、ロードバランシング仮想サーバーStyleBook用に作成したものと同様です。ヘッダーセクションで、**name**の値をbasic-lb-configに変更します。また、このStyleBookを適切に説明するために、**description**と**display-name**を更新します。**namespace**と**version**の値は変更する必要はありません。名前を変更したため、名前、名前空間、およびバージョンの組み合わせにより、システム内でこのStyleBookの一意の識別子が作成されます。

```
name: basic-lb-config

description: This StyleBook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"
```

### StyleBookのインポート

import-stylebooksセクションは変更ありません。これはnetscaler.nitro.config名前空間を参照し、Nitro構成オブジェクトを使用します。

```
import-stylebooks:

 -

 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

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

### パラメーター

パラメーターセクションを更新して、サービスまたはサーバーのリストと、サービスがリッスンするポートを定義するための2つの追加パラメーターを追加する必要があります。最初の3つのパラメーター、name、ip、およびlb-algは変更ありません。

```
parameters:

 -

 name: name

 type: string

 label: Application Name

 description: Name of the application configuration

 required: true

  -

   name: ip

   type: ipaddress

   label: Application Virtual IP (VIP)

   description: Application VIP that the clients access

   required: true

  -

   name: lb-alg

   type: string

   label: LoadBalancing Algorithm

   description: Choose the load balancing algorithm used for load
balancing client requests between the application servers.
```

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

```
      allowed-values:

      - ROUNDROBIN

      - LEASTCONNECTION

       default: ROUNDROBIN

   -

    name: svc-servers

    type: ipaddress\[\]

    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true

   -

    name: svc-port

    type: tcp-port

    label: Server Port

    description: The TCP port open on the application servers to receive
 requests.

    default: 80
```

この例では、アプリケーションのバックエンドサーバーを表すサービスのIPアドレスのリストを受け入れるために、パラメーター**svc-servers**が追加されます。これは、**required: true**で示されるように必須パラメーターです。2番目のパラメーター**svc-port**は、サーバーがリッスンするポート番号を示します。ユーザーによって指定されない場合、svc-portパラメーターのデフォルトポート番号は80です。

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

### コンポーネント

コンポーネントセクションも更新して、2つの新しいパラメーターを使用し、完全なロードバランシング構成を構築するような追加のコンポーネントを定義する必要があります。

この例では、コンポーネントセクションを次のように記述する必要があります。

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP

   ipv46: $parameters.ip

   port: 80

   lbmethod: $parameters.lb-alg



components:

 -

  name: svcg-comp

  type: ns::servicegroup

  properties:

   name: $parameters.name + "-svcgrp"

   servicetype: HTTP
```

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

```
components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver\_servicegroup\_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
  name: members-svcg-comp
  type: ns::servicegroup\_servicegroupmember\_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
```

この例では、元のコンポーネント**lbvserver-comp**（前の例から）は、現在、**svcg-comp**という子コンポーネントを持っています。そして、**svcg-comp**コンポーネントは、その中に2つの子コンポーネントを持っています。あるコンポーネント内に別のコンポーネントをネストすると、ネストされたコンポーネントが親コンポーネントの属性を参照することによって構成オブジェクトを作成できるようになります。ネストされたコンポーネントは、親コンポーネントで作成された各オブジェクトに対して1つ以上のオブジェクトを作成できます。

**svcg-comp**コンポーネントは、リソース「servicegroup」の属性に提供された値を使用して、NetScalerインスタンス上にサービスグループを作成するために使用されます。この例では、

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

servicetypeに静的な値を指定していますが、nameはその値を入力パラメーターから取得します。パラメーターセクションで定義されたパラメーター**name**は、**$parameters.name + "-svcgrp"という表記を使用して参照されます。ここで、-svcgrp**はユーザー定義の名前に付加（連結）されます。

コンポーネント **svcg-comp** には、**lbvserver-svg-binding-comp** と **members-svcg-comp** の2つの子コンポーネントがあります。

最初の子コンポーネントである **lbvserver-svg-binding-comp** は、その親コンポーネントによって作成されたサービスグループと、親の親コンポーネントによって作成された負荷分散仮想サーバー (lbvserver) の間の構成オブジェクトをバインドするために使用されます。$parent 表記は、親参照とも呼ばれ、親コンポーネント内のエンティティを参照するために使用されます。たとえば、**servicegroupname: $parent.properties.name** は親コンポーネント **svcg-comp** によって作成されたサービスグループを参照し、**name: $parent.parent.properties.name** は親の親コンポーネント **lbvserver-comp** によって作成された仮想サーバーを参照します。

**members-svcg** コンポーネントは、サービスリストと親コンポーネントによって作成されたサービスグループの間で構成オブジェクトをバインドするために使用されます。複数のバインディング構成オブジェクトの作成は、StyleBook の **repeat** 構造を使用して、パラメータ **svc-servers** で指定されたサーバーのリストを反復処理することで実現されます。反復処理中に、この StyleBook コンポーネントは、サービスグループ内の各サービス（**repeat-item** 構造では srv と呼ばれます）に対して **servicegroup_servicegroupmember_binding** 型の Nitro 構成オブジェクトを作成し、各 Nitro 構成オブジェクトの **ip** 属性を対応するサーバーの IP アドレスに設定します。

一般的に、コンポーネント内で **repeat** および **repeat-item** 構造を使用すると、そのコンポーネントが同じタイプの複数の構成オブジェクトを構築できるようになります。**repeat-item** 構造に変数名（例: srv）を割り当てて、反復処理における現在の値を指定できます。この変数名は、同じコンポーネントのプロパティまたは子コンポーネントで **$\<varname\>**（例: $srv）として参照されます。

上記の例では、この構成を簡単に構築するために、コンポーネントのネストを使用しました。この特定のケースでは、コンポーネントのネストが構成を構築する唯一の方法ではありませんでした。以下に示すように、ネストなしで同じ結果を達成することもできました。

```
components:

 -

  name: members-svcg-comp
```

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

```
 type: ns::servicegroup\_servicegroupmember\_binding
 repeat: $parameters.svc-servers
 repeat-item: srv
 properties:
  ip: $srv
  port: str($parameters.svc-port)
  servicegroupname: $components.svcg-comp.properties.name
-
 name: lbvserver-svg-binding-comp
 type: ns::lbvserver\_servicegroup\_binding
 properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.name
-
 name: lbvserver-comp
 type: ns::lbvserver
 properties:
  name: $parameters.name + "-lb"
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg
```

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

```
-

 name: svcg-comp

 type: ns::servicegroup

 properties:

 name: $parameters.name + "-svcgrp"

 servicetype: HTTP
```

ここでは、すべてのコンポーネントが同じレベル（つまり、ネストされていない）ですが、達成される結果（生成される NetScaler 構成）は、以前に使用されたネストされたコンポーネントの場合と同じです。また、StyleBook でコンポーネントが宣言される順序は、構成オブジェクトの作成順序には影響しません。この例では、**svcg-comp** と **lbvserver-comp** のコンポーネントは、最後に宣言されているにもかかわらず、2番目のコンポーネント **lbvserver-svg-binding-comp** を構築する前に構築する必要があります。これは、2番目のコンポーネントにこれらのコンポーネントへの前方参照があるためです。

**注**

慣例として、StyleBook、パラメータ、置換、コンポーネント、および出力の名前は小文字で記述されます。複数の単語を含む場合は、「-」文字で区切られます。たとえば、「lb-bindings」、「app-name」、「rewrite-config」などです。もう1つの慣例は、コンポーネント名に「-comp」という文字列を接尾辞として付けることです。

## 出力

新しい StyleBook に追加できる最後のセクションは、出力セクションです。ここでは、この StyleBook が構成の作成に使用された後、ユーザー（または他の StyleBook）に何を公開するかを指定します。たとえば、この StyleBook によって作成される lbvserver およびサービスグループ構成オブジェクトを公開するように出力セクションで指定できます。

```
outputs:

 -

  name: lbvserver-comp
```

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

```
  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

 -

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

StyleBook の出力セクションはオプションです。StyleBook は出力を返す必要はありません。ただし、一部の内部コンポーネントを出力として返すことで、複合 StyleBook を作成する際にわかるように、この StyleBook をインポートする StyleBook に柔軟性をもたらします。

**注**

コンポーネントの単一のプロパティ（たとえば、$components.lbvserver-comp.properties.name ではなく、$components.lbvserver-comp 全体）ではなく、StyleBook のコンポーネント全体を出力セクションで公開することをお勧めします。また、特定の出力が何を表すかを説明する記述を出力に追加してください。

### StyleBook を構築する

この StyleBook の必要なすべてのセクションを定義したので、それらをすべてまとめて2番目の StyleBook を構築します。この StyleBook ファイルはすでに **basic-lb-config.yaml** として保存されています。StyleBooks ページに組み込まれている YAML バリデーターを使用して、YAML コンテンツを検証およびインポートすることをお勧めします。

ファイル **basic-lb-config.yaml** の全内容は以下のとおりです。

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"
```

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

```
display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true
```

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

```
 -

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true



components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:
```

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

```
    name: $parameters.name + "-lb"
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
  -
   name: svcg-comp
   type: ns::servicegroup
   properties:
     servicegroupname: $parameters.name + "-svcgrp"
     servicetype: HTTP


  -
   name: lbvserver-svg-binding-comp
   type: ns::lbvserver_servicegroup_binding
   properties:
    name: $components.lbvserver-comp.properties.name
    servicegroupname: $components.svcg-comp.properties.servicegroupname
  -
   name: members-svcg-comp
   type: ns::servicegroup_servicegroupmember_binding
   repeat: $parameters.svc-servers
```

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

```
  repeat-item: srv

  properties:

   ip: $srv

   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname

outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

StyleBook を使用して構成を作成するには、NetScaler Console にインポートしてから使用する必要があります。詳細については、「ユーザー定義のStyleBookを使用する方法」を参照してください。

このStyleBookを他のStyleBookにインポートし、次のセクションで説明するようにそのプロパティを使用することもできます。

## 複合StyleBookを作成する

StyleBookの重要かつ強力な機能の1つは、他のStyleBookの構成要素として使用できることです。StyleBookは別のStyleBookにインポートでき、Nitroの組み込みStyleBookと同様に、2番目のStyleBookのコンポーネントで使用される**タイプ**として参照できます。

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

例えば、前のセクションで作成した**basic-lb-config** StyleBookを使用して、**composite-example**という別のStyleBookを作成できます。「basic-lb-config」StyleBookを使用するには、新しいStyleBookのimport-stylebooksセクションでインポートする必要があります。

### StyleBookを構築する

新しいStyleBookは次のようになります。

```
name: composite-example

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (HTTP/RoundRobin)

description: This StyleBook defines a RoundRobin load balancing
configuration with a monitor.

schema-version: "1.0"

import-stylebooks:

  -

   namespace: netscaler.nitro.config

   version: "10.5"

   prefix: ns

  -

   namespace: com.example.stylebooks

   version: "0.1"

   prefix: stlb

parameters:

  -
```

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

```
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true


  -
    name: response-code
    type: string[]
    label: List of Response Codes
```

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

```
    description: List of Response Codes - Provide a list of response codes
in integer.



components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config

    description: This component's type is another StyleBook that builds
the NetScaler lbvserver, servicegroups and services configuration objects.

    properties:

     name: $parameters.name

     ip: $parameters.ip

     svc-servers: $parameters.svc-servers

  -

     name: monit-comp

     type: ns::lbmonitor

     description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.

     properties:

       monitorname: $parameters.name + "-mon"

       type: HTTP

       respcode: $parameters.response-code

       httprequest: "'GET /'"
```

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

```
        lrtm: ENABLED

        secure: "YES"



      components:

         -

           name: monit-svcgrp-bind-comp

           type: ns::servicegroup_lbmonitor_binding

           properties:

             servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname

             monitor_name: $parent.properties.monitorname
```

import-stylebooksセクションでは、basic-lb-config StyleBookをその名前空間とバージョンを使用してインポートします。これらはプレフィックス「stlb」で参照されます。

componentsセクションでは、2つのコンポーネントが定義されています。最初のコンポーネントは**stlb::basic-lb-config**タイプです。「basic-lb-config」は、基本的な負荷分散構成を作成するためのStyleBookで作成したStyleBookの名前です。このコンポーネントに定義されているプロパティは、basic-lb-config StyleBookで宣言されている必須パラメーターに対応しています。ただし、StyleBookの任意のパラメーター（必須およびオプションの両方）を使用できます。lbvserver、サービスグループ、サービスとサービスグループのバインディングを再構築する代わりに、これらすべてを実行するStyleBookをコンポーネントとしてインポートし、それを使用して新しいStyleBookでこれらの構成オブジェクトを作成します。

StyleBookは、Nitroリソース「lbmonitor」（組み込みStyleBook）の属性を使用してモニター構成オブジェクトを作成する2番目のコンポーネント「monit-comp」を追加します。また、モニターを最初のコンポーネントで作成されたサービスグループにバインドするバインディング構成オブジェクトを作成するためのサブコンポーネント「monit-svcgrp-bind-comp」も含まれています。「basic-lb-config」StyleBookで作成されたサービスグループコンポーネントは出力として公開されているため、このStyleBookは式**$components.basic-lb-comp.outputs.servicegroup-comp**を使用してそれにアクセスできます。これは、インポートするStyleBookが、そうでなければアクセ

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

スできなかったインポートされたStyleBook内のコンポーネントにアクセスするために、outputsセクションをどのように使用できるかを示す例です。

次に、StyleBookの内容をテキストエディターにコピーして貼り付け、ファイルを**composite-example.yaml**として保存します。NetScaler Consoleにファイルをインポートする前に、YAMLコンテンツを検証してください。その後、NetScaler Consoleにインポートし、このStyleBookを使用して1つまたは複数の構成を作成します。

YAMLコンテンツを検証およびインポートするには、StyleBookに組み込まれているYAMLバリデーターを使用することをお勧めします。

## カスタムStyleBookでGUI属性を使用する

NetScaler Consoleに表示されるときにフィールドを直感的にするために、StyleBookのパラメータセクションにGUI属性を追加できます。

**例**。label属性を使用してパラメータに説明的な名前を追加し、description属性を使用してこのパラメータにツールチップを追加できます。

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.

type: ipaddress

required: true
```

**例**。オブジェクト型のパラメータがある場合、**gui**属性を使用してレイアウトを定義できます。この例では、レイアウトはフィールドが2つの列に表示される折りたたみ可能なオブジェクトです。

```
name: svcg-advanced

label: Advanced Application Server Settings

type: object

required: false

gui:
```

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

```
  collapse_pane: true

  columns: 2
```

**例**。NetScaler Console上の一部のStyleBookは、他のStyleBookの構成要素としてのみ使用されます。そのため、ユーザーがこれらのStyleBookから直接構成を作成することを望まない場合があります。これらのStyleBookは他のStyleBookの一部として使用されるためです。NetScaler Console GUIで構成を直接作成するためにStyleBookが使用されないように、StyleBookをプライベートとしてマークしてください。

```
name: basic-lb-config

description: This stylebook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

private: true

schema-version: "1.0"

version: "0.1"
```

## カスタムStyleBookをインポートする

StyleBookを作成したら、それを使用するためにNetScaler Consoleにインポートする必要があります。NetScaler Consoleでは、単一のStyleBookをYAML形式で、または複数のStyleBook YAMLファイルを.zip、.tgz、または.gz形式のバンドルとしてインポートできます。NetScaler Consoleシステムは、インポート時にStyleBookを検証します。これで、StyleBookは構成の作成に使用できるようになります。

NetScaler Consoleには、StyleBookのYAMLコンテンツを作成するために使用できる組み込みのYAMLエディターも用意されています。YAMLエディターを使用すると、NetScaler Console GUIから直接YAML構造を検証できます。これらの検証チェックのために別のツールを使用する必要はありません。コンテンツはYAML標準に対して検証され、逸脱がある場合は強調表示されます。その後、コンテンツを修正し、StyleBookをNetScaler Consoleにインポートできます。組み込みのYAMLエディターは、独自のStyleBookを作成する際に2つの利点を提供します。

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

- **色分け**。エディターはYAMLガイドラインに従って解析されたStyleBookコンテンツを表示し、色分けによりYAMLコンテンツで定義されているキーと値を簡単に区別できます。
- **YAML検証**。入力中にYAMLエラーがないかコンテンツが検証され、逸脱がある場合はすぐに強調表示されます。この検証により、NetScaler ConsoleにStyleBookをインポートする前でも、YAMLガイドラインに準拠したテキストを作成できます。

**注:**

現在、エディターはYAMLガイドラインに従ってコンテンツを検証します。コードの正確性や入力ミスは検証しません。

### StyleBookをインポートするには

1. NetScaler Consoleで、**Applications** > **Configuration** > **StyleBooks** の順に移動し、**Import New StyleBook** をクリックします。
2. StyleBookをインポートするには、次のいずれかのオプションをクリックします。

   - **ファイル** - ローカルストレージから必要なファイルまたはファイルのバンドルを選択します。

     **注:**

     この例では、StyleBook to Create a Load Balancing Virtual Server で作成した `lb-vserver.yml` StyleBook をインポートします。

     

   - **バンドル** - NetScaler Consoleでは、複数のStyleBookをYAML形式でインポートできます。zip (.zip) 形式またはtarball (.tgz、.gz) 形式で圧縮された複数のYAML StyleBookファイルをインポートできます。

     

     バンドル内の各StyleBookにアイコンを含めることができるようになりました。PNG、GIF、またはJPEG形式のアイコンを含むリソースフォルダがあることを確認してください。アイコンファイル名がStyleBook名と一致する場合、アイコンは自動的にStyleBookにマッピングされます。そうでない場合は、次の手順を実行します。

     a. リソースフォルダに `icon_mapping.json` ファイルを追加します。

     b. `icon_mapping.json` ファイルでStyleBookとアイコンを次のようにマッピングします。

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

```
<StyleBook file name> : <icon file name>
```

以下はStyleBookバンドルの例です。

- `resources`フォルダには必要なアイコンが含まれています。
- この例では、`sharepoint.yaml`ファイルと`skype.yaml`ファイルはそれぞれ`sharepoint.jpeg`と`skype.png`に自動的にマッピングされます。

`exchange.yaml`を`exch.png`にマッピングするには、`icon_mapping.json`ファイルで次のように指定します。

```
{

"exchange.yaml":"exch.png"

}
```

`defaulticon`エントリを指定すると、StyleBookは別のアイコンにマッピングされていない限り、デフォルトのアイコンにマッピングされます。

```
defaulticon: <icon file name>
```

**Applications > StyleBooks**で、インポートされたStyleBookはマッピングされたアイコンとともに表示されます。

- **Raw** - YAMLエディタでStyleBookのコンテンツを作成します。

StyleBookの文法エラーをチェックするために、StyleBookのコンテンツを検証できます。StyleBookのコンテンツを検証するには、**Validate Contents**をクリックします。

**注:**

StyleBookを作成する際は、以下の概念を理解していることを確認してください。

- NITRO API
- YAML

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

独自のStyleBookの作成方法の詳細については、独自のStyleBookの作成方法を参照してください。



- **リポジトリの同期** - このオプションには、NetScaler Consoleに追加されたリポジトリが一覧表示されます。NetScaler Consoleと同期するリポジトリを選択します。

**注:**

StyleBook YAMLファイルの内容をYAMLエディターにコピー＆ペーストすることもできます。

3. オプションで、StyleBookのアイコンを選択します。

   **アプリケーション > StyleBook**で、インポートされたStyleBookがこのアイコンとともに表示されます。

4. **作成**をクリックします。

   NetScaler Consoleは、StyleBookの文法に従って、すべての構文エラーと意味エラーについてStyleBookを検証します。エラーがある場合、StyleBookはNetScaler Consoleにインポートされません。

   エラーがない場合、StyleBookは正常にインポートされ、**StyleBooks**ページに表示されます。StyleBookのヘッダーセクションで定義した表示名でStyleBookを識別できます。

   **注:**

   ファイルのバンドルをインポートする場合、NetScaler Consoleは圧縮されたフォルダーを解凍し、すべてのStyleBookを検証します。 StyleBookファイルのいずれか1つでも検証テストに失敗すると、バンドルはインポートされません。

   StyleBookの文法、およびさまざまな構成要素と属性の構文の詳細については、「StyleBookの文法」を参照してください。

5. このStyleBookから構成を作成するには、**［構成の作成］**リンクをクリックします。

   StyleBookは、このStyleBookで定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして開きます。

6. パラメーターに必要な値を指定します。

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

次の例では、,

a. **アプリケーション名**と**ロードバランサーIPアドレス**の必須フィールドを指定します。

b. リストから**ロードバランシングアルゴリズム**を選択します。デフォルトでは、**ROUNDROBIN**が選択されています。

7. **［ターゲットインスタンス］**で、構成を展開するNetScalerインスタンスのIPアドレスを選択します。

   必要な数のターゲットインスタンスを指定することで、複数のNetScalerに構成を展開することもできます。

8. 構成を展開する前にNetScaler（NITRO）構成オブジェクトでテストする場合は、**［ドライラン］**をクリックします。

   構成が有効な場合、指定された値に基づいて構成オブジェクトが作成されます。

   この例では、StyleBookは`lbvserver`タイプのオブジェクトを1つだけ作成します。このロードバランシングサーバーは、この基本的な例のStyleBookで定義された唯一のコンポーネントでした。

   その後、**［作成］**をクリックして、選択したNetScalerインスタンスに構成を展開します。

構成が正常に展開されると、新しい構成パックが**［構成］**ページに表示されます。

**注：**

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスをこのウィンドウの利用可能なインスタンスのリストに追加することもできます。

## カスタムStyleBookを検索する

NetScaler Consoleでは、StyleBookをそのタイプに基づいて検索できるようになりました。つまり、デフォルトのStyleBookまたはカスタムStyleBookのいずれかを検索できます。このオプションは、多数のデフォルトStyleBookの中からユーザー定義のStyleBookを検索する必要がある場合に特に役立ちます。

### カスタムStyleBookを検索するには

1. NetScaler Consoleで、**Applications** > **Configurations** > **StyleBooks** に移動します。
2. 右上隅にある検索アイコンをクリックします。
3. 検索バーで、**Type** を選択し、サブリストから **Custom** を選択します。

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

4. NetScaler Consoleには、ユーザー定義のStyleBookのみが表示されます。

## 構成パックの作成と編集

NetScaler Consoleでは、StyleBookから構成パックを作成できます。構成パックは、作成元のStyleBookに紐付けられます。構成パックへの更新は、紐付けられているStyleBookを介して行われます。

### 構成パックの作成

StyleBookから構成パックを作成するには、以下を実行します。

1. **Applications > StyleBooks > Configurations** に移動します。
2. **Add** をクリックします。
3. **Choose StyleBooks** で、構成パックを作成する必要なStyleBookを選択します。

   このページでは、StyleBookがデフォルトStyleBookとカスタムStyleBookに分類されます。必要なStyleBookを見つけるには、それぞれのタブを選択します。
4. アプリケーション名、IPアドレス、ポート、プロトコルタイプなどの必要な詳細を指定します。

   GUIフィールドはStyleBookによって異なります。
5. **Target Instances** で、構成を実行するインスタンスまたはインスタンスグループを選択します。

   **注:**

   必要な数のターゲットインスタンスを指定することで、複数のNetScalerに構成を展開できます。
6. **Dry Run** をクリックします。

   **Objects** ページには、NetScalerインスタンスから作成、変更、または削除されるオブジェクトが表示されます。
7. **作成**をクリックします

   構成パックは、**StyleBook > 構成**ページに表示されます。

既存の構成パックを編集する場合は、構成パックを選択し、**編集**をクリックします。

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

### StyleBook の外部で作成された構成を再利用し、ConfigPack 間で構成を共有する

特定の運用上のニーズやレガシー設定により、Stylebook の外部で NetScaler® 構成を作成したことがあるかもしれません。これらの既存の構成を Stylebook 構成パックの一部として統合および管理できるようになり、より柔軟で一元的な管理が可能になります。

たとえば、この機能が導入される前は、NetScaler がすでに SSL プロファイルで構成されており、StyleBook の構成パック操作が同じ名前の SSL プロファイルを作成しようとすると、構成パック操作は「リソースがすでに存在します」というエラーで失敗していました。この機能が有効になったことで、構成パック操作は成功し、同じ名前の既存の SSL プロファイルを新しい構成パックで再利用できるようになりました。

同様に、ネットワーク設定、セキュリティポリシー、アプリケーション構成の一部などのリソースが複数のアプリケーションまたは構成で必要となるシナリオに直面することもあります。この機能により、複数の構成パック間で構成を共有できます。

この機能を有効にするには、次の手順に従います。

1. アプリケーション > 構成 > Stylebooks に移動します。
2. Stylebooks ページで、新しい構成パックの作成に使用する Stylebook、または編集中の構成パックに関連付けられている Stylebook を選択します。
3. 「アクションの選択」で、「設定の構成」をクリックします。
   
   
4. 次のいずれかまたは両方のオプションを選択して、設定を調整します。
   - 構成を作成する際に NetScaler 上の既存のリソースの再利用を有効にするには、**構成の作成中に NetScaler 上の既存のリソースの再利用を許可する**オプションを選択します。
   - 構成を削除する際に NetScaler 上で再利用されたリソースを保持するには、**構成の削除時に NetScaler 上で再利用されたリソースを保持しますか？**オプションを選択します。このオプションは、それらを参照する最後の構成パックが削除された場合でも、Stylebook の外部で元々作成されたリソースを NetScaler 上に保持し、それらの継続的な可用性を保証します。
5. 「**OK**」をクリックします。

### config packのStyleBookを変更する

機能を追加したり、問題を修正したりするために、StyleBookを更新する必要がある場合があります。以前のStyleBookを使用してconfig packをすでに作成している場合、新しい更新された

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

StyleBookを使用するようにそれらを更新したい場合があります。新しいStyleBookを使用するには、config packの既存のStyleBookを変更します。

NetScalerインスタンスに基本的なロードバランサー構成を展開する例のStyleBook「**example-lb**」を考えてみましょう。そして、このStyleBookからconfig pack CP1を作成します。

基本的なロードバランサー構成でモニターを構成したい場合、新しいStyleBookが必要です。したがって、基本的なロードバランサー構成とともにモニターを構成する機能を含む「**example-lb-mon**」StyleBookを作成します。

StyleBookを作成したら、既存のconfig pack CP1を更新してモニターを追加します。これを行うには、次の手順を実行します。

1. **Applications > StyleBooks > Configurations**に移動します。
2. StyleBookを変更するconfig packを選択します。

   この例では、リストからCP1を選択します。
3. 「**Change StyleBook**」をクリックします。
4. リストから必要なStyleBookを選択します。次に、「**Save Selection**」をクリックします。
5. 「**Change**」をクリックします。

   この例では、リストから「**example-lb-mon**」を選択します。

   config packのStyleBookを変更すると、新しいStyleBookのパラメーターは既存のStyleBookとは異なる構造を持つ場合があります。パラメーター構造が以前のStyleBookと類似している場合、パラメーターの値はそれぞれのフィールドに自動的に保持されます。そうでない場合、2つのStyleBook間で同じ構造を持つパラメーターのみが転送されます。たとえば、同じパラメーター名、タイプ、パラメーター親などです。

   config packのStyleBookを変更する(/en-us/netscaler-application-delivery-management-software/media/change-stylebook-configpack.gif)

   新しいStyleBookで新しい必須パラメータが追加された場合、StyleBookを変更した後、それらのパラメータの値を手動で指定する必要があります。

   この例では、**example-lb** StyleBookの構成ページに表示されるパラメータは次のとおりです。

   例のロードバランシング構成パック(/en-us/netscaler-application-delivery-management-software/media/nmas-migrate-configpack-3.png)

   新しい**example-lb-mon** StyleBookの構成ページに表示されるパラメータは次のとおりです。

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

構成パック移行後のパラメータの例(/en-us/netscaler-application-delivery-management-software/media/nmas-migrate-configpack-4.png)

この場合、新しいStyleBookは既存のパラメータを変更していないため、StyleBookは基本的なロードバランサー構成の古い値を保持します。そして、新しいパラメータのみを追加します。モニターパラメータについては、必要な値を手動で指定してください。

6. **ターゲットインスタンス**で、選択したインスタンスを確認し、必要に応じてリストを更新します。
7. **ドライラン**をクリックします。

   **オブジェクト**ページには、NetScalerインスタンスで作成、変更、または削除されるオブジェクトが表示されます。
8. **OK**をクリックします。

   **StyleBook > 構成**ページで、**StyleBook名**列には、選択した構成パックの新しいStyleBook名が表示されます。この場合、**example-lb-mon**と表示されます。

### 複数の構成パックを持つStyleBookを変更する

複数の構成パックを持つ既存のStyleBookを変更する場合は、次の手順を実行します。

1. 新しいStyleBookをNetScaler Consoleにインポートします。

   通常、新しいStyleBookは、既存のStyleBookよりも高いバージョンで同じ名前と名前空間を持ちます。ただし、名前、名前空間、またはバージョンが異なる場合は、この手順をスキップできます。
2. 既存のStyleBookに関連付けられているconfig packのStyleBookを変更します。

   選択したconfig packが同じStyleBookに関連付けられている場合にのみ、**StyleBookの変更**を選択できます。

   選択したconfig packについて、NetScaler Consoleは以下の条件が満たされた場合にStyleBookを正常に変更します。

   - 既存のStyleBookのすべての構成パラメータは、選択したStyleBookに存在する必要があります。
   - 選択したStyleBookからの新しいパラメータはオプションです。

   選択したconfig packの進行状況を確認するには、**Configurations**ページで**進行中/失敗した構成**を選択します。

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

3. すべてのconfig packが新しいStyleBookに紐付けられたら、NetScaler Consoleから古いStyleBookを削除します。

### config packのエクスポートまたはインポート

StyleBookと同様に、config packをエクスポートまたはインポートできます。この機能を使用すると、StyleBook構成を別のNetScaler Consoleに簡単に共有できます。config packをエクスポートすると、`tgz`または`zip`バンドルがローカルコンピューターにダウンロードされます。このバンドルには、config packで定義されているすべてのパラメータを含むJSONファイルが含まれています。

#### 構成のエクスポート

config packをエクスポートするには、次の手順を実行します。

1. **Applications > StyleBooks > Configurations**に移動します。
2. エクスポートするconfig packを選択します。
3. **アクションの選択**で、**構成のエクスポート**を選択します。

   構成のエクスポートオプション(/en-us/netscaler-application-delivery-management-software/media/export-configuration-pack.png)
4. 「**構成のエクスポート**」ペインで、以下を指定します。

   - **構成が展開されているターゲットインスタンスの情報**: このオプションを選択すると、エクスポートバンドルにターゲットインスタンスの情報が含まれます。
   - **構成に関連付けられたStyleBook**: このオプションを選択すると、StyleBookがエクスポートバンドルに含まれます。
   - **エクスポート構成データを保護するためのパスフレーズ**: エクスポートバンドルを暗号化するためのパスフレーズを指定します。このパスフレーズは、構成パックの機密データを保護します。
   - **圧縮ファイルの種類**: **ZIP**または**TGZ**ファイルの種類を選択します。

   ☐
5. **エクスポート**をクリックします。

   エクスポートバンドルをローカルコンピューターに保存します。

#### 構成のインポート

ローカルコンピューターから別のNetScaler Consoleに構成パックをインポートできます。構成パックをインポートするには、次の手順を実行します。

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

1. **Applications > StyleBooks > Configurations**に移動します。
2. **構成のインポート**を選択します。
3. コンピューターからインポートファイルバンドルを選択します。
4. エクスポート時に指定したパスフレーズを使用します。
5. オプションで、で、**すべての構成オブジェクトがNetScalerに既に存在する場合にのみ、新しい構成の作成を許可する**を選択します。

   このオプションは、NetScalerインスタンスに既に作成されているオブジェクトを変更しません。

   同じNetScalerインスタンスを2つのNetScaler Consoleサーバーに追加したとします。そして、あるNetScaler Consoleサーバーから別のサーバーに設定パックを移行したいとします。このオプションを使用して、NetScalerインスタンス上の設定オブジェクトを変更せずに設定パックをインポートします。

   **重要**

   このオプションを使用するには、指定された設定バンドルにターゲットインスタンス情報が含まれていることを確認してください。詳細については、「設定のエクスポート」を参照してください。

   このオプションは、すべてのオブジェクトがターゲットインスタンスに存在する場合にのみ設定を移行します。
6. **インポート**をクリックします。

設定パックをインポートすると、NetScaler Consoleは次のことを検証します。

- **関連付けられたStyleBook**: 関連付けられたStyleBookがNetScaler Consoleにない場合、設定パックとともにStyleBookをインポートします。
- **ターゲットインスタンス**: ターゲットインスタンスを確認し、指定されたターゲットインスタンスに設定を展開します。記載されているNetScalerインスタンスがNetScaler Consoleに存在しない場合、設定パックはターゲットインスタンスなしでインポートされます。
- **ソースNetScaler Console**: 同じNetScaler Consoleサーバーに設定パックをインポートする場合、選択したバンドルは既存の設定パックを更新します。

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

### 設定パックを下書きとして保存する

設定パックの**下書きとして保存**オプションを使用すると、設定の変更を下書きとして保存できます。この機能は、NetScalerインスタンスにすぐに展開することなく変更を保存します。

設定パックを下書きとして保存するには：

1. **アプリケーション > 設定 > 設定パック**に移動します。
2. 「**Configurations**」ページで、「**Add**」をクリックします。
3. 目的のスタイルブックを選択し、「**Select**」をクリックします。
4. 「**Create Configuration**」ページで、「**Save as Draft**」をクリックします。

下書きとして保存(/en-us/netscaler-application-delivery-management-software/media/save-as-draft.png)

コンフィグパックが下書きとして保存されると、構成の変更はNetScalerインスタンスに直接展開されません。代わりに、コンフィグパックは「**Pending Configurations**」の下にある「**Draft Configurations**」タブに下書きとして保存されます。

「**Draft Configurations**」タブで、以下の操作を実行するコンフィグパックを選択します。

- コンフィグパックの構成を編集します。
- 構成をNetScalerインスタンスに展開します。
- 展開せずに構成を削除するには、下書きを削除します。

下書き構成(/en-us/netscaler-application-delivery-management-software/media/draft-config.png)

保存した下書きを展開するタイミングをスケジュールすることもできます。

詳細については、「コンフィグパックのスケジュール」を参照してください。

### コンフィグパックのスケジュールを作成する

コンフィグパックを作成すると、デフォルトでNetScalerインスタンスに自動的に展開されます。この機能を使用すると、コンフィグパックを展開するタイミングをスケジュールできます。

コンフィグパックのスケジュールを作成するには：

1. **Applications > Configuration > Config Packs** の順に移動します。
2. 「**Configurations**」ページで、「**Add**」をクリックします。
3. StyleBookを選択し、「**Select**」をクリックします。

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

4. 「**Create Configuration**」ページで、「**Execution**」の下にある「**Execution Mode**」リストから「**Later**」を選択します。
5. スケジュールする希望の時間と日付を選択し、「**Submit**」をクリックします。

実行モード(/en-us/netscaler-application-delivery-management-software/media/execution-mode.png)

スケジュールされたすべての構成は、「**Pending Configurations**」の下にある「**Scheduled configurations**」タブに保存されます。作成されたスケジュールを選択して、編集、展開、またはキャンセルできます。

スケジュールされた構成(/en-us/netscaler-application-delivery-management-software/media/scheduled-config.png)

#### 展開された構成パックの場合

展開された構成パックを編集および削除するためのスケジュールを作成することもできます。

##### 構成パックの編集操作をスケジュールする

展開された構成パックを編集するためのスケジュールを作成するには：

1. **Applications > Configuration > Config Packs** の順に移動します。
2. 「**Configurations**」ページで、StyleBookを選択し、「**Edit**」をクリックします。
3. 「**Edit Configuration**」ページで、構成パックを編集します。
4. 「**実行モード**」リストで、「**後で**」を選択します。
5. スケジュールする希望の時間と日付を選択し、「**送信**」をクリックします。

##### 設定パックの削除操作をスケジュールする

展開された設定パックを削除するスケジュールを作成するには：

1. **アプリケーション > 設定 > 設定パック** に移動します。
2. 「**Configurations Page**」で、StyleBook を選択し、「**Delete**」をクリックします。
3. 「**実行モード**」リストで、「**後で**」を選択します。
4. スケジュールする希望の時間と日付を選択し、「**送信**」をクリックします。

### 設定パックからターゲットインスタンスをデタッチする

設定パックからターゲットインスタンスをデタッチするには、次の手順を実行します。

1. **アプリケーション > 設定 > 設定パック** に移動します。
2. 削除したいターゲットインスタンスを含む設定パックを選択します。

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

3. 「**Select Action**」で、「**Detach Targets**」を選択します。
4. 「**Detach Targets**」ペインで、設定パックから削除したいターゲットインスタンスを選択します。



5. 「**OK**」をクリックします。

ターゲットインスタンスが削除された状態で、重複するconfig packが作成されたことを確認するメッセージが表示されます。

### StyleBookを作成する

「**example-lb**」StyleBookの全コンテンツは、ご参考までに以下に示します。

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:
```

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

```
  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

「**example-lb-mon**」StyleBookの全コンテンツは、ご参考までに以下に示します。

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks
```

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

```
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
configuration objects
```

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

```
    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
```

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

```
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

## NetScaler Consoleにファイルをアップロードするための StyleBookを作成する

NetScaler Application Delivery Management (NetScaler Console) の StyleBooks を使用すると、NetScaler Console GUI または API を使用して、ローカルファイルシステムから NetScaler インスタンスにあらゆる種類のファイルをアップロードする機能などを含む NetScaler 構成を作成できます。これらのファイルは、例えば証明書ファイルや地理位置情報ファイルなどです。これらのファイルをアップロードするディレクトリを指定することもできます。

### StyleBook構成

以下は、NetScaler インスタンスに地理位置情報ファイルをアップロードする方法を説明する StyleBook の例です。地理ファイルは通常、地理位置情報に基づいた静的近接性を定義するために GSLB 構成で使用されます。

### StyleBookを構築する - 1

```
name: upload-geolocations

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

-

 namespace: netscaler.nitro.config
```

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

```
 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
Console

 type: file

 required: true



components:

-

 name: upload-file-comp

 type: ns::systemfile

 properties:

    filename: $parameters.locationfile.filename

    filelocation: "/var/netscaler/inbuilt_db/"

    filecontent: base64.encode($parameters.locationfile.contents)
```

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

**注**

この例で使用されているパラメーターは、ファイル型です。この StyleBook を NetScaler Console にインポートして、地理位置情報ファイルをアップロードするために使用できます。

このStyleBookでは、ファイルがNetScaler Consoleにすでに存在している必要があります（たとえば、scpのようなユーティリティを使用してNetScaler Consoleにすでにコピーしている場合など）。 NetScaler Consoleファイルシステムに最初にコピーせずに、NetScaler Consoleを介してNetScalerにファイルをアップロードしたい場合は、2つの「string」パラメーターを持つStyleBookを作成できます。1つはNetScalerで使用するファイル名を指定するためのもので、もう1つはファイルの内容を指定するためのものです。これらの2つのパラメーターをupload-file-compコンポーネントで使用します。以下は、geo-locationファイルをアップロードするための代替StyleBookです。

### StyleBookを構築する - 2

```
name: upload-geolocations-alt

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "11.1"

  prefix: ns
```

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

```
parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the NetScaler
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true


components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/NetScaler/inbuilt_db/"
```

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

```
filecontent: base64.encode($parameters.filecontents)
```

### ファイルをアップロードするための構成を作成する

以下の手順では、上記で説明した最初のStyleBookを使用して、選択したNetScaler instanceにgeolocationファイルをアップロードする構成を作成します。

**ファイルをアップロードするための構成を作成するには**:

1. In NetScaler Console, navigate to **Applications** > **Configuration**, and click **Create New**. The Choose StyleBook page displays all the StyleBooks that are available in your NetScaler Console. Scroll down and select the StyleBook that you imported.

   StyleBook パラメーターは、この StyleBook で定義されているすべてのパラメーターの値を入力できるユーザーインターフェイスページとして表示されます。
2. 基本ロードバランサー設定セクションで、ロードバランサーの名前と仮想 IP アドレスを入力します。
3. **Location File**セクションで、ファイルの名前または場所を入力します。

   **注**

   NetScaler Consoleで、ファイルが現在のテナントのフォルダーの下にのみ配置されていることを確認してください。任意のファイル転送プロトコルを使用して、ファイルをNetScaler Consoleファイルシステムにコピーします。
4. ターゲットインスタンスにアクセスする前に、ユーザー資格情報の提供を求められる場合があります。
5. 構成を作成する必要があるターゲットのNetScalerインスタンスを選択し、**作成**をクリックします。

**注**

インスタンスで実際の構成を実行する前に、ターゲットインスタンスで作成される構成オブジェクトを確認するために、**ドライラン**を選択することをお勧めします。

構成パックの作成が成功すると、ファイルはNetScalerインスタンスのファイルシステム上の次の場所に保存されます: /var/netscaler/inbuilt_db/

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

**注**

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスをこのウィンドウで使用可能なインスタンスのリストに追加することもできます。

### NetScaler Console APIを使用して構成パックを作成する

NetScaler Console APIを使用して、選択したNetScalerインスタンスにファイルをアップロードする構成パックを作成することもできます。APIの使用方法の詳細については、任意のファイルタイプをアップロードするための構成を作成するAPIの使用方法を参照してください。

## NetScaler ConsoleにSSL証明書と証明書キーファイルをアップロードするためのStyleBookを作成する

SSLプロトコルを使用するStyleBook構成を作成する場合、StyleBookパラメータで要求されるとおりにSSL証明書ファイルと証明書キーファイルをアップロードする必要があります。StyleBookを使用すると、NetScaler Console GUIを使用してローカルシステムからSSLファイルとキーファイルを直接アップロードできます。NetScaler Console APIを使用して、NetScaler Consoleによってすでに管理されている証明書ファイルとキーファイルをアップロードすることもできます。

### StyleBook構成

このドキュメントは、独自のStyleBook - **負荷分散仮想サーバー (SSL)** の作成を支援します。 SSL証明書とキーファイルをアップロードするためのコンポーネントを備えています。ここに例として提供されているStyleBookは、選択されたNetScalerインスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この構成はSSLプロトコルを使用します。このStyleBookを使用して構成を作成するには、仮想サーバーの名前とIPアドレスを指定し、負荷分散メソッドパラメータを選択し、仮想サーバーの証明書ファイルと証明書キーファイルをアップロードするか、NetScaler Consoleにすでに存在する証明書ファイルと証明書キーファイルを使用する必要があります。これらは、以下に示すように「parameters」セクションで指定されます。

```
parameters:

 -

  name: name

  type: string

  required: true
```

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

```
 -

  name: ip

  type: ipaddress

  required: true

 -

  name: lb-alg

  type: string

  allowed-values:

    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"
```

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

```
  type: keyfile
```

次に、以下に示すように、StyleBookのコンポーネントセクションに2つのコンポーネントが作成されます。「my-lbvserver-comp」コンポーネントはタイプ ns::lbvserver で、ここで：

- 「ns」は、import-stylebooksセクションで指定した組み込みの名前空間 netscaler.nitro.config およびバージョン 10.5 を参照するプレフィックスです。
- 「lbvserver」はこの名前空間の組み込みStyleBookです。これは、同名のNetScaler NITRO負荷分散仮想サーバーリソースに対応します。

2番目のコンポーネント「lbvserver-certificate-comp」はタイプ stlb::vserver-certs-binds です。プレフィックス「stlb」は、StyleBookのimport-stylebooksセクションで指定されている名前空間「com.citrix.adc.stylebooks」およびバージョン 1.0 を参照します。「com.citrix.adc.stylebooks」名前空間をフォルダと考えるなら、「vserver-certs-binds」はそのフォルダ内の別のStyleBook（またはファイル）です。「com.citrix.adc.stylebooks」名前空間にあるStyleBookは、NetScaler Consoleの一部として出荷されます。

ユーザー定義のStyleBookで使用される「vserver-certs-binds」StyleBookを使用すると、証明書とキーファイルをターゲットのNetScalerインスタンスにアップロードし、証明書とキーファイルの適切な仮想サーバーへのバインディングを構成することで、証明書を簡単に構成できます。このコンポーネントのプロパティは、lb仮想サーバーの名前と、構成パックの作成時に提供するSSL証明書の名前です。

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: SSL

   ipv46: $parameters.ip

   port: 443
```

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

```
    lbmethod: $parameters.lb-alg

  -

   name: lbvserver-certificate-comp

   type: stlb::vserver-certs-binds

   description: Binds lbvserver with server certificate

   properties:

    vserver-name: $components.my-lbvserver-comp.properties.name

    certificates:

     -

      cert-name: $parameters.name + "-lb-cert"

      cert-file: $parameters.certificate

      ssl-inform: PEM

      key-name: $parameters.name + "-key"

      key-file: $parameters.key
```

このようなStyleBookからAPIを使用して構成を作成する場合、ファイル名のみを使用します（完全なファイルパスは使用しません）。これらのファイルは、NetScaler Consoleの証明書およびキーファイルフォルダにすでに存在している必要があります。アップロードされたSSL証明書ファイルはNetScaler Consoleの /var/mps/tenants/.../ns_ssl_certs ディレクトリに保存され、SSL証明書キーファイルはNetScaler Consoleの /var/mps/tenants/.../ns_ssl_keys ディレクトリに保存されます。

### SSLファイルをアップロードするための構成の作成

以下の手順では、上記のStyleBookからSSLプロトコルを使用して、選択したNetScalerインスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この手順を使用して、NetScaler ConsoleにSSL証明書ファイルと証明書キーファイルをアップロードできます。

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

**ファイルをアップロードするための構成を作成するには**

1. NetScaler Consoleで、**Applications** > **Configuration > StyleBooks** に移動します。**StyleBooks** ページには、NetScaler Consoleで利用可能なすべてのStyleBookが表示されます。
2. 下にスクロールして **Load Balancing Virtual Server (SSL)** を選択するか、検索フィールドに **Load Balancing Virtual Server (SSL)** と入力して **Enter** キーを押します。
3. StyleBookパネルで**構成の作成**リンクをクリックします。

   StyleBookのパラメータは、このStyleBookで定義されているすべてのパラメータの値を入力できるユーザーインターフェイスページとして表示されます。
4. 基本ロードバランサー設定セクションで、ロードバランサーの名前と仮想IPアドレスを入力します。
5. **SSL証明書設定**セクションで、ローカルストレージフォルダーから該当するファイルを選択します。または、NetScaler Console自体に存在するファイルを選択することもできます。
6. 構成を作成するターゲットのNetScalerインスタンスを選択し、**作成**をクリックします。

**注:**

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを、このウィンドウで使用可能なインスタンスのリストに追加することもできます。

NetScaler Consoleでは、NetScaler Consoleの一部として提供される以下のデフォルトのStyleBookを使用すると、SSL証明書とキーをアップロードしてSSLサポートを作成できます。

- HTTP/SSLロードバランシングStyleBook (lb)
- HTTP/SSLロードバランシング (モニター付き) StyleBook (lb-mon)
- HTTP/SSLコンテンツスイッチングアプリケーション (モニター付き) (cs-lb-mon)
- CS、LB、SSL機能を使用するサンプルアプリケーションStyleBook (sample-cs-app)

上記のStyleBookで説明されているのと同じ方法で、SSL証明書を利用する独自のStyleBookを作成することもできます。

### StyleBookを作成する

ファイルlb-vserver-ssl.yamlの全内容は以下のとおりです。

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

```
name: lb-vserver-ssl

description: "This stylebook defines a load balancing virtual server
configuration."

display-name: "Load Balancing Virtual Server (SSL)"

namespace: com.example.ssl.stylebooks

schema-version: "1.0"

version: "0.1"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"

 -

  namespace: com.citrix.adc.stylebooks

  prefix: stlb

  version: "1.0"



parameters:

 -

  name: name

  type: string
```

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

```
  required: true

 -

  name: ip

  type: ipaddress

  required: true

 -

  name: lb-alg

  type: string

  allowed-values:

    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"
```

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

```
  type: keyfile


components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 443
    lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $ components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
```

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

```
    ssl-inform: PEM

    key-name: $parameters.name + "-key"

    key-file: $parameters.key
```

#### NetScaler Console API を使用した構成パックの作成

選択したNetScalerインスタンスに証明書ファイルとキーファイルをアップロードする構成パックを作成するには、NetScaler Console API を使用することもできます。API の使用方法の詳細については、「API を使用して証明書ファイルとキーファイルをアップロードする構成を作成する方法」を参照してください。(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/how-to-use-api.html)

#### NetScalerインスタンスで定義されたオブジェクトの表示

NetScaler Console でStyleBook構成パックが作成された後、「**作成されたオブジェクトの表示**」をクリックして、ターゲットのNetScalerインスタンスで作成されたすべてのNetScalerオブジェクトを表示します。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/stylebook-obejcts-created.jpg)

## StyleBookを使用して証明書ストアからSSL証明書を管理する

NetScaler Consoleの証明書ストアを使用すると、SSL証明書を1か所に保存して管理できます。そのため、SSL証明書をNetScaler Consoleに保存し、NetScalerの設定中に再利用できます。

この記事では、NetScaler Consoleの証明書ストアからSSL証明書をアップロードして再利用できるStyleBook定義を作成する方法について説明します。

### パラメータ

**StyleBook**定義は、新しい組み込みパラメータタイプとして`certkey`をサポートしています。このパラメータタイプを使用して、NetScaler Consoleの証明書ストアからSSL証明書を再利用できます。

```
parameters:

-

    name: certificate
```

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

```
    label: Certificate

    description: "Certificate to be bound to this virtual load balanced
application"

    type: certkey

    required: true
```

この例では、証明書パラメータはNetScaler Consoleの証明書ストアにあるSSL証明書または証明書チェーンを指します。

**StyleBook**定義では、`certkey`パラメータについて次のプロパティを参照できます。

- `certkeyname` – インスタンスに構成するSSL証明書キーの名前。
- `cert_filename` – SSL証明書のファイル名。
- `password` – 必要に応じてSSL証明書にアクセスするために必要なパスワード。
- `key_filename` – SSL証明書キーのファイル名。
- `keyfile_contents` – SSL証明書の内容。
- `subject` – SSL証明書に記載されているサブジェクト。
- `issuer` – SSL証明書を発行した機関。
- `certchain_certkeyname` – 証明書チェーンの名前。

> **注:**
>
> サーバー証明書は、複数の階層型認証局 (CA) によって署名されることがあり、その場合、証明書はチェーンを形成します。証明書ストアに証明書チェーンがある場合は、このプロパティを使用します。これにより、証明書を参照して相互にバインドできます。構成パックを作成すると、証明書チェーンはリストとして表示されます。

これらのプロパティは、**StyleBook** 定義で必要なコンポーネントを作成するのに役立ちます。

### コンポーネント

StyleBook に `type: certkey` パラメータがある場合、NetScaler Console 証明書ストアからこのパラメータの証明書を提供できます。このワークフローでは、NetScaler Console 証明書ストアから証明書を表示および選択するだけでなく、次のことも実行できます。

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

- 新しい証明書をアップロードします。
- 既存の証明書を更新します。たとえば、期限切れの証明書などです。
- 証明書を削除します。

**注:**

- NetScaler Console SSLダッシュボードを使用して、NetScaler Console 証明書ストアの証明書を管理することもできます。
- NetScaler Console 証明書ストアで SSL 証明書を更新した後、その SSL 証明書に関連付けられている構成パックを更新する必要があります。構成パックの更新の詳細については、「API を使用して既存の構成パックを更新する」または「構成パックを作成および編集する」を参照してください。

### StyleBook を構築する

次の StyleBook 定義は、NetScaler Console 証明書ストアの SSL 証明書を使用します。この StyleBook には、メイン証明書ファイルとキーファイルを NetScaler インスタンスにアップロードするコンポーネントが含まれています。これらのファイルがすでに NetScaler インスタンスに存在する場合、NetScaler Console はアップロード手順をスキップし、これらのコンポーネントは影響を与えません。

```
name: lb-with-cert-from-certstore

namespace: com.example.stylebooks

version: "1.0"

display-name: Application using a CertStore certificate

description: This StyleBook defines a simple SSL Vserver.

schema-version: "1.0"



import-stylebooks:

 -
```

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

```
    namespace: netscaler.nitro.config

    version: "13.0"

    prefix: ns



parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true

 -

  name: certificate

  label: Application Certificate

  description: Certificate chain and key to be bound to this application

  type: certkey
```

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

```
  required: true




components:

 -

    name: pem-cert-files-comp

    type: ns::systemfile

    description: This component uploads the PEM certificate file onto the
NetScaler

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.cert_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.certfile_contents)

      fileencoding: BASE64

 -

    name: pem-KEY-files-comp

    type: ns::systemfile

    description: This component uploads the PEM key file onto the
NetScaler.

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.key_filename
```

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

```
      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.keyfile_contents)

      fileencoding: BASE64

 -

    name: cert-files-comp

    type: ns::sslcertkey

    description: This component creates the certkey on the NetScaler using
the uploaded files.

    condition: $parameters.certificate

    properties:

      certkey:  $parameters.certificate.certkeyname

      cert: $parameters.certificate.cert_filename

      key: $parameters.certificate.key_filename

 -

  name: lbvserver-comp

  type: ns::lbvserver

  description: This component creates the lbvserver of the application.

  properties:

   name: $parameters.name + "-lbvserver"

   servicetype: SSL

   ipv46: $parameters.ip

   port: 443
```

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

```
 lbmethod: ROUNDROBIN

components:

    -

      name: sslvserver-comp

      type: ns::sslvserver

      description: This component configures SSL settings on the vserver

      properties:

        vservername: $parent.properties.name

        ssl3?: ENABLED

        tls1?: ENABLED

        tls11?: ENABLED

    -

     name: cert-bindings-adv-comp

     type: ns::sslvserver_sslcertkey_binding

     description: This component binds the certkey to the vserver

     condition: $parameters.certificate

     properties:

       vservername: $parent.properties.name

       certkeyname: $parameters.certificate.certkeyname
```

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

## StyleBookで定義された仮想サーバーでアナリティクスを有効にし、アラームを設定する

オペレーション構成を使用して、NetScaler Consoleアナリティクスを設定し、StyleBookの一部である仮想サーバーコンポーネントによって処理されるすべてのトラフィックトランザクションまたは一部のトラフィックトランザクションでAppFlowレコードを収集できます。この構成を使用してアラームを設定し、仮想サーバーによって管理されるトラフィックに関する洞察を得ることもできます。

次の例は、StyleBookのオペレーションセクションを示しています。

```
operations:

  analytics:

   -

    name: lbvserver-ops

    properties:

    target: $components.basic-lb-comp.outputs.lbvserver

    filter: HTTP.REQ.URL.CONTAINS("catalog")

   -

    alarms:

     -

      name: lbvserver-alarm

      properties:

      target: $outputs.lbvserver

      email-profile: $parameters.emailprofile

      sms-profile: "NetScalerSMS"
```

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

```
    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
```

アナリティクスセクションの属性は、NetScaler Consoleアナリティクス機能に、ターゲットプロパティによって識別される仮想サーバーコンポーネントでAppFlowレコードを収集するように指示するために使用されます。オプションで、仮想サーバーでAppFlowレコードが収集されるリクエストをフィルタリングするためのNetScalerポリシー式を受け入れるフィルタプロパティを指定することもできます。

このStyleBookから構成パックが作成されると、NetScaler Consoleアナリティクス機能は、構成パックの作成プロセスで作成されたときに指定された仮想サーバーでAppFlowレコードを収集するように構成されます。

アラームセクションの属性は、ターゲットプロパティによって識別される仮想サーバーでアラームを生成し、通知を送信するためのしきい値を設定するために使用されます。上記の例では、email-profileおよびsms-profileプロパティは、通知の送信先を指定するために使用されます。rulesセクションはしきい値を定義します。たとえば、仮想サーバーによって処理される合計リクエストが25を超え、ユーザーによって定義された期間にわたる場合、アラームが設定され、通知が送信されます。「period-unit」は、アラームがトリガーされる頻度を指定します。これは、日、時間、または週の値を取ることができます。

メトリック値をしきい値と比較する場合、次の演算子を使用できます。

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

- ">" の場合は "greaterthan"
- "<" の場合は "lessthan"
- ">=" の場合は "greaterthanequal"
- "<=" の場合は "lessthanequal"

StyleBookは、NetScaler ConsoleアナリティクスGUIに表示される名前ではなく、メトリックのAPI名を使用することに注意してください。

構成パックの一部として作成された仮想サーバーで収集されたデータを表示および分析する方法については、NetScaler Consoleアナリティクスドキュメントを参照してください。

## インスタンスロール

NetScaler Consoleでは、単一のアプリケーションに対して複数のNetScalerインスタンスを設定する必要があるシナリオや、各NetScalerインスタンスに異なる構成を展開する必要があるシナリオが発生する可能性があります。このようなケースの例として、デフォルトのMicrosoft Skype for Business StyleBookがあります。

StyleBooksは現在、構成パックを作成し、複数のNetScalerインスタンスに同じ構成を適用する機能をサポートしています。すべてのNetScalerインスタンスで構成が同一であるこのようなシナリオは、対称構成と呼ばれます。

StyleBooksの「インスタンスロール」機能を使用すると、非対称構成、つまり複数のNetScalerインスタンスに適用できるが、異なるNetScalerインスタンスには異なる構成が適用される構成パックを作成できます。

インスタンスロール機能を持つStyleBookを使用して構成パックを作成する場合、構成パック内の各NetScalerインスタンスには異なるロールを割り当てることができます。このロールは、NetScalerインスタンスが受け取る構成パックの構成オブジェクトを決定します。

**注意点:**

- StyleBook内のインスタンスロールのセットは、StyleBookの作成時に定義されます。
- ロールは、構成パックの作成または更新時に特定のNetScalerインスタンスに割り当てられます。

### ターゲットロールセクション

StyleBookに「target-roles」という新しいセクションが導入され、StyleBookでサポートされるすべてのロールが宣言されます。

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

このセクションは通常、StyleBookの「import-StyleBooks」セクションの後、およびパラメータセクションの前に配置されます。

次のStyleBookの例では、「target-roles」セクション内に2つのロール（AとB）が定義されています。

```
target-roles:



  -

   name: A

   name: B

     min-targets: 2

     max-targets: 5
```

ロールBには、オプションのサブプロパティであるmin-targetsとmax-targetsも定義されていることがわかります。

これら2つのサブプロパティはオプションですが、min-targetsは、このStyleBookから構成パックを作成する際にこのロールを割り当てる必要があるNetScalerインスタンスの最小必須数を指定し、max-targetsは、このStyleBookから構成パックを作成する際にこのロールを割り当てることができるNetScalerインスタンスの最大数を指定します。

これらのサブプロパティが指定されていない場合、そのロールに対して構成できるNetScalerインスタンスの数に制限はありません。min-targets = 0の場合、そのロールに関連付けられた構成はオプションであり、min-targets = 1の場合、その構成は必須であり、少なくとも1つのNetScalerインスタンスがそのロールに対して構成される必要があります。

### 「default」ロール

明示的に定義されたロールに加えて、すべてのStyleBookが持つ暗黙的なロールがあり、そのロールはデフォルトロールと呼ばれます。このロールは、StyleBook内の他のロールと同様に使用できます。設定パックを作成する際、NetScalerインスタンスに特定のロールが割り当てられていない場合、そのインスタンスは暗黙的に「default」ロールに割り当てられます。これにより、インスタンスは「default」ロールを持つコンポーネントによって生成された設定オブジェクトを受け取ります。

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

### ロールを持つコンポーネント

StyleBookがサポートできるロール（「default」ロールを含む）が定義された後、そのロールはStyleBookのコンポーネントセクションで使用できます。特定のロールを果たすNetScalerインスタンスにのみコンポーネントをデプロイしたい場合は、コンポーネントの一部としてroles属性を指定できます。コンポーネントの以下の例に示すとおりです。

```
-

  name: C1

  type: ns::lbvserver

  roles:

    - A

  properties:

    name: lb1

    servicetype: HTTP

    ipv46: 1.1.1.1

    port: 80
```

上記の例では、コンポーネントはロールAを果たすインスタンスにデプロイされる「lbvserver」を生成します。コンポーネントのroles属性はリストであり、コンポーネントには複数のロールを割り当てることができることに注意してください。これらのロールは、StyleBookの「target-roles」セクションで宣言されているはずです。

注: StyleBook内のコンポーネントがロール属性を指定しない場合、そのコンポーネントによって生成された設定オブジェクトは、そのロールに関係なくすべてのNetScalerインスタンスに作成されます。この機能を利用して、設定パックのすべてのインスタンスに適用できる設定オブジェクトを効果的に作成できます。

ロールAとBが定義され、4つのコンポーネントを含むStyleBookがあると仮定しましょう。

- コンポーネントC1はロールAとBを持ちます
- コンポーネントC2はロールBを持ちます

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

- コンポーネントC3にはロールが定義されていません
- コンポーネントC4は「default」ロールを持ちます

このStyleBookのコンポーネントセクションを以下に示します。

```
components:

  -

    name: C1

    type: ns::lbvserver

    roles:

      - A

      - B

    properties:

      name: lb1

      servicetype: HTTP

      ipv46: 1.1.1.1

      port: 80

  -

    name: C2

    type: ns::lbvserver

    roles:

      - B

    properties:

      name: lb2
```

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

```
    servicetype: HTTP
    ipv46: 12.12.12.12
    port: 80
-
  name: C3
  type: ns::lbvserver
  properties:
    name: lb3
    servicetype: HTTP
    ipv46: 13.13.13.13
    port: 80
-
  name: C4
  type: ns::lbvserver
  roles:
    - default
  properties:
    name: lb4
    servicetype: HTTP
    ipv46: 14.14.14.14
    port: 80
```

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

コンポーネントC3にはロールが定義されていないことに注意してください。これは、そのロールに関係なく、コンポーネントがすべてのインスタンスにデプロイされることを意味します。一方、コンポーネントC4は「default」ロールを持ちます。これは、明示的なロールが割り当てられていない任意のインスタンスに適用されることを意味します。

さて、このStyleBookを使用して設定パックを作成し、5つのNetScalerインスタンスにデプロイしたいとします。この段階で、インスタンスにロールを次のように割り当てることができます。

- ロールAはインスタンスT1、T2、T3、T4に割り当てられます
- ロールBはインスタンスT2、T3、T4に割り当てられています。
- インスタンスT5にはどのロールも割り当てられていません。

次の図は、ロールの割り当てを要約し、各NetScalerインスタンスが受け取る結果の構成を示しています。

コンポーネントC3にはロール属性がなかったため、ロールに関係なくすべてのインスタンスにデプロイされることに注意してください。

コンフィグパックを作成する際に「ドライラン」機能を使用すると、ロールの正しい割り当てと、各NetScalerインスタンスで作成される構成オブジェクトを表示および検証できます。

### StyleBookを構築する

StyleBook「demo-target-roles」の全内容は以下のとおりです。

```
---

name: demo-target-roles

namespace: com.example.stylebooks

version: "1.2"

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns
```

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

```
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
```

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

```
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
```

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

```
  -

    name: C4

    type: ns::lbvserver

    roles:

      - default

    properties:

      name: lb4

      servicetype: HTTP

      ipv46: 14.14.14.14

      port: 80
```

次の図は、サンプルコンフィグパック用に作成されたオブジェクトを示しています。



### APIの使用

REST APIを使用する場合、コンフィグパックの作成または更新時に、各NetScalerインスタンスのロールを次のように指定できます。「targets」ブロックで、個々のコンポーネントをデプロイする特定のNetScalerインスタンスのUUIDを指定します。

```
"targets": [

            {

             "id": "<ADC-UUID>",

             "roles": ["A"]

            },

           ]
```

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

完全なサンプルREST APIは、参考のために提供されています。

POST /`<Console-IP>`/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]

        },

        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",

          "roles": ["A", "B"]

        },

        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",

          "roles": ["A", "B"]

        },

        {
```

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

```
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```

## 非CRUD操作を実行するStyleBookを作成する

StyleBookは、NetScalerインスタンス上で必要な構成オブジェクトを計算することで、NetScalerの構成を管理します。これらのオブジェクトは、ConfigPackを作成または更新するたびにインスタンスに追加、更新、または削除されます。これが「目的の状態」を指定するタイミングです。

ただし、一部のNetScaler構成オブジェクトは、作成、更新、または削除（CRUD操作）以外のいくつかの操作をサポートしています。たとえば、ロードバランサーオブジェクト（lbvserver）またはNetScaler機能オブジェクト（nsfeature）は、「有効化」または「無効化」操作をサポートできます。同様に、NetScalerの証明書キーは、証明書を別の証明書にリンクまたはリンク解除するための「リンク」および「リンク解除」操作をサポートします。NetScalerオブジェクトに対するこれらの操作は、非CRUD操作と呼ばれます。このセクションでは、StyleBookを使用して、それらをサポートする構成オブジェクトに対して非CRUD操作を実行する方法について説明します。

**注**

構成オブジェクト間のバインディング（たとえば、証明書キーをlbvserverにバインドする）は、非CRUD操作とは見なされません。これは、Nitroバインディングがそれ自体で構成オブジェクトとして表現されるためです。これらのオブジェクトは、他のNetScaler構成オブジェクトと同様に作成および削除されます。

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

### 非CRUD操作のサポート

「meta-properties」と呼ばれる新しいコンストラクトが、「properties」コンストラクトと同じレベルのコンポーネントに追加されました。このコンストラクトで現在サポートされている唯一の属性は「action」と呼ばれます。この属性は、その構成オブジェクトでサポートされている「enable」や「disable」などの値を取ることができます。

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  meta-properties

   action: enable

  properties:

    name: $parameters.name

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg
```

上記の例では、「my-lbvserver-comp」コンポーネントは「ns::lbvserver」タイプです。「ns」は、import-stylebooksセクションで指定した名前空間netscaler.nitro.configおよびバージョン10.5を参照するプレフィックスです。「lbvserver」はこの名前空間のNITROリソースです。暗黙的なアクションとして、lbvserverはまずStyleBookによって作成され、その後「enable」操作が実行されます。

meta-propertiesで指定されたアクションは、ConfigPackの作成時にのみ構成オブジェクトに対して実行されます。ConfigPackの更新では、非CRUDアクションは実行されません。

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

**注**

action属性の値は、動的に評価されるStyleBook式にすることはできません。

## StyleBookのconfig packを別のStyleBookに移行する

NetScaler Consoleでは、config packは常に作成元のStyleBookにバインドされます。config packへの更新は、そのconfig packがバインドされているStyleBookを介してのみ実行できます。NetScaler Consoleでは、既存のconfig packを新しいStyleBookに移行できるようになりました。新しいStyleBookは、config packにバインドされている現在のStyleBookのより元のバージョンである可能性があります。または、config packをまったく別のStyleBookに移行することもできます。

たとえば、**example-lb**というStyleBookを作成しました。このStyleBookは、NetScalerインスタンスに基本的なロードバランサー構成を展開するために使用されます。このStyleBookからNetScalerインスタンス上にconfig pack CP1を作成しました。その後、StyleBookに監視構成が含まれていないことに気づきました。そこで、**example-lb-mon**というStyleBookを新しく作成しました。このStyleBookは、example-lb StyleBookと同じロードバランサー構成を持っていますが、モニターを構成する機能が追加されています。

config pack CP1で作成された既存の構成を更新して、モニターを追加したいとします。以前は、config pack CP1を削除し、新しいStyleBookからconfig pack CP2を作成して、構成にモニターを追加する必要がありました。CP1を削除すると、1つ以上のNetScalerインスタンス上のconfig pack CP1で作成されたすべての構成が削除されます。以前は、すべてのパラメーターの値を入力して、新しいStyleBookを介して新しいconfig packを再作成する必要がありました。

代わりに、既存のconfig pack CP1を新しいexample-lb-mon StyleBookに移行できるようになりました。新しいStyleBookは、モニターの詳細を構成できます。config packが展開されたNetScalerインスタンスには、モニター関連の構成オブジェクトのみが追加されます。これで、モニターの詳細を提供するだけで済みます。変更されていないNetScalerインスタンスに展開された既存の構成は影響を受けません。

### config packを移行する

#### example-lb StyleBookを使用して作成されたconfig packをexample-lb-mon StyleBookに移行するには

1. NetScaler Consoleで、**Applications** \> **Configurations**に移動します。**Configurations**ページには、システムに存在するすべてのconfig packが表示されます。

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

2. 以前に作成した**example-lb** config packを見つけるまでスクロールし、**Migrate Configpack**をクリックします。
3. **Choose target StyleBook for migration**ページが開き、NetScaler Consoleで利用可能なすべてのStyleBookが一覧表示されます。**example-lb-mon** StyleBookを見つけるまでスクロールし、**Select StyleBook**をクリックします。example-lb-monと入力してStyleBookを検索することもできます。

   あるStyleBookから別のStyleBookに移行する場合、2つのStyleBookのすべてのパラメーターが同じ構造であるとは限りません。パラメーター構造が類似している場合、以前の値はパラメーターフィールドに自動的に保持されます。新しいStyleBookの一部のパラメーターは新規であるか、その構造が変更されている可能性があります。そのような場合は、StyleBookパラメーターの値を手動で入力する必要があります。たとえば、次の図はexample-lb StyleBookのパラメーターを示しています。

   

   次の図は、config packをexample-lb-mon StyleBookに移行した後のパラメーターを示しています。

   

   この場合、StyleBookが基本的なロードバランサー構成の古い値を保持していることがわかります。しかし、モニターパラメーターの値は手動で入力する必要があります。
4. インスタンスでモニターを作成するために使用される新しいパラメーターの値を入力します。
5. **ターゲットインスタンス**で、構成を実行するNetScalerインスタンスのIPアドレスをクリックして選択します。必要な数のターゲットインスタンスを指定することで、複数のNetScalerに構成を展開できることに注意してください。
6. **ドライラン**をクリックします。**オブジェクト**ページには、NetScalerインスタンスから新しく作成、変更、または削除されるオブジェクトが表示されます。
7. **作成**をクリックして、選択したインスタンスの構成を作成または更新します。ターゲットインスタンスが新しい場合、構成パックが作成されます。それ以外の場合は、インスタンスに展開されている既存の構成が更新されます。

**注：**

更新アイコンをクリックして、最近検出されたNetScalerインスタンスを追加することもできます。これにより、これらのインスタンスはこのウィンドウのインスタンスリストにすぐに表示されます。更新アイコンは現在、NetScaler Consoleでのみ利用可能です。

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

構成パックをStyleBookのあるバージョンから次のバージョンに移行することもできます。ここでも、新しいバージョンに存在する新しい必須パラメーターの値を入力する必要がある場合があります。構成パックをStyleBookの古いバージョンに移行することもできます。この場合、古いStyleBookに存在しない余分なパラメーターは削除されます。**オブジェクト**ページには、構成から削除されたオブジェクトが表示されます。

移行が成功すると、ConfigPackは新しいStyleBookにバインドされます。

構成パックの名前と構成パックIDは以前と同じであることがわかります。しかし、NetScaler ConsoleはStyleBook名をexample-lbからexample-lb-monに更新します。

### StyleBookを構築する

**example-lb** StyleBookの全内容は、参考のために以下に示します。

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:
```

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

```
  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

**example-lb-mon** StyleBookの全内容は、参考のために以下に示します。

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks
```

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

```
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
configuration objects
```

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

```
    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
```

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

```
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

# データソースの管理

NetScaler Consoleでデータソースを定義すると、StyleBook構成の作成または更新時に、外部ソースからのデータを入力として使用できます。そうしないと、StyleBookで必要とされる各入力を明示的に指定する必要があります。NetScaler Consoleでは、管理対象のNetScalerインスタンスをStyleBook構成への入力のデータソースとして使用できます。また、構成の作成または更新時に入力として機能するカスタムデータソースを定義することもできます。

**コレクション**: データベースに複数のテーブルがあるように、データソースには複数のコレクションを含めることができます。各コレクションには名前があり、類似したタプルのリストが含まれています。各タプルはキーと値のペアのセットです。たとえば、コレクションは、各タプルが(`<name>: <value>, <virtualip>:<value>`) を持つタプルで構成できます。

**データソースタイプ**: データソースタイプは、データが取得されるソースのタイプを区別します。NetScaler Consoleは2つのデータソースタイプをサポートしています。

- **managed-adc** - これは組み込みのデータソースです。NetScaler Consoleによって管理されている既存のNetScalerからデータを取得するために使用されます。詳細については、「NetScalerインスタンスをデータソースとして使用する」を参照してください。

  ターゲットのNetScalerインスタンスをデータソースとして使用することもできます。詳細については、「ターゲットのNetScalerインスタンスをデータソースとして使用する」を参照してください。
- **カスタムデータソースタイプ** - データがNetScaler® Consoleにローカルに投入されるカスタムデータソースタイプを定義できます。

  データソースタイプ `Environment` を考えてみましょう。このデータソースタイプには、`Production` と `Staging` の2つのデータソースがあります。StyleBook構成を作成する際、StyleBookユーザーはタイプ `Environment` の任意のデータソースを選択できます。選択に応じて、`Production` または `Staging` のいずれかのデータ値がStyleBookへの入力として使用されます。

  詳細については、「カスタムデータソースを使用する」を参照してください。

**コレクションスキーマ**: コレクションタプルに格納できるデータのタイプを記述します。コレクションスキーマは、タプル内の各キーの名前とその予期されるタイプを記述します。データベース

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

の類推では、コレクションスキーマは、各列に明確に定義された名前とサポートするタイプがあるテーブルのデータベーススキーマに似ています。

次の図は、データソースのさまざまなコンポーネントとそれらの相互関係を一般的に表したものです。



## NetScalerインスタンスをデータソースとして使用する

管理対象のNetScalerインスタンスをデータソースとして使用できます。`managed-adc`は、NetScaler Consoleでデータソースとしてすぐに使用できる組み込みのデータソースタイプです。NetScaler Consoleの各管理対象NetScalerインスタンスは、デフォルトでデータソースです。設定パックの作成時に、NetScaler Consoleによって管理されている既存のNetScalerからデータが必要な場合は、StyleBookでこれらのデータソースの使用を開始できます。

StyleBookの定義で、`datum`組み込みタイプパラメータを指定します。StyleBookでデータソースタイプを使用できます。StyleBookユーザーは、そのソースからデータを取得するために使用できるデータソースを選択できます。

### コレクションなしで組み込みデータソースを使用する

```
parameters:

  - name: selected-adc

    label: Select an existing NetScaler

    type: datum

    required: true

    data-source:

      type: managed-adc
```

この例では、`datum`パラメータを使用して、NetScaler Consoleによって管理されている任意のNetScalerインスタンスを選択します。`managed-adc`組み込みデータソースを使用すると、NetScaler Consoleによって管理されている任意のNetScalerインスタンスからデータを取得できます。

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

StyleBookでは、選択したNetScalerインスタンスから任意の構成にアクセスできます。そして、同じNetScalerまたは別のNetScalerインスタンスで構成を作成または更新する際に、その構成を使用できます。これは、選択したターゲットNetScalerインスタンスによって異なります。

**データソースからコレクションにアクセスする**:

選択したNetScalerインスタンスでコレクションにアクセスするには、次の式を使用します。

```
$parameters.selected-adc.collections.<collection-name>
```

例:

```
$parameters.selected-adc.collections.lbvserver
```

この式は、選択したNetScalerインスタンス上の`lbvserver`エンティティのリストを返します。たとえば、このリストを反復処理して、特定の条件を満たす特定の`lbvserver`を選択できます。

**コレクションなしのStyleBookの例**

```
name: add-vservers-from-managed-adc-instances

namespace: com.citrix.adc.stylebooks

version: "1.0"

schema-version: "1.0"



import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:
```

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

```
    -

      name: selected-adc

      label: Select a NetScaler instance

      type: datum

      required: true

      data-source:

        type: "managed-adc"



components:

  -

    name: sslvserver-comp

    type: ns::sslvserver

    repeat: $parameters.selected-adc.collections.lbvserver

    repeat-item: lbvs

    repeat-condition: $lbvs.attributes.servicetype == "SSL"

    properties:

      name: $lbvs.attributes.name

      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED
```

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

```
      tls12: ENABLED
```

構成パックGUIには、NetScaler Consoleによって管理されているNetScalerインスタンスが表示され、StyleBookユーザーは構成パックの作成または更新時に任意のNetScalerを選択できます。

組み込みのNetScalerデータソース（コレクションなし）(/en-us/netscaler-application-delivery-management-software/media/managed-adc-without-collection.png)

このStyleBookは、選択したNetScalerを使用し、すべての`lbvserver`エンティティを反復処理します。SSL仮想サーバーを選択し、各仮想サーバーで許可されるSSLプロトコルバージョンを設定します。

次の式を使用すると、NetScalerインスタンス内の`lbvserver`エンティティのリストを反復処理できます。

```
repeat: $parameters.selected-adc.collections.lbvserver
```

- `collections`: NetScalerインスタンス上のすべてのエンティティタイプを指します。例えば、`csvserver`、`lbmonitor`、`servicegroup`など。
- `lbvserver`: NetScalerインスタンス内のロードバランシング仮想サーバーエンティティのリストを指します。

### コレクションで組み込みデータソースを使用する

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

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

この例では、`datum`パラメーターを使用して、ユーザーがNetScalerインスタンスと特定の`lbvserver`の両方を`managed-adc`データソースタイプから選択できるようにします。

`parameters`セクションでコレクションタイプを定義すると、StyleBookユーザーはNetScalerインスタンスとそのインスタンス上のコレクションから特定のエンティティを選択できます。

**選択したアイテムの属性にアクセスする**:

StyleBookユーザーが仮想サーバーを選択すると、StyleBook内の次の式で、選択したアイテムの任意の属性にアクセスできます。

```
$parameters.selected-lbvserver.attributes.<attribute-name>
```

この例では、選択された`datum`は`lbvserver`です。したがって、`name`、`servicetype`、`ipv46`など、NetScalerエンティティ`lbvserver`の任意の属性にアクセスできます。

例:

```
$parameters.selected-lbvserver.attributes.ipv46
```

この式は、選択したロードバランシング仮想サーバーのIPを取得します。NetScalerエンティティ（コレクション）とその属性の詳細については、NetScaler NITRO APIリファレンスを参照してください。

**コレクションから複数のアイテムを選択する**:

次のパラメーターセクションでは、StyleBookユーザーがコレクションの複数のアイテムを選択できます。

```
parameters:

  - name: selected-lbvservers

    label: Select existing lbvservers

    type: datum[]

    required: true

    data-source:
```

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

```
      type: managed-adc

      collection: lbvserver
```

この例では、datumパラメーターはデータソース配列を定義するために使用されます。ユーザーは、単一のNetScaler®インスタンスから、または複数のNetScalerインスタンスにわたって、1つ以上のlbvserverを選択できます。

以下のコードスニペットは、選択したアイテムとその属性にアクセスする方法を示しています。

```
components:

  - name: sslvserver-comp

    type: ns::sslvserver

    repeat:

      repeat-list: $parameters.selected-lbvservers

      repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.name

      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

**選択したアイテムの参照によるコレクションへのアクセス**:

StyleBookユーザーが管理対象のNetScalerインスタンスで特定のエンティティを選択できるようにするだけでなく、選択したNetScalerインスタンス上の同じまたは異なるコレクションから任意の

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

エンティティにアクセスすることもできます。そのNetScalerインスタンス上の別のコレクションにアクセスするには、`components`セクションで次の式を使用します。

```
$parameters.selected-lbvserver.datasource.collections.<collection-name>
```

例:

```
$parameters.selected-lbvserver.datasource.collections.csvserver
```

この式は、選択したNetScalerインスタンスからコンテンツスイッチング仮想サーバーのリストを返します。

また、次の式は、`lbvservers`と`servicegroups`間のすべてのバインディングのリストを返します。

```
$parameters.selected-
lbvserver.datasource.collections.lbvserver_servicegroup_binding
```

**コレクションを含むStyleBookの例**

以下は、管理対象のNetScalerインスタンスをデータソースとして使用する方法を示すStyleBookの例です。

```
name: bind-lb-to-servicegroup-using-ADC-as-datasource

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration where we allow the user to select an existing lbvserver on
the NetScaler using datum type parameter. Then a servicegroup for the
selected lb is created if it does not exist on the NetScaler. Finally, the
selected lbvserver is bound to the service "

schema-version: "1.0"

import-stylebooks:
```

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

```
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"


parameters:
  -
    name: selected-vserver
    label: "Select an Existing VServer"
    description: "Load Balancing Application Vservers to be bound to
service on the ADC"
    type: datum
    required: true
    data-source:
      type: managed-adc
      collection: lbvserver


components:
  -
    name: servicegroup-discovery-comp
    type: object
    repeat: $parameters.selected-
vserver.datasource.collections.servicegroup
```

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

```
    repeat-item: svcgrp

    repeat-condition: $svcgrp.attributes.servicegroupname ==
 $parameters.selected-vserver.attributes.name + "-svcgrp"

    properties:

      servicegroupname: $svcgrp.attributes.servicegroupname

  -

    name: servicegroup-creation-if-not-exists-comp

    type: ns::servicegroup

    condition: not exists($components.servicegroup-discovery-comp)

    properties:

      servicegroupname: $parameters.selected-vserver.attributes.name + "-
svcgrp"

      servicetype: $parameters.selected-vserver.attributes.servicetype

    components:

      -

        name: lbvserver-servicegroup-binding

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parameters.selected-vserver.attributes.name

          servicegroupname: $parent.properties.servicegroupname
```

このStyleBookでは、`components`セクションは、選択したロードバランシング仮想サーバー名と`svcgrp`を連結したものに一致するサービスグループ名をチェックします。

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

選択したロードバランシング仮想サーバーの名前が`lbv1`の場合、このStyleBookは`lbv1-svcgrp`という名前のサービスグループをチェックします。見つからない場合、サービスグループ`lbv1-svcgrp`を作成し、`lbv1`仮想サーバーにバインドします。

次の式は、NetScalerインスタンス内のサービスグループのリストを取得します。

```
repeat: $parameters.selected-vserver.datasource.collections.servicegroup
```

この式では:

- `datasource`: NetScaler Consoleによって管理されている選択したNetScalerインスタンスを指します。
- `collections`: NetScalerインスタンス内のすべてのエンティティを指します。
- `servicegroup`: NetScalerインスタンス内のサービスグループを指します。

**コレクションデータのフィルタリング:**

以下のパラメータセクションでは、StyleBook定義で組み込みデータソースコレクションにフィルターを指定する方法を説明します。これにより、StyleBookユーザーはフィルターされたコレクションから特定の項目を選択できます。

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver

      collection-filters:

        protocol: SSL
```

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

```
```

この例では、datumパラメータを使用して、ユーザーがNetScalerインスタンスと、managed-adcデータソースタイプからSSLプロトコルを持つ特定のlbvserverの両方を選択できるようにします。

StyleBookユーザーが仮想サーバーを選択した後、選択された項目の任意の属性は、前のセクションで説明したのと同じ方法でアクセスできます。

## ターゲットNetScalerインスタンスをデータソースとして使用する

設定のターゲットNetScaler自体を、設定のデータソース入力として使用することもできます。このシナリオでは、ターゲットNetScaler上の既存の設定を参照して、そのNetScaler上に新しい設定を作成したい場合があります。

ターゲットインスタンスをデータソースとして使用する場合、StyleBookユーザーがNetScalerインスタンスを選択する必要がないため、`datum`組み込み型パラメーターを使用する必要はありません。ターゲットNetScalerインスタンスからデータを取得する式を、StyleBookの`components`セクションに直接記述できます。

ターゲットNetScalerインスタンスから以下を取得するには、次の式を使用します。

- コレクション:

  ```
  $current-target-as-datasource.collections.<collection-name>
  ```

  例:

  ```
  $current-target-as-datasource.collections.lbvserver
  ```

- 属性:

  ```
  $current-target-as-datasource.collections.attributes.<attribute>
  ```

### ターゲットNetScalerインスタンスをデータソースとして使用するStyleBookの例

ターゲットNetScalerインスタンスをデータソースとして使用する方法を示すStyleBookの例を次に示します。

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

```
---

name: lb-add-service-with-target-adc

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration."

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



components:

  -

    name: servicegroup-comp

    type: ns::servicegroup

    properties:

      servicegroupname: "lb-demo-svcgrp"

      servicetype: "HTTP"
```

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

```
components:
  -
    name: lbvserver-svg-binding
    type: ns::lbvserver_servicegroup_binding
    repeat: $current-target-as-datasource.collections.lbvserver
    repeat-item: lbvsrvr
    repeat-condition: $lbvsrvr.attributes.name == "lb-demo-lb"
    properties:
      name: $lbvsrvr.attributes.name
      servicegroupname: $parent.properties.servicegroupname
```

この例では、構成パックはターゲットNetScalerインスタンス内の負荷分散仮想サーバーをチェックします。そして、指定された負荷分散仮想サーバーのIPアドレスが一致した場合、その名前とサービスグループ名を取得します。

ターゲットNetScalerインスタンスをデータソースとして使用(/en-us/netscaler-application-delivery-management-software/media/target-instance-as-datasource.png)

## カスタムデータソースを使用する

(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/manage-data-sources/built-in-datasource.html)に加えて、入力データが複数の構成を作成するために繰り返し使用される場合、カスタムデータソースを定義して使用できます。入力データをNetScaler Consoleにデータソースとして保存できます。また、StyleBookユーザーが繰り返し入力を提供する必要なく、このデータを消費するようにStyleBookを変更できます。

StyleBook定義でカスタムデータソースを使用する前に、カスタムデータソースを定義するために以下を実行します。

1. (#add-a-data-source-type)。
2. (#add-a-collection-schema-under-data-source-type)。
3. (#add-a-data-source)。

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

4. (#add-a-collection-data)。

データソースを追加した後、StyleBook定義でこのデータソースを使用できます。詳細については、(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/manage-data-sources/built-in-datasource.html)を参照してください。

### データソースタイプを追加する

データが取得されるソースを区別するために、データソースタイプを指定します。

1. **アプリケーション > 構成 > データソース**で。
2. **Data Source Type**を選択し、**Add**をクリックします。
3. データソースタイプの**Name**と**Description**を指定します。
4. **Proceed**をクリックして**Data Source Type**を保存します。変更を保存せずにワークフローを終了するには、**Close**をクリックします。

(/en-us/netscaler-application-delivery-management-software/media/data-source-type.png)

この例では、データソースタイプは**Environment**に設定されています。このタイプは、アプリケーション環境をデータソースとして定義するために使用できます。

### データソースタイプの下にコレクションスキーマを追加する

**データソースタイプ**を追加すると、「「データソースタイプ**」の**コレクションスキーマ**を追加する画面が表示されます。

1. **追加**をクリックします。
2. コレクションスキーマの**コレクション名**を指定します。
3. **説明**を入力します。
4. 必要に応じて、**属性の詳細**の下に属性（名前とそのタイプ）を追加します。
5. **作成**をクリックします。

コレクションタイプ(/en-us/netscaler-application-delivery-management-software/media/add-collection-type.png)

この例では、**App-virtual-servers**コレクションスキーマには4つの属性があります。したがって、保存したいコレクションには、設定されたデータ型のこれらの属性が必要です。

### データソースを追加する

特定のデータソースタイプに対してデータソースを定義します。

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

1. **アプリケーション > 構成 > データソース**に移動します。
2. **データソース**タブを選択し、**追加**をクリックします。
3. **名前**を指定します。
4. 「**データソースタイプ**」を選択し、「**説明**」を入力します。
5. 「**続行**」をクリックして「**データソース**」を保存します。「**閉じる**」をクリックすると、変更を保存せずにワークフローを終了します。

カスタムデータソース(/en-us/netscaler-application-delivery-management-software/media/add-data-source.png)

この例では、「**本番環境**」がデータソースとして追加されています。

### コレクションデータを追加する

**データソース**を追加すると、**データソース**のデータを入力する画面が表示されます。**コレクションスキーマ**のリストが表示されます。

1. コレクションデータを追加する**コレクションスキーマ**を選択します。
2. 「**コレクションデータの管理**」をクリックします。
3. コレクションにデータを追加します。データを1つずつ追加することも、CSVファイルをアップロードすることもできます。CSVファイルをアップロードする場合は、列名がコレクションスキーマの属性名と一致していることを確認してください。
4. 「**OK**」をクリックします。

コレクション(/en-us/netscaler-application-delivery-management-software/media/collection.png)

### コレクションなしでカスタムデータソースを使用する

以下の`parameters`セクションでは、コレクションなしでStyleBook定義にカスタムデータソースを定義する方法について説明します。

```
parameters:

    - name: selected-environment

      label: Select a custom datasource environment

      type: datum

      required: true
```

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

```
      data-source:

        type: "Environment"
```

構成パックGUIには、適用可能なデータソースが表示され、StyleBookユーザーはそれらのいずれかを選択して構成パックを作成できます。

コレクションなしのカスタムデータソース(/en-us/netscaler-application-delivery-management-software/media/custom-datasource-without-collection.png)

この例では、`Production` データソースを使用してデータを取得します。

`Environment` データソースタイプで、`App-virtual-servers` コレクションタイプにアクセスするには、次の式を使用します。

```
$parameters.selected-environment.collections.App-virtual-servers
```

**例のスニペット**:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    repeat: $parameters.selected-environment.collections.App-virtual-
servers

    repeat-item: app

    properties:

      name: $app.attributes.Name + "-lb"

      ipv46: ip($app.attributes.IPv46 )

      port: $app.attributes.Port

      servicetype: $app.attributes.Protocol
```

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

```
    components:


      -

        name: servicegroup-comp

        type: ns::servicegroup

        properties:

          servicegroupname: $parent.properties.name + "-svcgrp"

          servicetype: $parent.properties.servicetype


        components:

          -

            name: lbvserver-svg-binding

            type: ns::lbvserver_servicegroup_binding

            properties:

              name: $parent.parent.properties.name

              servicegroupname: $parent.properties.servicegroupname
```

### コレクションでカスタムデータソースを使用する

以下の `parameters` セクションでは、StyleBook 定義でカスタムデータソースを定義する方法について説明します。これにより、StyleBook ユーザーはコレクションの特定の項目を選択できます。

```
parameters:

  - name: selected-app-vserver
```

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

```
    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

この例では、`datum` パラメータを使用してカスタムデータソースを定義します。これは、`Production` データソースを使用して `App-virtual-servers` コレクションスキーマからデータを取得します。

`Environment` データソースタイプで、`App-virtual-servers` コレクションからプロトコルにアクセスするには、次の式を使用します。

```
$parameters.selected-app-vserver.attributes.Protocol
```

**例のスニペット**:

```
components:

  - name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $parameters.selected-app-vserver.attributes.Name

      ipv46: $parameters.selected-app-vserver.attributes.IPv46

      port: $parameters.selected-app-vserver.attributes.Port

      servicetype: $parameters.selected-app-vserver.attributes.Protocol
```

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

`parameters` セクションでコレクションタイプを定義すると、StyleBook ユーザーはデータソースとコレクションを選択できます。

**コレクションから複数の項目を選択する:**

以下のパラメータセクションでは、StyleBook ユーザーがコレクションの複数の項目を選択できます。

```
parameters:

  - name: selected-app-vservers

    label: Select app-vservers from the collection

    type: datum[]

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

この例では、datum パラメータを使用してカスタムデータソース配列を定義します。ユーザーは、単一のデータソースまたは複数のデータソースから「App-virtual-servers」コレクションから1つ以上の項目を選択できます。

以下のコードスニペットは、選択された項目とその属性にアクセスする方法を示しています。

```
components:

  -

   name: lbvserver-comp

   type: ns::lbvserver

   repeat:

   repeat-list: $parameters.selected-app-vservers
```

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

```
   repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.Name

      ipv46: $vserverObj.attributes.IPv46

      port: $vserverObj.attributes.Port

      servicetype: $vserverObj.attributes.Protocol
```

**コレクションデータのフィルタリング:**

以下のパラメータセクションでは、StyleBook 定義でカスタムデータソースコレクションにフィルタを指定する方法について説明します。これにより、StyleBook ユーザーはフィルタリングされたコレクションから特定の項目を選択できます。

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers

      collection-filters:

        Protocol: SSL
```

この例では、datum パラメータを使用してカスタムデータソースを定義します。これは、Environment タイプのデータソースを使用して、App-virtual-servers コレクションスキーマからフィルタリングされたデータを取得します。

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

StyleBook ユーザーが仮想サーバーを選択した後、選択したアイテムの任意の属性は、前のセクションで説明したのと同じ方法でアクセスできます。

## APIを使用してStyleBookから構成を作成する

StyleBookを構築したら、NetScaler Console GUIを使用するか、NetScaler Console APIを使用してインポートする必要があります。インポート時にNetScaler ConsoleはStyleBookを検証します。検証が成功すると、StyleBookはNetScaler ConsoleのStyleBookカタログに表示され、構成の作成に使用できるようになります。

このStyleBookに基づいて構成を作成するために、StyleBook APIを使用できるようになりました。cURLコマンドラインツールやPostman Chromeブラウザ拡張機能など、任意のツールを使用してNetScaler ConsoleにHTTPリクエストを送信できます。

### 例1

StyleBook to Create a Load Balancing Virtual Serverで作成したlb-vserver StyleBookを検討してください。このStyleBookから構成パックを作成するには、REST APIを次のように使用します。

**HTTPメソッド**: POST **URL**: `https://<IP>/stylebook/nitro/v2/config/configpacks`

**リクエストヘッダー**:

コンテンツタイプ: application/json

受諾: application/json

**リクエストボディペイロード**:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31"
```

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

```
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

このHTTPリクエストでは、IPアドレス10.102.117.31を持つロードバランシング仮想サーバー `lb1` が、インスタンスID「deecee30-f478-4446-9741-a85041903410」を持つNetScalerインスタンス上に作成されます。NetScalerインスタンスのインスタンスIDはNetScaler Consoleから取得されます。

NetScaler Consoleによって管理されているインスタンスのIDを取得するには、NetScaler Console APIを使用できます。たとえば、IPアドレスが192.168.153.160であるNetScalerインスタンスのインスタンスIDを取得するには、次のAPIを使用できます。

**HTTPメソッド**: GET

**URL**: `https://<IP>/nitro/v2/config/ns?filter=ip_address:192.168.153.160`

**リクエストヘッダー**:

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

受け入れ: application/json

レスポンスにはjsonペイロードにIDが含まれています。

**予期される応答ヘッダー（成功時）：**

200 OK

コンテンツタイプ: application/json

**予期される応答本文（成功時）：**


```
{
  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {
    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
```


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

```
    }
  ]
}
```

設定（config pack）が正常に作成されると、以下のHTTP応答が返されます。

**予期される応答ヘッダー（成功時）：**

202 OK

コンテンツタイプ: application/json

**予期される応答本文（成功時）：**

```
{
  "job":
  {
    "job_id": "1460806080"
  }
}
```

ID 1460806080 を使用して一意に識別される最初のジョブを作成しました。このIDを使用して、設定のクエリ、更新、または削除を行うことができます。

ジョブのステータスを照会するには、以下のURLを使用できます。

`https://<IP>/stylebook/nitro/v2/config/jobs/<jobid>`.

## 例 2

同じStyleBookを使用して、別の設定パックを作成し、同じまたは異なるNetScalerインスタンスで実行できます。この例では、別の設定を作成し、仮想サーバーに異なる名前とIPアドレスを指定します。ロードバランシング方法としてLEASTCONNECTIONを指定します。この設定を2つのNetScalerインスタンスに展開します。

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

HTTPリクエストは次のとおりです。

**HTTPメソッド**: POST

**URL**: `https://<IP>/stylebook/nitro/v2/config/configpacks`

**リクエストヘッダー**:

コンテンツタイプ: application/json

アクセプト: application/json

**リクエストボディペイロード**:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31",
      "lb-alg": "LEASTCONNECTION"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "instance_id": "abcdee30-f478-4446-9741-a85041903410"
```

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

```
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

このHTTPリクエストでは、IPアドレス10.102.117.31を持つロードバランシング仮想サーバーlb1が、インスタンスID「deecee30-f478-4446-9741-a85041903410」と「abcdee30-f478-4446-9741-a85041903410」を持つ2つのNetScalerインスタンス上に作成されます。

設定パックが正常に作成されると、次のHTTPレスポンスが受信されます。

**予期されるレスポンスヘッダー (成功時)**:

202 OK

コンテンツタイプ: application/json

**予期されるレスポンスボディ (成功時)**:

```
{
    "job": {
        "job_id": "165769629"
    }
}
```

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

この新しい設定パックには、異なるID 1657696292があります。このIDを使用して、この設定を更新または削除できます。

## 例 3

基本的な負荷分散構成を作成するためのStyleBookで作成した「basic-lb-config」StyleBookを検討します。このStyleBookからREST APIを使用してconfig packを作成するには、次の手順に従います。

**HTTPメソッド**: POST

**URL**: `https://<IP>/stylebook/nitro/v2/config/configpacks`

**リクエストヘッダー**:

コンテンツタイプ: application/json

アクセプト: application/json

**リクエストボディペイロード**:

```
Content-Type: application/json

Accept: application/json

{

  "configpack":

  {

    "parameters":

    {

      "name": "myapp",

      "ip": "10.70.122.25",

      "svc-servers": ["192.168.100.11","192.168.100.12"],

       "svc-port": 8080

    },
```

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

```
    "targets":
    [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abcdefgi-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "basic-lb-config",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
}
```

**予期される応答ヘッダー（成功時）**:

202 OK

コンテンツタイプ: application/json

**予期される応答ボディ（成功時）**:

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

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

このHTTPリクエストでは、負荷分散構成が2つのNetScalerインスタンスで実行されます。これらのNetScalerインスタンスにログオンして、仮想サーバーと、2つのサービスがバインドされたサービスグループが作成されているかどうかを確認できます。

## 例 4

複合StyleBookの作成で作成した複合StyleBook「**composite-example**」を検討します。このStyleBookからREST APIを使用してconfig packを作成するには、次の手順に従います。

**HTTP メソッド**: POST

**URL**: `https://<IP>/stylebook/nitro/v2/config/configpacks`

**リクエストヘッダー**:

コンテンツタイプ: application/json

アクセプト: application/json

**リクエストボディペイロード**:

```
{

  "configpack":

  {

    "parameters": {

      "name": "myapp",

      "ip": "2.2.2.2",
```

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

```
      "svc-servers": ["10.102.29.52","10.102.29.53"]
    },
    "targets":
    [
     {
      "id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "id": "abcdefgg-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "composite-example",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
```

このHTTPリクエストでは、設定はIDで表される2つのNetScalerインスタンス上に作成されます。NetScalerインスタンスにログインすると、「composite-example」StyleBookにインポートされた「basic-lb-config」StyleBookによって作成された設定オブジェクトを表示できます。また、「composite-example」StyleBookの一部であったmyapp-monという新しいHTTPモニターも確認できます。

設定パックの作成が成功すると、以下のHTTPレスポンスが受信されます。

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

**予期されるレスポンスヘッダー (成功時)**:

202 OK

コンテンツタイプ: application/json

**予期されるレスポンスボディ (成功時)**:

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

### 設定の更新

IPアドレス10.102.29.54を持つ新しいバックエンドサーバーで更新したい設定があるとします。そのサーバーをロードバランシング仮想サーバーmyappに追加するには、以下のAPIを使用します。

**HTTP メソッド**: PUT

**URL**: `https://<IP>/stylebook/nitro/v2/config/configpacks/<configpackid>`

**リクエストヘッダー**:

コンテンツタイプ: application/json

承認: application/json

**リクエストボディペイロード**:

```
{

  "configpack": {

    "parameters": {

      "name": "myapp",
```

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

```
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
  },
  "targets":
   [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abdcedff-d589-4557-8632-a74032802412"
     }
   ]
  }
}
```

設定パックの更新が成功すると、以下のHTTPレスポンスが受信されます。

**予期されるレスポンスヘッダー (成功時)**:

202 OK

コンテンツタイプ: application/json

**予期されるレスポンスボディ (成功時)**:

```
{
    "job": {
        "job_id": "3628681382"
```

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

```
    }

}
```

### 設定の削除

この設定 (すべてのNetScalerインスタンスから) を削除するには、設定パックを削除するためのAPIを次のように使用できます。

設定パックの削除が成功すると、以下のHTTPレスポンスが受信されます。

**HTTPメソッド**: DELETE

**URL**: `https://<DNS-or-IP>//stylebook/nitro/v2/config/configpacks/<configpackid>`

**リクエストヘッダー**:

受け入れ: application/json

**予期される応答ヘッダー (成功時)**:

202 OK

コンテンツタイプ: application/json

**予期される応答ペイロード (成功時)**:

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

NetScalerインスタンスにログオンし、この構成パックの一部であるすべての構成オブジェクトが削除されていることを確認します。

すべてのインスタンスからではなく、特定のNetScalerインスタンスから構成を削除するには、構成の更新で構成パックの更新操作を使用します。JSONペイロードのターゲット属性を変更して、特定のNetScalerインスタンスIDを削除します。

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

## APIを使用して、証明書とキーファイルをアップロードするための構成を作成する

このStyleBookに基づいて構成を作成するには、StyleBook APIを使用します。curlコマンドラインツールやPostman Chromeブラウザ拡張機能など、任意のツールを使用してNetScaler ConsoleにHTTPリクエストを送信できます。

NetScaler ConsoleにSSL証明書と証明書キーファイルをアップロードするStyleBookを作成する方法で、証明書とキーファイルをアップロードするために作成したStyleBookの例を検討してください。このStyleBookから構成パックを作成するには、次のようにREST APIを使用します。

```
POST



https://<MAS_IP_Address>/stylebook/nitro/v2/config/configpacks?mode=async
```

```
Content-Type: application/jsonAccept: application/json



{

    "configpack": {

        "stylebook": {

            "name": "lb-mon_test",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "2.0"

        },

        "parameters": {

            "lb-service-type": "SSL",

            "ip-address-type": "IP Address",
```

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

```
            "lb-appname": "testvip",
            "lb-virtual-port": 80,
            "svc-service-type": "SSL",
            "lb-virtual-ip": "10.10.20.11",
            "certificates": [
                {
                    "ssl-inform": "PEM",
                    "certkey-param": {
                        "id": "d0982579-42a9-417a-b24e-1f9ae5592f1d",
                        "name": "testcertkey"
                    }
                }
            ]
        },
        "targets": [
            {
                "instance_id": "f383b454-b777-454a-8c17-c477f0bad21e"
            }
        ]
    }
}
```


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

```
```

この構成パックは、ID f383b454-b777-454a-8c17-c477f0bad21eを使用して一意に識別されます。このIDを使用して、構成のクエリ、更新、または削除を行うことができます。構成パックが正常に更新されると、証明書とキーファイルはNetScaler Consoleファイルシステムにアップロードされます。

## APIを使用して、あらゆるファイルタイプをアップロードする構成を作成する

NetScaler Console APIを使用して、選択したNetScalerインスタンスにファイルをアップロードする構成パックを作成することもできます。 あらゆる種類のファイルをアップロードする例については、NetScaler MAサービスにファイルをアップロードするStyleBookを作成する方法を参照してください。 例で説明されているように、構成パックを作成し、「locationfile」パラメーターの値をNetScaler Console上のロケーションファイルのファイルパスに設定します。 このStyleBookから構成パックを作成するには、次のようにREST APIを使用します。

```
POST



https://<mas_ip>/stylebook/nitro/v2/config/configpacks?mode=sync
```

```
Content-Type: application/json

Accept: application/json

{

    "configpack": {

        "stylebook": {

            "name": "upload-geolocations",

            "namespace": "com.citrix.adc.stylebooks.samples",

            "version": "1.0"

        },
```

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

```
        "parameters": {
            "locationfile": {
                "name": "servercert1.key",
                "contents": "<base64-contents>",
                "encoding_type": "base64"
            }
        },
        "targets": [
            {
                "instance_id": "d9dca475-abde-47ef-bf99-8434fe6ad886"
            }
        ]
    }
}
```

## APIを使用してカスタムStyleBookをインポートする

NetScaler ConsoleにカスタムStyleBookをインポートするために、StyleBook APIを使用できるようになりました。curlコマンドラインツールやPostman Chromeブラウザ拡張機能などの任意のツールで、このStyleBookから設定パックを作成するには、次のようにREST APIを使用します。たとえば、NetScalerインスタンスでロードバランサー設定を作成するために使用できる、example-lbという名前のStyleBookをインポートできます。

```
HTTP Method: POST

URL: http://<mas-ip>/stylebook/nitro/v2/config/stylebooks/actions/import?
mode=sync
```

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

```
Headers:

Content-Type: application/json

Accept: application/json

RequestBody:

{

    "import": {

        "file_name": "example-lb.yaml",

        "source": "<base64-contents>",

        "encoding": "base64"

    }

}
```

ここで、「source」属性の値は、StyleBookファイルの内容のbase64エンコーディングです。StyleBookファイルのYAMLコンテンツをオンラインツールに貼り付け、例えば、`<https://www.browserling.com/tools/file-to-base64>` を使用して、上記の「source」属性の値として使用できるbase64文字列を取得できます。

このAPI呼び出しを使用すると、複数のStyleBookファイルを含む圧縮tarballファイル（.tgzファイル）を1つのAPI操作でアップロードすることもできます。これを行うには、file_name属性を.tgzファイル名に変更し、source属性の値を.tgzファイルの内容のbase64エンコーディングに変更するだけです。

ツールでAPIが正常に実行されると、StyleBookがNetScaler Consoleにインポートされたことを示す次の応答が得られます。

```
200 OK
```

**応答本文:**

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

```
{

    "import": {

        "name": "example-lb",

        "namespace": "com.citrix.adc.stylebooks",

        "version": "2.0"

    }

}
```

## APIを使用してカスタムStyleBookをダウンロードする

以下のStyleBooks REST APIを提供することで、カスタムStyleBookをダウンロードできます。

```
POST

http://<MAS_IP>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>/actions/actions/download?dependencies=true



payload



dependencies=true
```

IPアドレス、名前、バージョン、および名前空間フィールドを変更した後、curlコマンドラインツールやPostman Chromeブラウザ拡張機能などの任意のツールでAPIを実行できます。

```
POST



http://10.102.201.246/stylebook/nitro/v2/config/stylebooks/
com.samples.adc.stylebooks/1.2/lb-mon/actions/download?dependencies=true
```

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

```
payload

dependencies=true
```

.yaml形式のStyleBookがダウンロードされます。

## APIを使用してカスタムStyleBookを削除する

次のStyleBook REST APIを提供することで、カスタムStyleBookを削除できます。

```
DELETE



http://<MAS_IP>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>?dependencies=true
```

URL内の依存関係クエリパラメータが指定されていない場合、またはその値がfalseに設定されている場合、StyleBookの依存関係は削除されません (StyleBook自体のみが削除されます)。

HTTP応答ステータスコード200を受信した場合、それはカスタムStyleBookとその依存関係がNetScaler Consoleから正常に削除されたことを意味します。

**注:**

MA Service内に、それに依存する他のStyleBookがあるカスタムStyleBookは削除できません。

たとえば、NetScaler Consoleで「lb-virtual-ssl-extended」という名前のStyleBookを作成したとします。後でそのStyleBookを削除することにしました。

IPアドレス、名前、バージョン、および名前空間のフィールドを変更した後で、APIはcurlコマンドラインツールやPostman Chromeブラウザ拡張機能など、任意のツールで実行できます。

DELETE `<http://10.102.201.246/stylebook/nitro/v2/config/stylebooks/com.citrix.adc.stylebooks/2.0/lb-mon_delete?dependencies=false>`

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

StyleBookはNetScaler Consoleから削除されます。

## StyleBooks の文法

独自の StyleBooks を設計し、NetScaler Console にインポートして、NetScaler Console GUI または API を使用して構成を作成できます。独自の StyleBooks を作成できるようにするには、まず、使用できるさまざまな構成要素と属性の文法と構文を理解する必要があります。

このドキュメントでは、StyleBooks の作成時に使用できるさまざまな構成要素と参照について説明します。

詳細を表示するには、以下の表のセクション、構成要素、または参照名をクリックしてください。

| | |
|---|---|
| ヘッダー | StyleBooks のインポート |
| パラメータ | パラメータのデフォルトソース構成要素 |
| 置換 | コンポーネント |
| オプションのプロパティ | ヘルパーコンポーネント |
| プロパティのデフォルトソース | ネストされたコンポーネント |
| 条件構成要素 | 「繰り返しコンストラクト」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/repeat-construct.html) |
| 「繰り返し条件コンストラクト」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/repeat-condition-construct.html) | 「出力」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/outputs.html) |
| 「ネストされた繰り返し」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/nested-repeats.html) | 「親参照」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/parent-reference.html) |
| 「パラメータ参照」(/ja-jp/netscaler-application-delivery-management-software/ | 「置換参照」(/ja-jp/netscaler-application-delivery-management-software/current- |

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

| | |
|---|---|
| current-release/stylebooks/stylebooks-grammar/parameter-reference.html) | release/stylebooks/stylebooks-grammar/substitutions-reference.html) |
| 「コンポーネント参照」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/components-reference.html) | 「操作」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/operations.html) |
| 「変数参照」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/variable-reference.html) | 「アラーム」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/alarms.html) |
| 「アナリティクス」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/analytics.html) | 「組み込み関数」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/built-in-functions.html) |
| 「式」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/expressions.html) | 「依存関係の検出」(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/dependency-detection.html) |
| インプレース補間(/ja-jp/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar/in-place-interpolations.html) | |

**注**

repeat-item、repeat-index、または置換関数の引数を定義する際に、ユーザー定義変数の名前に以下の予約語を使用しないでください、$`<var-name>`

- stylebook、パラメータ、置換、コンポーネント、プロパティ、出力、親、自身、操作、分析、アラーム
- リピートアイテム, リピートアイテム-0, リピートアイテム-1, リピートアイテム-2
- リピートインデックス, リピートインデックス-0, リピートインデックス-1, リピートインデックス-2
- デフォルト

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

- ロール、ロール、ターゲット、ターゲット
- コンテキスト、parent-context、parent_context

独自のStyleBookを設計する方法に関する情報と例については、「独自のStyleBookを作成する方法」を参照してください。

## ヘッダー

StyleBookの最初の6行はヘッダーセクションを構成します。このセクションでは、StyleBookのIDを定義し、その機能について説明できます。これは必須セクションです。

次の表は、ヘッダーセクションの属性について説明しています。

| 属性 | 説明 |
| --- | --- |
| 名前 | StyleBookを識別するための名前です。この属性は必須です。 |
| 表示名 | StyleBookの記述的な名前です。この名前はNetScaler Console GUIに表示されます。これはオプションの属性です。 |
| 説明 | このStyleBookが何をするかを定義する説明テキストです。この説明はNetScaler Console GUIに表示されます。これはオプションの属性です。**注:** これはHTMLフラグメントであり、HTMLタグを使用して見出しをカスタマイズしたり、URLまたは埋め込み画像を含む`<img>`タグを使用して画像を挿入したりできます。 |
| 作成者 | StyleBookを作成する作成者（個人または組織）です。これはオプションの属性です。 |
| 名前空間 | 名前の衝突を避けるために、名前空間はStyleBookの一意の識別子の一部を形成します。名前空間は任意の文字列にできますが、StyleBookのセットを作成または所有する会社、部門、または単位に名前を付けるために使用するのが良い習慣です。たとえば、次の形式を使用できます: `<company>.<department>.<unit>.stylebooks`。これは必須属性です。 |

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

| 属性 | 説明 |
| --- | --- |
| バージョン | StyleBookのバージョン番号。StyleBookを更新する際にバージョン番号を変更できます。異なるバージョンのStyleBookは共存できます。これは必須属性です。 |
| スキーマバージョン | StyleBooksスキーマのバージョン。NetScaler Consoleの現在のリリースでは「1.0」という値を取ります。これは必須属性です。 |
| プライベート | この属性がtrueに設定されている場合、StyleBookはNetScaler Console GUIに表示されません。これは、他のStyleBookの構成要素であり、ユーザーが直接使用することを意図していないStyleBookにとって便利な設定です。これはオプション属性です。デフォルト値はfalseです。 |

**例**:

```
    name: lb

    description: "This stylebook defines a sample load balancing
configuration."

    display-name: "Load Balancing StyleBook (HTTP)"

    author: Mike Smith (ACME Infra team)

    namespace: com.example.stylebooks

    schema-version: "1.0"

    version: "0.1"
```

名前、名前空間、およびバージョンの組み合わせによって、システム内でStyleBookが一意に識別されます。NetScaler Consoleでは、名前、名前空間、およびバージョンの組み合わせが同じStyleBookを2つ持つことはできません。ただし、名前とバージョンが同じで名前空間が異なる

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

StyleBook、または名前空間とバージョンが同じで名前が異なるStyleBookを持つことはできます。

## StyleBookのインポート

これはStyleBookの2番目のセクションで、現在のStyleBookから参照したい他のStyleBookを宣言できます。これにより、独自のStyleBookで同じ構成を再構築する代わりに、他のStyleBookをインポートして再利用できます。これは必須セクションです。

現在のStyleBookで参照したいStyleBookの**名前空間**と**バージョン**番号を宣言する必要があります。すべてのStyleBookは、NITRO構成オブジェクトを直接使用する場合、netscaler.nitro.config名前空間を参照する必要があります。この名前空間には、lbvserverサービスやモニターなど、すべてのNetScaler NITROタイプが含まれています。NetScalerバージョン10.5以降のStyleBookがサポートされており、これは、StyleBookを使用してリリース10.5以降を実行している任意のNetScalerインスタンスで構成を作成および実行できることを意味します。

import-stylebooksセクションで使用される**プレフィックス**属性は、名前空間とバージョンの組み合わせを参照するための省略形です。たとえば、「ns」プレフィックスは、バージョン10.5のnetscaler.nitro.config名前空間を参照するために使用できます。StyleBookの後のセクションでは、この名前空間とバージョンを持つStyleBookを参照するたびに名前空間とバージョンを使用する代わりに、選択したプレフィックス文字列とStyleBookの名前を組み合わせて使用するだけで、一意に識別できます。

**例**:

```
import-stylebooks:
 -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
-
 namespace: com.acme.stylebooks
  version: "0.1"
```

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

```
        prefix: stlb
```

上記の例では、最初に定義されたプレフィックスはnsと呼ばれ、netscaler.nitro.config名前空間とバージョン10.5を参照します。2番目に定義されたプレフィックスはstlbと呼ばれ、com.acme.stylebooks名前空間とバージョン0.1を参照します。

プレフィックスを定義した後、特定の名前空間とバージョンに属するタイプまたはStyleBookを参照したい場合は常に、**\<namespace-shorthand\>::\<type-name\>**という表記を使用できます。たとえば、**ns::lbvserver**は、netscaler.nitro.config名前空間、バージョン10.5で定義されているlbvserverタイプを参照します。

同様に、com.acme.stylebooks名前空間でバージョン「0.1」のStyleBookを参照したい場合は、**stlb::\<stylebook-name\>**という表記を使用できます。

**注**

慣例により、プレフィックス「ns」はNetScalerのNITRO名前空間を参照するために使用されます。

## パラメータ

このセクションでは、設定を作成するためにStyleBookで必要となるすべてのパラメータを定義できます。StyleBookが受け取る入力を記述します。このセクションはオプションですが、ほとんどのStyleBookで必要となる場合があります。パラメータセクションは、StyleBookを使用してNetScalerインスタンスで設定を作成するユーザーのためのフィールドを定義するものと考えることができます。

StyleBookをNetScaler Consoleにインポートして設定を作成する際、GUIはStyleBookのこのセクションを使用してフォームを表示します。このフォームは、定義されたパラメータ値の入力を受け取ります。

次のセクションでは、このセクションの各パラメータに指定する必要がある属性について説明します。

### 「名前」

定義したいパラメータの名前です。英数字の名前を指定できます。

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

名前はアルファベットで始まり、さらにアルファベット、数字、ハイフン（-）、またはアンダースコア（_）を含めることができます。

StyleBookを作成する際、この「name」属性を使用して、$parameters.\<name>という表記で他のセクションのパラメータを参照できます。

**必須**ですか？はい

### 「ラベル」

NetScaler Console GUIでこのパラメータの名前として表示される文字列です。

**必須**ですか？いいえ

### 「説明」

パラメータの用途を説明するヘルプ文字列です。ユーザーがこのパラメータのヘルプアイコンをクリックすると、NetScaler Console GUIにこのテキストが表示されます。

**必須**ですか？いいえ

### 'タイプ'

これらのパラメータが取りうる値のタイプ。パラメータは、以下の 組み込みタイプのいずれかになります。

- string: 文字の配列。長さが指定されていない場合、文字列値は任意の数の文字を取ることができます。ただし、min-lengthおよびmax-length属性を使用することで、文字列型の長さを制限できます。
- `number`: 整数。min-valueおよびmax-value属性を使用することで、このタイプが取りうる最小値と最大値を指定できます。
- `boolean`: trueまたはfalseのいずれかになります。YAMLは、すべてのリテラルをブール値と見なします（例: YesまたはNo）。
- `ipaddress`: 有効なIPv4またはIPv6アドレスを表す文字列。
- `ipnetwork`: 2つの部分から構成されます。最初の部分はIPアドレスで、2番目の部分はネットマスクです。

  ネットマスクは、ネットマスク長 ( `netmask-len` ) またはネットマスクIPアドレス ( `netmask_ip` ) で構成されます。ネットマスク長は、IPv6アドレスの場合、0〜32および0〜

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

128の間の整数です。これは、ネットワーク内のIPアドレス数を決定するために使用されます。

NetScaler Console GUIから構成パックを作成または更新する際、以下のいずれかのアクションを実行できます。

- ネットマスク長を有効にし、IPアドレスとネットマスク長を入力します
- ネットマスク長を無効にし、IPアドレスとネットマスクIPアドレスを入力します

APIでは、ネットマスク長とネットマスクIPアドレスは、次の例に示すように単一の値として利用できます。

**例:**

```
Content-Type: application/json

Accept: application/json

{

“configpack”:

{

      “stylebook”: {

      “namespace”: “com.example.stylebook”,

      “version”:“1.0”,

      “name”: “ipnetwork-example”,

      ..

      },

      “parameters”: {

         “name: “test-app”,

          “virtual-ip”: “212.100.30.0/255.255.255.0”,

      },
```

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

```
        “targets”:

        [

        ]

  }

  }
```

- `tcp-port`: TCPまたはUDPポートを表す0から65535までの数値。
- `password`: 不透明な/秘密の文字列値を表します。NetScaler Console GUIがこのパラメータの値を表示するとき、アスタリスク (*****) として表示されます。
- `certfile`: 証明書ファイルを表します。この値を使用すると、NetScaler Console GUIを使用してStyleBook構成を作成する際に、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、NetScaler Consoleのディレクトリ `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` に保存されます。

  証明書ファイルは、NetScaler Consoleによって管理される証明書のリストに追加されます。
- `keyfile`: 証明書キーファイルを表します。この値を使用すると、NetScaler Console GUIを使用してStyleBook構成を作成する際に、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、NetScaler Consoleのディレクトリ `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` に保存されます。

  証明書キーファイルは、NetScaler Consoleによって管理される証明書キーのリストに追加されます。
- `file`: ファイルを表します。
- `object`: このタイプは、関連する複数のパラメータを親要素の下にグループ化する場合に使用します。親パラメータのタイプを「object」として指定します。「object」タイプのパラメータには、含まれるパラメータを記述するためのネストされた「parameters」セクションを含めることができます。
- `another StyleBook`: このタイプのパラメータを使用する場合、このパラメータは、そのタイプを示すStyleBookで定義されたパラメータの形式で値が指定されることを期待します。

パラメータは、タイプのリストである `type` を持つこともできます。そのためには、タイプの最後に `[]` を追加します。たとえば、`type` 属性が `string[]` の場合、このパラメータは文字列

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

のリストを入力として受け取ります。このStyleBookから構成を作成する際に、このパラメータに1つ、2つ、または複数の文字列を指定できます。

**必須**ですか？はい

### 'ネットワーク'

`type: ipaddress` の場合、NetScaler Console IPAMネットワークからIPアドレスを自動割り当てするために `network` 属性を指定できます。

StyleBook構成を作成すると、NetScaler Consoleは `network` 属性からIPアドレスを自動割り当てします。

例：

```
name: virtual-ip

label: "Load Balancer IP Address"

type: ipaddress

network: "network-1"

required: true
```

この例では、`virtual-ip` フィールドは `network-1` からIPアドレスを自動割り当てします。構成が削除されると、IPアドレスはネットワークに解放されます。

### 「動的割り当て」

`dynamic-allocation` 属性は `type:ipaddress` のパラメータ定義に追加されます。この属性を使用して、NetScaler Console IPAM ネットワークを動的にリストします。この属性は、入力として `true` または `false` のいずれかを受け入れることができます。`type: ipaddress` の場合、NetScaler Console にある NetScaler Console IPAM ネットワークを動的にリストするには、`dynamic-allocation: true` 属性を指定します。設定パック作成フォームでは、次のことができます。

1. リストから必要な IPAM ネットワークを選択します。
2. 選択した IPAM ネットワークから割り当てる IP アドレスを指定します。

   IP アドレスが指定されていない場合、NetScaler Console は選択した IPAM ネットワークから IP アドレスを自動割り当てします。

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

**例:**

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"

  type: ipaddress

  dynamic-allocation: true

  required: true
```

この例では、`virtual-ip` フィールドに NetScaler Console にある NetScaler Console IPAM ネットワークがリストされます。リストからネットワークを選択して、そのネットワークから IP アドレスを自動割り当てします。設定が削除されると、IP アドレスはネットワークに解放されます。

### 「キー」

このパラメータが StyleBook のキーパラメータであるかどうかを示すために、true または false を指定します。

StyleBook には、「キー」パラメータとして定義されたパラメータを1つしか持つことができません。

同じStyleBookから異なる構成を作成する場合（同じまたは 異なるNetScalerインスタンス上）、各構成はこの パラメータに対して異なる/一意の値を持ちます。

デフォルト値は false です。

**必須**ですか？ いいえ

### 「必須」

パラメータが必須かオプションかを示すために、trueまたはfalseを指定します。trueに 設定されている場合、そのパラメータは必須であり、ユーザーは構成を作成する際にこの パラメータの値を指定する必要があります。

NetScaler Console GUI は、このパラメーターに有効な値を指定するようユーザーに強制します。

デフォルト値は false です。

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

**必須**ですか？ いいえ

### '許可される値'

この属性を使用して、型が「string」に設定されている場合に、パラメーターの有効な値のリストを定義します。

NetScaler Console GUI から構成を作成する際、ユーザーはこのリストからパラメーター値を選択するよう求められます。

**注**

リスト値をラジオオプションとして表示したい場合は、`layout` 属性を設定します。

**例 1：**

```
-

      name: ipaddress

      type: string

      allowed-values:

            -  SOURCEIP

            -  DEST IP

            -  NONE
```

**例 2：**

```
-

      name: TCP Port

      type: tcp-port

      allowed-values:

            -  80
```

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

```
            -  81

            -  8080
```

**例 3：**

`tcp-ports` のリスト。リストの各要素は、`allowed-values` で指定された値のみを持つことができます。

```
-

      name: tcpports

      type: tcp-port[]

      allowed-values:

            -  80

            -  81

            -  8080

            -  8081
```

**必須**ですか？ いいえ

### 'デフォルト'

この属性を使用して、オプションのパラメーターにデフォルト値を割り当てます。ユーザーが値を指定せずに構成を作成した場合、デフォルト値が使用されます。

以下の条件が満たされた場合、パラメータは値を取りません。

- パラメータにデフォルト値がありません。
- ユーザーがパラメータに値を指定しません。

**例 1：**

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

```
-

      name: timeout

      type: number

      default: 20
```

**例 2：**

パラメータのデフォルト値を一覧表示するには：

```
-

      name: protocols

      type: string[]

      default:

            -  TCP

            -  UDP

            -  IP
```

**例 3：**

```
-

      name: timeout

      type: number

      default: 20
```

**例 4：**

```
-

      name: tcpport
```

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

```
      type: tcp-port

      default: 20
```

**必須**ですか？ いいえ

### 「パターン」

この属性を使用して、パラメータのタイプが「string」の場合に、この パラメータの有効な値のパターン（正規表現）を定義します。

**例**：

```
-

      name: appname

      type: string

      pattern: "[a-z]+"
```

**必須**ですか？ いいえ

### 「最小値」

この属性を使用して、`number` または `tcp-port` 型のパラメータの最小値を定義します。

**例**:

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

数値の`min-value`は負の値にすることができます。ただし、`tcp-port`の`min-value`は正の値である必要があります。

**必須**? いいえ

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

### '最大値'

この属性を使用して、`number`または`tcp-port`型のパラメータの最大値を定義します。

定義されている場合、最大値が最小値より大きいことを確認してください。

**例**:

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000

      max-value: 15000
```

**必須**? いいえ

### '最小長'

この属性を使用して、「string」型のパラメータに受け入れられる値の 最小長を定義します。

値として定義された文字の最小長が0以上であることを確認してください。

**例**:

```
-

      name: appname

      type: string

      min-length: 3
```

**必須**? いいえ

### '最大長'

この属性を使用して、「string」型のパラメータに受け入れられる値の 最大長を定義します。

値の最大長が、`min-length`で定義された文字の長さ以上であることを確認してください。

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

**例：**

```
-

      name: appname

      type: string

      max-length: 64
```

**必須？**いいえ

### '最小項目数'

この属性を使用して、リストであるパラメータの最小項目数を定義します。

最小項目数が0以上であることを確認してください。

**例：**

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2
```

**必須？**いいえ

### '最大項目数'

この属性を使用して、 リストであるパラメータの最大項目数を定義します。

最大項目数が、定義されている場合は最小項目数よりも大きいことを確認してください。

**例：**

```
-

      name: server-ips

      type: ipaddress[]
```

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

```
      min-items: 2

      max-items: 250
```

**必須**？いいえ

### 'GUI'

この属性を使用して、NetScaler Console GUIでのパラメータのレイアウトをカスタマイズします。

**必須**ですか？ いいえ

### 「カラム」

この属性は、`gui` 属性のサブ属性です。この属性を使用して、NetScaler Console GUI に `type: object[]` パラメータを表示する列の数を定義します。

**必須**ですか？ いいえ

### 「更新可能」

この属性は、`gui` 属性のサブ属性です。この属性を使用して、設定作成後にパラメータを更新できるかどうかを指定します。この属性は、文字列、ブール値、数値などの単純なパラメータ型にのみ設定してください。

値が `false` に設定されている場合、設定を更新するときに、パラメータフィールドはグレー表示されます。

**必須**ですか？ いいえ

### 「'collapse_pane'」

この属性は、`gui` 属性のサブ属性です。この属性を使用して、このオブジェクトパラメータのレイアウトを定義するペインを折りたたみ可能にするかどうかを指定します。

値が true に設定されている場合、ユーザーはこの親パラメータの下にある子パラメータを展開または折りたたむことができます。

**例**:

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

```
gui:


 collapse_pane: true


 columns: 2
```

完全なパラメータセクションの例:

```


parameters:


   -


      name: name


      label: Name


      description: Name of the application


      type: string


      required: true
```

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

```
-

   name: ip

   label: IP Address

   description: The virtual IP address used for this application

   type: ipaddress

   required: true

-

   name: svc-servers

   label: Servers

   type: object\[\]

   required: true
```

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

```
    parameters:

      -

            name: svc-ip

            label: Server IP

            description: The IP address of the server

            type: ipaddress

            required: true

      -

            name: svc-port

            label: Server Port

            description: The TCP port of the server
```

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

```
            type: tcp-port

            default: 80

        -

            name: lb-alg

            label: LoadBalancing Algorithm

            type: string

            allowed-values:

               - ROUNDROBIN

               - LEASTCONNECTION

            default: ROUNDROBIN

        -
```

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

```
            name: enable-healthcheck


            label: Enable HealthCheck?


            type: boolean


            default: true
```

以下は、リストのすべての属性と、以前のセクションで説明した値を定義する例です。

```
      -
            name: features-list


            type: string[]


            min-length: 1


            max-length: 3


            min-items: 1


            max-items: 3
```

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

```
            pattern: "\[A-Z\]+"

            allowed-values:

              - SP

              - LB

              - CS

            default:

              - LB
```

### 「レイアウト」

この属性は、`gui`属性のサブ属性です。この属性を使用して、リスト値をラジオボタンとして表示します。StyleBook定義のパラメータセクションで、`layout`属性を`radio`に設定します。これは、`allowed-values`属性を持つパラメータに適用されます。設定パックを作成すると、NetScaler Console GUIは`allowed-values`リストの値をラジオボタンとして表示します。

例:

```
-

    gui:

        layout: radio
```

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

```
allowed-values:
    - One
    - Two
    - Three
```

One、Two、Threeの値は、NetScaler Console GUIにラジオボタンとして表示されます。

### 「依存パラメータ」

この属性は、`gui`属性のサブ属性です。これは、別のパラメータで指定された値に基づいて、StyleBook設定フォームでのパラメータの表示または初期値を動的に制御します。

この属性は、フォーム上のパラメータの動作を制御するソースパラメータに指定します。他のパラメータを制御する複数の条件を含めることができます。たとえば、ソースパラメータ`protocol`は、`protocol`パラメータの値が`SSL`の場合にのみ表示される従属パラメータ`certificate`を持つことができます。

各条件には、次の属性を含めることができます。

- **target-parameter**: この条件が適用されるターゲットパラメータを指定します。
- **matching-values**: アクションをトリガーするソースパラメータの値のリストを指定します。
- **action**: ターゲットパラメータに対して、次のいずれかのアクションを指定します。
  - `read-only`: パラメータは読み取り専用になります。
  - `show`: パラメータが非表示の場合、フォームに表示されます。
  - `hide`: パラメータはフォームから削除されます。
  - `set-value`: パラメータ値は、value属性で指定された値に設定されます。
- **value**: アクションが`set-value`の場合のターゲットパラメータの値。

ユーザー入力がソースパラメータで指定された値と一致すると、ターゲットパラメータの表示または値が指定されたアクションに従って変更されます。

**例:**

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

```
-

   name: lb-virtual-port

   label: "Load Balanced App Virtual Port"

   description: "TCP port representing the Load Balanced application"

   type: tcp-port

   gui:

     updatable: false

     dependent-parameters:

           -

             matching-values:

               - 80

             target-parameter: $parameters.lb-service-type

             action: set-value

             allowed-values:

             - HTTP

             - TCP

             - UDP


   default: 80
```

この例では、依存パラメータは`lb-virtual-port`パラメータ（ソースパラメータ）の下に指定されています。

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

ソースパラメータの値が`80`に設定されると、`lb-service-type`パラメータが`set-value`アクションをトリガーします。その結果、ユーザーは以下のいずれかのオプションを選択できます。

- HTTP
- TCP
- UDP

## Parameters-default-sources コンストラクト

このコンストラクトを使用して、他のStyleBookからパラメータ定義を再利用できます。

パラメータまたはパラメータのグループが複数のStyleBookで繰り返し使用されるシナリオを考えてみましょう。新しいStyleBookを作成するたびにこれらのパラメータを再定義するのを避けるため、一度定義し、**parameters-default-sources** コンストラクトを使用して、これらのパラメータを必要とするStyleBookにその定義をインポートできます。

例えば、多くのStyleBookで仮想IPを設定する必要がある場合、作成する新しいStyleBookごとに仮想IPに関連する同じパラメータを定義しなければならないかもしれません。その代わりに、例えば「vip-params」という別のStyleBookを作成し、次の例に示すように、そこに関連するすべてのパラメータを定義できます。

```
-

name: vip-params

namespace: com.acme.commontypes

version: "1.0"

description: This StyleBook defines a typical virtual IP config.

private: true

schema-version: "1.0"

parameters:

  -

      name: lb-appname

      label: Load Balanced Application Name
```

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

```
          description: Name of the Load Balanced application
           type: string
           required: true
       -
           name: lb-virtual-ip
           label: Load Balanced App Virtual IP address
           description: Virtual IP address representing the Load Balanced
application
           type: ipaddress
           required: true
       -
           name: lb-virtual-port
           label: Load Balanced App Virtual Port
           description: TCP port representing the Load Balanced
application
           type: tcp-port
           default: 80
       -
           name: lb-service-type
           label: Load Balanced App Protocol
           description: Protocol used for the Load Balanced application.
           type: string
           default: HTTP
```

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

```
            required: true

            allowed-values:

                 - HTTP

                 - SSL

                 - TCP
```

その後、これらのパラメータを利用する他のStyleBookを作成できます。そのようなStyleBookの例を次に示します。

```
     -

     name: acme-biz-app

     namespace: com.acme.stylebooks

     version: "1.0"

     description: This stylebook defines the NetScaler configuration for
Biz App

     schema-version: "1.0"

     import-stylebooks:

       -

          namespace: com.acme.commontypes

          prefix: cmtypes

          version: "1.0"

     parameters-default-sources:

           - cmtypes::vip-params

     parameters:
```

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

```
        -
          name: monitorname
          label: Monitor Name
          description: Name of the monitor
          type: string
          required: true
        -
          name: type
          label: Monitor Type
          description: Type of the monitor
          type: string
          required: true
          allowed-values:
            - PING
            - TCP
            - HTTP
            - HTTP-ECV
            - TCP-ECV
            - HTTP-INLINE
```

StyleBook「acme-biz-app」では、まず「import-stylebooks」セクションを使用してvip-params StyleBookの名前空間とバージョンがインポートされます。次に、**parameters-default-sources** コ

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

ンストラクトが追加され、StyleBook名、つまりvip-paramsが指定されます。これは、vip-params StyleBookのパラメータをこのStyleBookに直接定義するのと同じ効果があります。

parameters-default-sourcesはリストであり、リスト内の各項目はStyleBookであると想定されているため、複数のStyleBookからパラメータを含めることができます。

他のStyleBookからパラメータを含めることに加えて、parametersセクションを使用して独自のパラメータを定義することもできます。StyleBookのパラメータの完全なリストは、他のStyleBookから含まれるパラメータとこのStyleBookで定義されるパラメータの組み合わせです。したがって、式 **$parameters** はこのパラメータの組み合わせを指します。

なお、パラメータがインポートされたStyleBookと現在のStyleBookの両方で定義されている場合、現在のStyleBookの定義が、他のStyleBookからインポートされた定義を上書きします。必要に応じてインポートされたパラメータの一部をカスタマイズすることで、残りのインポートされたパラメータはそのまま使用しながら、これを効果的に使用できます。

parameters-default-sources コンストラクトは、示すようにネストされたパラメータでも使用できます。

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true

      parameters-default-sources:

              - cmtypes::vip-params
```

これは、StyleBook vip-paramsのパラメータが、このStyleBookのvip-detailsパラメータの子パラメータとして直接追加されるのと似ています。

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

## パラメータソースコンストラクト

`parameters-source` コンストラクトを使用すると、設定パックの作成時にインポートされたパラメータがGUIにどのように表示されるかを制御できます。このコンストラクトを説明するStyleBookの例を次に示します。

```
parameters:

  -

    name: appname

    label: "LBVserver Name"

    description: "Name of the Load Balancer"

    type: string

    required: true

  -

   parameters-source: stlb::lb

  -

    name: vip-ipaddress

    label: "Load Balancer IP Address"

    description: "IP Address of the Load Balancer VIP"

    type: ipaddress

    required: true
```

この例では、`parameters-source` コンストラクトは `parameters` セクションに追加されます。`parameters-source` には、`parameters-default-sources` セクションのリスト項目に相当する値が含まれています。`parameters-source` を使用すると、異なるStyleBookからパラメータを目的の位置にインポートし、GUIにレンダリングできます。一方、`parameters-default-sources` セクションは属性をインポートし、GUIの先頭にのみレンダリングします。

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

## パラメータ条件

パラメータ条件は、StyleBook定義内の一部のパラメータの動作を変更するために使用されます。StyleBook定義内のパラメータは、設定パックを作成するために提供される入力です。定義内でパラメータ条件を定義するには、`parameters-conditions`を使用します。

StyleBook定義では、パラメータに多くの制約を設定できます。パラメータ条件は、ユーザーがパラメータの動作を変更したときに競合を解決するために使用されます。たとえば、ユーザーがSSLプロトコルを選択した場合、設定パックを作成するには証明書の詳細が必要です。ただし、証明書の詳細は最初、必須フィールドとして設定されていない場合があります。

パラメータ条件には、次の属性があります。

- `target`: アクションを適用するターゲットパラメータを指定します。複数のターゲットパラメータを指定できます。
- `action`: ターゲットパラメータに対して実行するアクションを指定します。パラメータ条件は、次のアクションをサポートしています。
  - 許可される値を増やす
  - パラメータの表示または非表示
  - デフォルト値を設定する
  - 必須フィールドとして設定する
  - 許可される値を設定する
  - パラメータのラベルを設定する
  - パラメータの説明を設定する
  - パラメータペインの折りたたみまたは展開
  - パラメータのパターンを設定する
- `condition`: オプション。指定されたターゲットパラメーターにアクションを適用する条件を指定します。条件を指定しない場合、アクションはターゲットパラメーターに直接適用されます。
- `value`: アクションに応じて、ターゲットパラメーター属性の値を設定します。

**注:**

現在、リストオブジェクト内のパラメーターには、パラメーター条件を適用できません。

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

### 'オーグメント・アロード・バリュー'

アクションが`augment-allowed-values`の場合、ターゲットパラメーターはGUIにドロップダウンメニューとして表示されます。ドロップダウンメニューには、StyleBook定義の`value`属性で定義された値が設定されます。

**例:**

```
parameters-conditions:

  -

   target: $parameters.rewritepolicy.action

   action: augment-allowed-values

   value:  $parameters.rewriteaction
```

### 'show' または 'hide'

アクションが`show`で、指定された条件が`True`を返す場合、ターゲットパラメーターはGUIに表示されます。

アクションが`hide`で、指定された条件が`True`を返す場合、ターゲットパラメーターはGUIから非表示になります。

**例:**

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: show

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初、`security-settings`パラメーターの証明書詳細は非表示になっています。ユーザーがSSLまたはSSL-Bridgeプロトコルを選択すると、証明書詳細が表示されます。

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

### 'セット・デフォルト'

アクションが `set-default` で、指定された条件が `True` を返す場合、ターゲットパラメーターの値はデフォルト値に設定されます。

**例 1:**

```
parameters-conditions:

  -

   target: $parameters.port

   action: set-default

   condition: $parameters.protocol == "SSL"

   value: 443

  -

   target: $parameters.port

   action: set-default

   condition: $parameters.protocol != "SSL"

   value: 80
```

**例 2**:

```
parameters-conditions:

  -

   target: $parameters.port

   action: set-default

   value: if-then-else($parameters.protocol == "SSL", 443, 80)
```

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

ユーザーが**SSL**プロトコルを選択すると、デフォルトのポート値は`443`に設定されます。その他のプロトコルの場合、デフォルトのポート値は`80`に設定されます。例 1 と 2 は同じ結果になります。

### 'セットリクワイアード'

アクションが`set-required`で、指定された条件が`True`を返すと、ターゲットパラメータは設定パックを作成するための必須フィールドになります。

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: set-required

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初は、`security-settings`パラメータに証明書の詳細が必要ない場合があります。ユーザーが**SSL**または**SSL-Bridge**プロトコルを選択すると、証明書の詳細は、設定パックを作成するための必須フィールドになります。

### 'セットアロードバリュー'

アクションが`set-allowed-values`で、指定された条件が`True`を返すと、ターゲットパラメータでは、指定された値のみを選択できます。

**例**:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-allowed-values

   value:

    - "SSL"
```

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

```
   condition: $parameters.lb-virtual-port ==  443
```

ユーザーがロードバランサーの仮想ポートとして`443`を指定すると、アプリケーション名では**SSL**オプションのみが許可されます。

### 'セットラベル'

アクションが`set-label`で、指定された条件が`True`を返すと、ターゲットパラメータのラベルは指定されたテキストに変更されます。

**例**:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-label

   value: if-then-else($parameters.lb-service-type == "TCP",
"TCPApp","UDPApp")
```

ユーザーがロードバランサープロトコルとして**TCP**を選択すると、アプリケーションのラベルは**TCPApp**に変更されます。ユーザーが別のオプションを選択した場合、アプリケーションのラベルは**UDPApp**に変更されます。

### 'セットディスクリプション'

アクションが`set-description`で、指定された条件が`True`を返すと、ターゲットパラメータの説明は指定されたテキストに変更されます。この説明は、ターゲットパラメータのツールチップに表示されます。

**例**:

```
parameters-conditions:

  -

   target: $parameters.app-name
```

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

```
   action: set-description

   value: if-then-else($parameters.lb-service-type == "TCP", "Select a TCP
application name","Select a UDP application name")
```

ユーザーがロードバランサープロトコルとして **TCP** を選択すると、アプリケーションのツールチップに `Select a TCP application name` と表示されます。ユーザーが別のオプションを選択した場合、アプリケーションの説明に `Select a UDP application name` と表示されます。

### 'コラプス・ペイン' または 'エクスパンド・ペイン'

アクションが `collapse-pane` で、指定された条件が `True` を返す場合、GUI でターゲットパラメータのペインが折りたたまれます。

アクションが `expand-pane` で、指定された条件が `True` を返す場合、GUI でターゲットパラメータのペインが展開されます。

**例**:

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details

    action: expand-pane

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初は、`security-settings` パラメータの証明書詳細ペインは展開されていない場合があります。ユーザーが **SSL** または **SSL-Bridge** プロトコルを選択すると、証明書詳細ペインが GUI 上で展開されます。

### 'セット・パターン'

アクションが `set-pattern` で、指定された条件が `True` を返す場合、ターゲットパラメータフィールドは指定されたパターンに設定されます。

**例**:

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

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-pattern

    value: "[a-z]+"
```

この例では、アプリケーション名には小文字の英字のみが許可されます。

### ネストされたパラメータ条件

StyleBook 定義では、パラメータ条件内にパラメータ条件を指定できます。これらの条件はネストされたパラメータ条件と呼ばれ、これらの条件を定義するために繰り返しコンストラクトを使用します。ネストされたパラメータ条件は、あるパラメータから別のパラメータに対してアクションを適用したい場合に役立ちます。

**例**:

```
parameters-conditions:

  -

    repeat: $parameters.lbvservers

    repeat-item: lbvserver

    parameters-conditions:

      -

        target: $lbvserver.port

        action: set-allowed-values

        condition: $lbvserver.protocol == "HTTPS"

        value: $parameters.ssl-ports
```

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

この例では、ユーザーがロードバランシング仮想サーバーの HTTPS プロトコルを選択すると、ポート値が動的に入力されます。そして、リスト内の各ロードバランシング仮想サーバーに適用されます。

## 置換

置換は、StyleBook内の複雑な式を置き換えることができる短縮名を定義するために使用され、StyleBookの可読性を高めます。

置換は、StyleBook内で同じ式や値（例えば定数値）が繰り返し使用される場合にも役立ちます。パラメーターに置換名を使用すると、StyleBook内のパラメーターのすべての出現箇所を更新する代わりに、置換値のみを更新できるため、エラーが発生しにくくなります。

置換は、値間のマッピングを定義するためにも使用されます。

リスト内の各置換は、キーと値で構成されます。値は、単純な値、式、関数、またはマップにすることができます。

以下の例では、2つの置換が定義されています。最初の置換は`http-port`で、8181の短縮形として使用できます。置換を使用することで、StyleBookの残りの部分で8181の代わりに**$substitutions.http-port**としてこれを参照できます。

**置換**:

```
http-port: 8181
```

ポート番号にニーモニック名を指定し、StyleBook内の1箇所でこのポート番号を定義できます。使用回数に関係なく、ポート番号を8080に変更したい場合は、置換セクションで変更でき、ニーモニック名`http-port`が使用されているすべての箇所に変更が適用されます。

以下の例は、コンポーネントで置換がどのように使用されるかを示しています。

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"
```

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

```
          servicetype: HTTP

          ipv46: $parameters.ip

          port: **$substitutions.http-port**

          lbmethod: $parameters.lb-alg
```

置換は複雑な式にすることもできます。以下の例は、2つの置換が式を使用する方法を示しています。

```
substitutions:

  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS

  app-name: str("acme-") + $parameters.name + str("-app")
```

置換式は、以下の例に示すように、既存の置換式を使用することもできます。

```
substitutions:

  http-port: 8181

  app-name: str("acme-") + $parameters.name + str($substitutions.http-
port) + str("-app")
```

置換のもう1つの便利な機能はマップです。マップでは、キーを値にマッピングできます。以下はマップ置換の例です。

```
substitutions:

    secure-port:

        true: int("443")

        false: int("80")

    secure-protocol:

        true: SSL
```

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

```
        false: HTTP
```

以下の例は、secure-portとsecure-protocolのマップを使用する方法を示しています。

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: $substitutions.secure-protocol[$parameters.is-
secure]

          ipv46: $parameters.ip

          port: $substitutions.secure-port[$parameters.is-secure]

          lbmethod: $parameters.lb-alg
```

これは、StyleBookのユーザーがis-secureパラメーターにブール値「true」を指定するか、NetScaler Console GUIでこのパラメーターに対応するチェックボックスを選択した場合、このコンポーネントの`servicetype`プロパティに**SSL**が割り当てられ、`port`プロパティに**443**が割り当てられることを意味します。ただし、ユーザーがこのパラメーターに「false」を指定するか、NetScaler Console GUIで対応するチェックボックスをオフにした場合、`servicetype`には**HTTP**が割り当てられ、ポートには**80**が割り当てられます。

次の例は、置換を関数として使用する方法を示しています。置換関数は1つ以上の引数を取ることができます。引数は、文字列、数値、IPアドレス、ブール値などの単純な型にすることができます。

**置換**:

form-lb-name(name): $name + "-lb"

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

この例では、「form-lb-name」という置換関数が定義されており、「name」という文字列引数を受け取り、**** その「name」引数の文字列に「-lb」を付加する文字列を作成します。この置換関数を使用する式は次のように記述されます。

`$substitutions.form-lb-name("my")`

これは `my-lb` を返します。

別の例を考えてみましょう。

**置換**:

cspol-priority(priority): 10100 - 100 * $priority

置換 `cspol-priority` は、「priority」という引数を受け取り、それを使用して値を計算する関数です。StyleBookの残りの部分では、この置換は次のように示されます。

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:

         name: $parameters.csvserver-name

         policyname: $components.cspolicy-comp.properties.policyname

         priority: $substitutions.cspol-
priority($parameters.pool.priority)
```

置換は、キーと値で構成することもできます。値は、単純な値、式、関数、マップ、リスト、または辞書にすることができます。

次に示すのは、値がリストである `slist` という置換の例です。

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

```
substitutions:

  slist:

    - a

    - b

    - c
```

置換の値は、以下の `sdict` という置換の例に見られるように、キーと値のペアの辞書にすることもできます。

```
substitutions:

  sdict:

    a: 1

    b: 2

    c: 3
```

リストと辞書を組み合わせることで、より複雑な属性を作成できます。たとえば、`slistofdict` という置換は、キーと値のペアのリストを返します。

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port

      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
```

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

しかし、次の例では、置換 `sdictoflist` はキーと値のペアを返しますが、その値自体が別のリストになっています。

```
sdictoflist:
  a:
    - 1
    - 2
  b:
    - 3
    - 4
```

コンポーネントでは、これらの置換は、条件、プロパティ、繰り返し、および繰り返し条件の構成で使用できます。

コンポーネントの以下の例は、置換を使用してプロパティを指定する方法を示しています。

```
  properties:
    a: $substitutions.slist
    b: $substitutions.sdict
    c: $substitutions.slistofdict
    d: $substitutions.sdictoflist
```

値がリストまたは辞書である置換を定義するユースケースは、コンテンツスイッチング仮想サーバーと複数のロードバランシング仮想サーバーを構成する場合です。同じコンテンツスイッチング仮想サーバーに紐付けられたすべてのロードバランシング仮想サーバーが同一の構成を持つ可能性があるため、置換リストと辞書を使用して構成を構築し、すべてのロードバランシング仮想サーバーで同じ構成を繰り返すことを避けます。

次の例は、コンテンツスイッチング仮想サーバー構成を作成するための `cs-lb-mon` StyleBooks の置換とコンポーネントを示しています。`cs-lb-mon` StyleBooks のプロパティを構築する際、複雑な置換「lb-properties」は、コンテンツスイッチング仮想サーバーに関連付けられたロードバ

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

ランシング仮想サーバーのプロパティを指定します。「lb-properties」置換は、名前、サービスタイプ、仮想IPアドレス、ポート、およびサーバーをパラメータとして受け取り、値としてキーと値のペアを生成する関数です。`cs-pools` コンポーネントでは、この置換の値を各プールの `lb-pool` パラメータに割り当てることができます。

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
```

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

```
  -

    name: cs-pools

    type: stlb::cs-lb-mon

    description: | Updates the cs-lb-mon configuration with the different
pools provided. Each pool with rule result in a dummy LB vserver, cs
action, cs policy, and csvserver_cspolicy_binding configuration.

    condition: $parameters.server-pools

    repeat: $parameters.server-pools

    repeat-item: pool

    repeat-condition: $pool.rule

    repeat-index: ndx

    properties:

      appname: $parameters.appname + "-cs"

      cs-virtual-ip: $parameters.vip

      cs-virtual-port: $substitutions.cs-port($parameters.protocol ==
"HTTP")

      cs-service-type: $parameters.protocol

      pools:

        -

          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP",
"0.0.0.0", 0, $pool.servers)

          rule: $pool.rule

          priority: $ndx + 1
```

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

### 置換マップ

キーを値にマッピングする置換を作成できます。たとえば、各プロトコル（キー）に使用するデフォルトポート（値）を定義したいシナリオを考えてみましょう。このタスクには、次のように置換マップを記述します。

```
substitutions:

     port:

          HTTP: 80

          DNS: 53

          SSL: 443
```

この例では、HTTP は 80 に、DNS は 53 に、SSL は 443 にマッピングされています。パラメータとして与えられた特定のプロトコルのポートを取得するには、次の式を使用します。

$substitutions.port\[$parameters.protocol\]

この式は、ユーザーが指定したプロトコルに基づいて値を返します。

- キーが HTTP の場合、式は 80 を返します。
- キーが DNS の場合、式は 53 を返します。
- キーが SSL の場合、式は 443 を返します。
- キーがマップに存在しない場合、式は値を返しません。

### 置換リストを反復処理する

次の例では、StyleBook は `apps` と呼ばれる置換リストを反復処理して、一連の `lbvserver` コンポーネントと、それに対応するサービスグループおよびバインドされたサーバーを作成します。

```
substitutions:

  apps:

    -

      name: lb1

      vip: 1.2.3.4
```

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

```
      vport: 80
      protocol: HTTP
      servers:
        -
          ip: 10.8.11.11
          port: 8080
        -
          ip: 10.8.11.12
          port: 8080
    -
      name: lb2
      vip: 1.2.3.5
      vport: 81
      protocol: HTTP
      servers:
        -
          ip: 10.9.11.28
          port: 8080
        -
          ip: 10.9.11.29
          port: 8181
components:
```

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

```
-
  name: lbvserver-comp
  type: ns::lbvserver
  repeat: $substitutions.apps
  repeat-item: app
  properties:
    name: $app["name"]
    ipv46: $app["vip"]
    port: $app["vport"]
    servicetype: $app["protocol"]
  components:
    -
      name: servicegroup-comp
      type: ns::servicegroup
      properties:
        servicegroupname: $parent.properties.name + "-svg"
        servicetype: HTTP
      components:
        -
          name: servers-comp
          type: ns::server
          repeat: $app["servers"]
```

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

```
            repeat-item: server

            properties:

              name: $server["ip"]

              ipaddress: $server["ip"]

            components:

              -

                name: servicegroup-servicegroupmember-binding-comp

                type: ns::servicegroup_servicegroupmember_binding

                properties:

                  servicegroupname:
$parent.parent.properties.servicegroupname

                  servername: $parent.properties.name

                  port: $server["port"]
```

## コンポーネント

StyleBookのComponentsコンストラクトは、StyleBookの中で最も重要なセクションと見なされます。このセクションでは、作成する必要がある構成オブジェクトを定義します。このコンストラクトを使用すると、同じタイプの構成オブジェクトを1つまたは複数作成できます。

componentsコンストラクトは、parametersセクションで提供される入力を使用して、StyleBookによって生成される構成を調整できます。これはオプションのセクションですが、ほとんどのStyleBookにはcomponentsセクションがあります。

次の表は、コンポーネントの主な属性について説明しています。

| 属性 | 説明 |
| --- | --- |
| 名前 | コンポーネントの名前。英数字の名前を指定できます。名前はアルファベットで始まり、追加のアルファベット、数字、ハイフン（-）、 |

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

| 属性 | 説明 |
| --- | --- |
| | またはアンダースコア（_）を含めることができます。 |
| 説明 | StyleBookにおけるこのコンポーネントの役割の説明。 |
| タイプ | タイプは、このコンポーネントが提供するプロパティを決定します。コンポーネントには2種類のタイプがあります。**組み込みタイプ**: このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITROエンティティタイプ「lbvserver」や「servicegroup」などです。コンポーネントに組み込みタイプ属性がある場合、NetScaler上にそのタイプの構成オブジェクトを作成します。たとえば、コンポーネントが組み込みタイプ「lbvserver」を参照する場合、このコンポーネントは、構成のターゲットであるNetScalerインスタンス上にロードバランシング仮想サーバーを作成します。**複合タイプ**: このタイプは、NetScaler Consoleに作成およびインポートした既存のStyleBookを参照します。コンポーネントに複合タイプ属性がある場合、参照されるStyleBookで指定されたすべての構成オブジェクトを、構成のターゲットであるNetScalerインスタンス上に作成します。これにより、複数のStyleBookを組み合わせることができ、各StyleBookが最終構成の一部を作成します。複合StyleBookの詳細については、「複合StyleBookの作成」を参照してください。 |
| プロパティ | コンポーネントタイプ属性に使用できるサブ属性。コンポーネントに有効なプロパティは、そのタイプによって決定されます。組み込みタイプの場合、これらは対応するNitroオブジェクトのプロパティまたは属性です。タイプが別のStyleBookであるコンポーネント、つまり複合タイプの場合、プロパティはそのStyleBookで定義されたパラメーターに対応します。 |

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

**例**:

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
```

この例では、my-lbvserver-comp というコンポーネントを定義しました。このコンポーネントは ns::lbvserver 型（組み込み型）です。「ns」は、import-stylebooks セクションで指定したネームスペース netscaler.nitro.config とバージョン 10.5 を参照するプレフィックスであり、「lbvserver」はこのネームスペース内の NITRO リソースです。

このセクションのプロパティには、「lbvserver」リソースの必須属性が4つとオプション属性が1つ（lbmethod）含まれており、これらの属性の値を指定できます。この例では、servicetype と port には静的な値を指定し、name、ipv46、lbmethod のプロパティは入力パラメータから値を取得します。パラメータセクションで定義されたパラメータ名は、$parameters.\<name\> の表記を使用して参照します（例: $parameters.ip）。

**注**

NITRO リソースタイプ（そのコンポーネントプロパティ）の属性名には小文字を使用する必要があります。そうしないと、StyleBook のインポートは失敗します。

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

## ヘルパーコンポーネント

StyleBookのコンポーネントセクションの主な用途は、Nitroの組み込みタイプまたは実際の構成オブジェクトを作成する別のStyleBookを介して構成オブジェクトを生成することです。ヘルパーコンポーネントは、それ自体で構成オブジェクトを構築しません。ヘルパーコンポーネントは、パラメーターオブジェクト、他のコンポーネントのプロパティ、または他のコンポーネントの出力などの他のセクションからの入力を受け取り、それらを別の形式に変換します。これは、後で他のコンポーネントによって実際の構成オブジェクトを生成するために使用できます。ヘルパーコンポーネントには、オブジェクトタイプ、またはコンポーネントセクションを含まない別のStyleBookの2種類があります。

次の例は、NetScalerインスタンスでモニター (lb-mon-comp) を使用してロードバランシングサーバーを作成するために使用されるStyleBookの抜粋を示しています。

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress


components:
  -
```

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

```
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
-
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
```

パラメーターセクションでは、アプリケーションの名前とロードバランシングサーバーのIPアドレスを入力できます。lb-mon-compコンポーネントセクションでは、lb-mon StyleBookのsvc-serversパラメーターは、各項目にipとportの2つのサブパラメーターを持つオブジェクトのリストを想定しています。

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

しかし、このStyleBookのパラメーターセクションは、$parameters.ipsを介してサーバーIPのみを受け入れます。StyleBookは、すべてのサーバーがポート80で実行されていると想定しています。lb-mon StyleBookを使用してロードバランシング構成を作成するには、$parameters.ipsをオブジェクトのリストに変換する必要があります。これは、上記の例のヘルパーコンポーネントであるhelp-compを使用して実現されます。help-compコンポーネントはserver-ip-port-params StyleBookタイプです。このStyleBookにはコンポーネントがありません。その結果、構成オブジェクトは作成されません。help-compは、$parameters.ipsに対して繰り返しリストを作成し、$parameters.ipsの各項目に対してipとport（静的な80に設定されています）で構成されるオブジェクトを構築します。したがって、help-compはIPアドレスのリストを、後でlb-mon-compでsvc-serversプロパティを割り当てるために使用できるオブジェクトのリストに変換します。help-compの結果は、lb-mon-compのsvc-serversプロパティに割り当てられます。

## オプションのプロパティ

場合によっては、コンポーネントのプロパティは式から値を取得します。この式は、パラメータ参照のような単純な式である場合もあれば、より複雑な式である場合もあります。このプロパティ値の設定は、コンポーネントではオプションです。式が実際の値を返す場合にのみプロパティ値を設定することを選択でき、それ以外の場合はこのプロパティを設定しないことを選択できます。

例えば、設定したいプロパティの1つが、タイプがns::lbvserverであるコンポーネントのlbmethod (ロードバランシングアルゴリズム) であるとします。プロパティlbmethodの値は、以下に示すように、ユーザーが提供するパラメータ値から取得されます。

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
```

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

```
        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
```

ここで、パラメータ **lb-advanced.algorithm** がオプションのパラメータであるとします。そして、ユーザーがオプションであるためこのパラメータに値を提供しない場合、式 **$parameters.lb-advanced.algorithm** は空白値に評価されます。したがって、lbmethodプロパティには無効な値が渡されます。このような状況を避けるために、プロパティ名に「?」を付けて、プロパティをオプションとして注釈付けできます。以下に示します。

```
components
   -
     name: lbvserver_comp
     type: ns::lbvserver
     properties:
       name: $parameters.lb-appname + "-lb"
       servicetype: $parameters.lb-service-type
       ipv46: $parameters.lb-virtual-ip
       port: 80
       lbmethod?: $parameters.lb-advanced.algorithm
```

「?」を使用すると、右側の式が何も評価されない場合にプロパティが省略されます。これは、この場合、次のように定義されたコンポーネントと同等になります。

```
components
  -
```

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

```
    name: lbvserver_comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb-appname + "-lb"

      servicetype: $parameters.lb-service-type

      ipv46: $parameters.lb-virtual-ip

      port: 80
```

**lbmethod** はオプションであるため、これを省略しても有効なコンポーネントになります。lbmethodは、そのタイプ「ns::lbvserver」でデフォルト値が定義されている場合、そのデフォルト値を取る可能性があることに注意してください。

## プロパティーズ・デフォルト・ソース 構成要素

properties-default-sources 構成要素は、parameters-default-sources 構成要素に類似しています。parameters-default-sources 構成要素が（他のStyleBookからの）既存のパラメーターをStyleBook内で再利用できるようにするのに対し、properties-default-sources 構成要素は、既存のソースに基づいてコンポーネントのプロパティを指定することを可能にします。

コンポーネントのプロパティは、StyleBookのさまざまなセクションに分散している場合があります。例えば、プロパティはオブジェクトパラメーター、オブジェクトを返す置換、他のコンポーネントのプロパティ、または他のコンポーネントの出力から取得される場合があります。そのような場合、コンポーネントの定義において、StyleBookの他のセクションに存在するプロパティを再定義する必要があります。明らかに、これは冗長であり、エラーにつながる可能性があります。この問題に対処するために、properties-default-sources 構成要素を使用できます。properties-default-sources 構成要素は、各項目がコンポーネントのいくつかのプロパティのソースを識別するリストです。

例えば、lbvserver構成を作成するコンポーネントを考えてみましょう。このコンポーネントは、lbvserverのプロパティを次のように定義する必要があります。

```
parameters:

  -
```

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

```
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
```

上記の例では、コンポーネントセクションで定義されているすべてのプロパティの値が$parameters.lbオブジェクトから取得されていることに注目してください。それらは単一のソースから取得されていますが、プロパティはStyleBookで再度定義されています。さらに、$parameters.lbオブジェクトにlbvserverの構成に関連する新しいサブパラメーターが追加された場合、新しいサブパラメーターに対応する新しいプロパティを追加するためにlb-compコンポーネントを更新する必要があります。

プロパティの再定義を避け、プロパティセクションに明示的にリストすることなくコンポーネントのすべての関連プロパティを取得するために、properties-default-sources 構成要素を使用できます。上記の例は次のように記述できます。

```
parameters:
  -
    name: lb
```

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

```
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
```

上記の例では、properties-default-sources 構成要素を使用することで、コンポーネント定義のサイズが削減され、コンポーネントを簡潔に定義できるようになります。さらに、コンポーネントのプロパティのソースが変更されるたびに、その変更は自動的に反映されます。例えば、「persistencetype」という新しいプロパティが$parameters.lbオブジェクトに追加された場合、persistencetypeはlbvserverのプロパティであるため、このプロパティはデフォルトでlb-compの構成に追加されます。したがって、properties-default-sources 構成要素は、コンポーネントのプロパティのソースで発生する変更を心配することなく、コンポーネントを定義するための動的なインターフェースを提供します。

### コンポーネントのプロパティの計算

このセクションでは、properties-default-sources 構成要素がコンポーネントで使用された場合に、プロパティがどのように取得されるかについて説明します。まず、StyleBooksコンパイラは、そのタイプ（上記の例ではlbvserver）に基づいてコンポーネントのプロパティのリストを識別します。次に、コンパイラは、定義されている順序（コンポーネントのproperties-default-sourcesセクション）で、複数のソースからこれらのプロパティを取得します。複数のソースにプロパティが存在する場合、最後のソースに現れるプロパティが他のプロパティよりも優先されます。最後に、properties-default-sources 構成要素を使用して取得されたプロパティは、コンポーネントのプロパティセクションで上書きできます。コンポーネントセクションの定義には、少なくともproperties-default-sourcesセクションまたはpropertiesセクションのいずれかを含める必要があることに注意することが重要です。両方を含めることもできます。

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

## ネストされたコンポーネント

別のコンポーネント内にコンポーネントをネストすると、ネストされたコンポーネントは、親コンポーネントによって作成された構成オブジェクトまたはコンテキストを参照して、独自の構成オブジェクトを作成できます。ネストされたコンポーネントは、親コンポーネントで作成された各オブジェクトに対して1つ以上のオブジェクトを作成できます。別のコンポーネント内にコンポーネントをネストしても、作成された構成オブジェクト間に何らかの関係があることを示すものではありません。ネストは、親コンポーネントの既存のコンテキスト内で構成オブジェクトを構築するというコンポーネントのタスクを容易にする方法です。

**例**:

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
```

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

```
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
        components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                name: $parent.parent.properties.name
                servicegroupname: $parent.properties.name
                  -
                    name: members-svcg-comp
                    type: ns::servicegroup_servicegroupmember_binding
                    repeat:
                      repeat-list: $parameters.svc-servers
                      repeat-item: srv
                    properties:
                      ip: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
```

この例では、多段階のネストが使用されています。コンポーネント my-lbvserver-comp には、my-svcg-comp という子コンポーネントがあります。そして、my-svcg-comp コンポーネントには、その中に2つの子コンポーネントがあります。my-svcg-comp コンポーネントは、組み込みの NITRO リソースタイプ "servicegroup" の属性に値を提供することで、NetScaler インスタンス上にサービ

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

スグループ構成オブジェクトを作成するために使用されます。my-svcg コンポーネントの最初の子コンポーネントである lbvserver-svg-binding-comp は、その親コンポーネントによって作成されたサービスグループを、親の親コンポーネントによって作成された負荷分散仮想サーバー (lbvserver) にバインドするために使用されます。$parent 表記（親参照とも呼ばれます）は、親コンポーネント内のエンティティを参照するために使用されます。2番目の子コンポーネントである members-svcg-comp は、サービスのリストを親コンポーネントによって作成されたサービスグループにバインドするために使用されます。このバインディングは、StyleBook の繰り返しコンストラクトを使用して、パラメータ svc-servers に指定されたサービスのリストを反復処理することで実現されます。繰り返しコンストラクトの詳細については、「繰り返しコンストラクト」を参照してください。

コンポーネントのネストを使用せずに、同じ構成オブジェクトを作成することもできます。詳細と例については、「基本的な負荷分散構成を作成するためのStyleBook」を参照してください。

## 条件コンストラクト

条件コンストラクトを使用することで、コンポーネントを条件付きにすることができます。条件コンストラクトの値は、trueまたはfalseに評価されるブール式です。条件がtrueの場合、そのコンポーネントは設定オブジェクトを構築するために使用されます。条件がfalseの場合、そのコンポーネントはスキップされ、それを通じて設定オブジェクトは作成されません。ブール式は、多くの場合、パラメータ値に基づいています。

**例**:

```
components:

      -

        name: servicegroup-comp

        type: ns::servicegroup

        condition: $parameters.svc-server-ips

        properties:

              name: $parameters.name + "-svcgrp"

              servicetype: HTTP
```

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

この例では、ユーザーがオプションパラメータsvc-server-ipsに値を指定した場合、コンポーネントservicegroup-compはStyleBookエンジンによって処理されます。条件がfalseの場合、つまり、ユーザーがこのパラメータに値を指定せず、このパラメータにnull値が割り当てられてfalseと評価される場合、StyleBookエンジンはこのコンポーネントの存在を無視し、サービスグループは作成されません。

ブール式は、StyleBookでサポートされている任意の有効な式に基づいていることに注意してください（例えば、別のコンポーネントが存在するかどうか、またはパラメータが特定の値を持つかどうかなど）。

次の例では、条件がtrueと評価された場合、NITROタイプns::systemfileの設定オブジェクトを構築します。

**例**:

```
     components

          -

            name: pem_key_files

            type: ns::systemfile

            condition: "$components.der-certificate-files-comp or
$components.pem-certificate-files-comp"

            properties:

                  filecontent: $certificate.keyfile.contents

                  fileencoding: "BASE64"

                  filelocation: "/nsconfig/ssl"

                  filename: $certificate.keyfile.filename
```

この例では、条件は複雑な「OR」式であり、StyleBook内の他の2つのコンポーネントが処理されている（スキップされていない）場合にのみ、この設定オブジェクトをStyleBookによって作成したいと考えています。そのため、コンポーネント間に依存関係が作成されます。

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

## 繰り返し構成要素

コンポーネントの**repeat**構成要素を使用して、同じ種類の複数の構成オブジェクトを作成できます。

次の例では、**members-svcg-comp**コンポーネントを使用して、親コンポーネントによって作成されたサービスグループにサービスのリストをバインドします。各サーバーをサービスグループにバインドする構成オブジェクトを作成するには、**repeat**構成要素を使用して、パラメータ**svc-servers**に指定されたサービスのリストを反復処理します。この反復処理中に、コンポーネントはサービスグループ内の各サービス（**repeat-item**構成要素では**srv**として参照されます）に対して**servicegroup_servicegroupmember_binding**タイプのNITROオブジェクトを作成し、各NITROオブジェクトの**ip**属性を対応するサービスのIPアドレスに設定します。

**例**:

```
components:

  -

      name: my-lbvserver-comp

      type: ns::lbvserver

      properties:

           name: $parameters.name + "-lb"

           servicetype: HTTP

           ipv46: $parameters.ip

           port: 80

           lbmethod: $parameters.lb-alg

          components:

               -

                  name: my-svcg-comp

                  type: ns::servicegroup
```

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

```
                properties:
                     name: $parameters.name + "-svcgrp"
                     servicetype: HTTP
               components:
                      -
                      name: lbvserver-svg-binding-comp
                      type: ns::lbvserver\servicegroup\binding
                      properties:
                            name: $parent.parent.properties.name
                            servicegroupname: $parent.properties.name
                      -
                      name: members-svcg-comp
                      type: ns::servicegroup\servicegroupmember\binding
                      repeat:
                        repeat-list: $parameters.svc-servers
                        repeat-item: srv
                      properties:
                             ip: $srv
                             port: $parameters.svc-port
                             servicegroupname: $parent.properties.name
```

**repeat**はそれ自体がオブジェクトであり、**repeat-list**と**repeat-item**はrepeatオブジェクトの属性です。

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

- repeat-listは、コンポーネントが反復処理するリストを識別する必須属性です。
- repeat-itemはオプションであり、反復処理中の現在の項目にわかりやすい名前を付けるために使用されます。

指定されていない場合、現在の項目には式**$repeat-item**を使用してアクセスできます。上記の例の最後のコンポーネントは、次のように記述することもできます。

```
        -

        name: members-svcg-comp

        type: ns::servicegroup_servicegroupmember_binding

        repeat:

          repeat-list: $parameters.svc-servers

        properties:

               ip: $repeat-item

               port: $parameters.svc-port

               servicegroupname: $parent.properties.name
```

リストを反復処理中に現在の項目を参照できることに加えて、**repeat-index**を使用してリスト内の項目の現在のインデックスを参照することも可能です。次の例では、**repeat-index**を使用して現在のインデックスに基づいてポート番号を計算します。

```
           name: services

           type: ns::service

           repeat:

              repeat-list: $parameters.app-services

              repeat-item: srv

           properties:
```

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

```
            ip: $parameters.app-ip

            port: $parameters.base-port + repeat-index

            servicegroupname: $parent.properties.name
```

**repeat-item**構成要素と同様に、反復処理の現在のインデックスを参照するために別の変数名を割り当てることができます。前の例は次の例と同等です。

```
    -

        name: services

        type: ns::service

        repeat:

           repeat-list: $parameters.app-services

           repeat-item: srv

           repeat-index: idx

        properties:

            ip: $parameters.app-ip

            port: $parameters.base-port + $idx

            servicegroupname: $parent.properties.name
```

## リピート条件構文

リピート条件構文は、リピート構文の各イテレーションで評価され、その結果によって、そのイテレーションで構成オブジェクトを構築するか、次のイテレーションに進むかが決定されます。次の例は、リピート条件構文の使用法を示しています。

**例**:

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

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

         filecontent: base64($certificate.keyfile.contents)

         fileencoding: BASE64

         filelocation: /nsconfig/ssl

         filename: $certificate.keyfile.file
```

この例では、der-key-files-comp コンポーネントは、ユーザーによって指定されたすべての証明書を反復処理しますが、DERエンコーディングを持つ証明書に対応する構成オブジェクトのみを構築します。各イテレーションで、リピート条件式が評価され、証明書のエンコーディングがDERタイプであるかどうかがテストされます。DERタイプでない場合、現在のイテレーションでは構成オブジェクトは構築されず、イテレーションはリスト内の次の証明書に進みます。

## ネストされた繰り返し

ネストされた繰り返し構造を使用すると、コンポーネントの定義に応じて、各コンポーネントに複数の繰り返し構造を持たせることができます。2レベルのネストされた繰り返しを考えてみましょう。外部リスト (最初の繰り返しリスト) の各要素に対して、内部リスト (2番目の繰り返しリスト) のすべての要素の繰り返しリストを作成できます。StyleBookコンパイラは、最大3つのネストされた繰り返しをサポートしています。各繰り返しレベルには、repeat-item属性とrepeat-index

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

属性が関連付けられています。repeat-item属性とrepeat-index属性の両方はオプションです。さらに、各繰り返しはrepeat-conditionも指定できます。

**例**:

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
  -
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
         repeat-list: $parameters.vips
         repeat-item: ip
         repeat:
              repeat-list: $parameters.vip-ports
              repeat-item: port
      properties:
```

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

```
        name: str("lb-") + str($ip) + '-' + str($port)

        servicetype: HTTP

        ipv46: $ip

        port: $port
```

上記の例では、$parameters.vips内の各項目に対して、$parameters.vip-portsのすべての項目を反復処理します。したがって、$parameters.vipsで指定された各IPアドレスに対して、$parameters.vip-portsで指定されたすべてのポートのlbvserver構成オブジェクトを作成します。プロパティセクションは、IPアドレスとポートの組み合わせに対して「lb」をプレフィックスとしてオブジェクトの名前を定義します。そのため、各反復処理で、$ip + $portはIPアドレスとポート番号の一意の組み合わせを定義します。

repeat-item属性が指定されていない場合、コンパイラはそれに対してデフォルト値を生成します。repeat-itemのデフォルト値は、各繰り返しレベルに対してそれぞれ$repeat-item、$repeat-item-1、$repeat-item-2です。同様に、repeat-index属性が指定されていない場合、コンパイラはそれに対してデフォルト値を生成します。repeat-indexのデフォルト値は、各繰り返しレベルに対してそれぞれ$repeat-index、$repeat-index-1、および$repeat-index-2です。

次の例は、ネストされた繰り返しオブジェクトにrepeat-item属性とrepeat-index属性がない場合の命名規則について説明しています。

**例**:

```
components:

-

     name: lbvservers-comp

     type: ns::lbvserver

     repeat:

         repeat-list: $parameters.vips

         repeat:
```

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

```
            repeat-list: $parameters.vip-ports
    properties:
       name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)
       servicetype: HTTP
       ipv46: $repeat-item
       port: $repeat-item-1
```

## 出力

出力セクションでは、StyleBookがすべての構成オブジェクトの作成を正常に完了した後、ユーザーに公開する内容を指定します。StyleBookの出力セクションはオプションです。StyleBookが出力を返す必要はありません。ただし、一部の内部コンポーネントを出力として返すことで、複合StyleBookを作成する際に確認できるように、それをインポートするStyleBookにより高い柔軟性をもたらします。

次の表は、出力セクションで使用される属性について説明しています。

| 属性 | 説明 | 必須 |
|---|---|---|
| 名前 | 公開したい構成オブジェクトに対応する出力の名前。 | はい |
| 説明 | 出力を説明するテキスト文字列。 | いいえ |
| 値 | この属性は、StyleBookによって返される値を抽出する方法を指定します。 | はい |

**例：**

```
outputs:
 -
```

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

```
    name: lbvserver

    description: LBVServer component

    value: $components.my-lbvserver-comp

  -

    name: svc-grp

      description: ServiceGroup name

      value: $components.my-svcg.properties.name
```

この例では、StyleBookによって作成される**lbvserver**コンポーネントとサービスグループの**名前**を公開します。**lbvserver**という名前の出力の値は、**my-lbvserver-comp**コンポーネントです。同様に、**svc-grp**という名前の出力の値は、**my-svcg**コンポーネントによって作成されるサービスグループの名前です。

## パラメータリファレンス

コンポーネントの構成では、パラメータセクションで定義されたパラメータを `$parameters.<parametername>` 表記を使用して参照します。`<parametername>` 自体がパラメータを含む場合（タイプがオブジェクトの場合）、`$parameters.<parametername>.<sub-parametername>` の表記を使用する必要があります。以下同様です。

**例**:

```
parameters:

  -

    name: name

    label: Name

    type: string

    required: true

     -
```

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

```
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
```

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

```
      name: $parameters.name

      servicetype: HTTP

      ipv46: $parameters.vip.ip

      port: $parameters.vip.port
```

## 親参照

ネストされたコンポーネントを使用している場合、$parent表記を使用して親コンポーネントを参照できます。親コンポーネントがrepeatコンストラクトを使用して複数の構成オブジェクトを構築し、各イテレーション内で子コンポーネントが他の構成オブジェクトを構築する場合、$parent表記は常に親コンポーネントの現在のイテレーションを参照します。たとえば、$parent.properties.nameは、親によって現在のイテレーションで構築された構成オブジェクトのnameプロパティを参照します。

**例**:

```
components:

 -

   name: my-lbvserver-comp

   type: ns::lbvserver

   properties:

     name: $parameters.name + "-lb"

     servicetype: HTTP

     ipv46: $parameters.ip

     port: 80

     lbmethod: $parameters.lb-alg

     components:
```

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

```
    -
      name: my-svcg-comp
      type: ns::servicegroup
      properties:
        name: $parameters.name + "-svcgrp"
        servicetype: HTTP
        components:
         -
           name: lbvserver-svg-binding-comp
           type: ns::lbvserver_servicegroup_binding
           properties:
              name: $parent.parent.properties.name
              servicegroupname: $parent.properties.name
                -
                  name: members-svcg-comp
                  type: ns::servicegroup_servicegroupmember_binding
                  repeat: $parameters.svc-servers
                  repeat-item: srv
                  properties:
                    ip: $srv
                    port: str($parameters.svc-port)
```

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

```
                    servicegroupname: $parent.properties.name
```

最上位コンポーネントまで、親の親のプロパティにアクセスすることで、コンポーネントの階層を上位に移動することもできます。たとえば、コンポーネント**lbvserver-svg-binding-comp**のプロパティ名は、**$parent.parent**表記を使用することで、その親の親である**my-lbvserver-comp**コンポーネントのプロパティ名から値を取得します。

## コンポーネントリファレンス

コンポーネント構成では、**$components.\<componentname\>** 表記を使用してStyleBook内のトップレベルコンポーネントを参照します。トップレベルコンポーネント内にネストされたコンポーネントがある場合、それらを参照するために使用される表記は**$components.\<componentname\>.components.\<component-name\>** となり、以下同様です。

**例**:

```
components:

 -

    name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

           name: $parameters.name + "-lb"

           servicetype: HTTP

           ipv46: $parameters.ip

           port: 80

           lbmethod: $parameters.lb-alg

  -

     name: my-svcg-comp

     type: ns::servicegroup
```

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

```
    properties:

         name: $parameters.name + "-svcgrp"

         servicetype: HTTP

-

    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv

    properties:

       ip: $srv

         port: str($parameters.svc-port)

         servicegroupname: $components.my-svcg-comp.properties.name

-

    name: lbvserver-svg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    properties:

           name: $components.my-lbvserver-comp.properties.name

           servicegroupname: $components.my-svcg-comp.properties.name
```

この例では、最後のコンポーネント**lbvserver-svg-binding-comp**を構築する前に、コンポーネント**my-svcg-comp**と**my-lbvserver-comp**を構築する必要があります。これは、この最後のコンポーネントにこれらのコンポーネントへの参照があるためです。これらの参照は、**$components.\<componentname\>**で示されるコンポーネント参照を使用して提供されます。

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

## 置換リファレンス

コンポーネントセクションまたはオペレーションセクションでは、置換セクションで定義された置換を `$substitutions.<substitution-name>` 表記を使用して参照します。例: **$substitutions.http-port**。

置換がマップである場合、マップ内の要素を `$substitutions.<substitutions-name>[<map-key>]` として参照できます。例: `$substitutions.protocol-map[$parameters.port]`。

## 変数参照

コンポーネントでrepeatおよびrepeat-itemコンストラクトを使用して複数の構成オブジェクトを構築する場合、repeat-itemコンストラクトに変数名を割り当てることができます。この変数は、そのコンポーネントのプロパティまたは子コンポーネントで、** `$\<varname\>` **という表記を使用して参照できます。なお、コンポーネントでrepeatコンストラクトがrepeat-itemコンストラクトなしで使用される場合、$repeat-itemというデフォルト変数を使用して反復項目にアクセスできます。

**例**:

```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names

    repeat: $parameters.svc-server-domain-names

    repeat-item: server-name

    properties:

      name: $server-name + "-server"

      domain: $server-name

    components:

      -
```

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

```
        name: service-members-comp

        type: ns::service

        properties:

          name: $server-name + "-service"

          servername: $parent.properties.name

          servicetype: $parameters.svc-service-type

          port: $parameters.svc-server-port
```

上記の例では、server-nameという変数名がrepeat-itemコンストラクトに割り当てられています。この変数名は、同じコンポーネントのプロパティおよび子コンポーネント**`$\<varname\>`**で参照されます。

## 操作

操作はStyleBookのオプションセクションです。このセクションでは、NetScaler Consoleアナリティクスを設定して、すべてのトラフィックトランザクションまたは一部のトラフィックトランザクションでAppFlowレコードを収集できます。StyleBookを使用してNetScalerインスタンス上に作成された仮想サーバーが、これらのトラフィックトランザクションを処理します。このセクションでは、仮想サーバーで特定のトラフィック条件が満たされたときにアラームをトリガーするようにNetScaler Consoleを設定することもできます。

StyleBookを介してNetScaler Consoleを設定し、以下に示すさまざまなNetScaler Console Insightsからトラフィック統計を収集できます。

- ウェブインサイト
- WAFセキュリティ違反
- HDX™ インサイト
- NetScaler Gateway インサイト。

サポートされている仮想サーバーは、負荷分散、コンテンツスイッチング、およびVPN仮想サーバーです。

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

負荷分散またはコンテンツスイッチング仮想サーバーでのアナリティクス用に、Web InsightとWAFセキュリティ違反の両方、またはそのいずれかを有効にします。ただし、VPN仮想サーバーの場合は、HDX InsightとNetScaler Gateway Insightの両方、またはそのいずれかを有効にする必要があります。

StyleBookを介してNetScalerインスタンスで有効になっているNetScaler Console Insightは、IPFIXプロトコル（AppFlow）を使用して、インスタンスからNetScalerにデータを送信します。

また、Web Insightを有効にすると、負荷分散仮想サーバーとコンテンツスイッチング仮想サーバーでクライアント側測定が有効になります。クライアント側測定が有効になっている場合、NetScaler ConsoleはHTMLインジェクションを介してHTMLページのロード時間とレンダリング時間のメトリックをキャプチャします。これらのメトリックを使用して、管理者はL7遅延の問題を特定できます。

**例1**:

次の例は、VPN仮想サーバーでHDX InsightとNetScaler Gateway Insightの両方を有効にするために、StyleBookでoperationsセクションを記述する方法を示しています。

```
name: simple-vpn-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable hdxinsight and gatewayinsight on a
VPN vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns
```

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

```
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                 type: hdxinsight**
                  -
                    type: gatewayinsight
outputs:
```

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

```
  -

    name: myvpns

    value: $components.vpnvserver-comp
```

**例2**:

次の例は、負荷分散仮想サーバーでWeb InsightとWAFセキュリティ違反の両方を有効にするために、StyleBookでoperationsセクションを記述する方法を示しています。

```
name: simple-lb-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable webinsight and securityinsight on LB
vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

components:

    -

        name: lbvserver-comp

        type: ns::lbvserver
```

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

```
        properties:

            name: str("lb-") + str($current-target.ip)

            servicetype: HTTP

            ipv46: 1.1.21.37

            port: 80

operations:

    analytics:

        -

            name: comp-ops

            properties:

                target: $components.lbvserver-comp

                filter: "true"

                 insights:

                 -

                  type: webinsight

                    -

                  type: securityinsight

outputs:

  -

    name: mylbs

    value: $components.lbvserver-comp
```

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

## アナリティクス

アナリティクスセクションの各要素は、StyleBooksで作成された1つまたは複数の仮想サーバーに対して、NetScaler Consoleのアナリティクス機能を構成するために使用されます。

アナリティクスセクションの要素には、次の属性があります。

| 属性 | 説明 | 必須 |
| --- | --- | --- |
| 名前 | アナリティクス要素の名前。 | はい |
| 説明 | この要素が何であるかを説明するテキスト文字列。 | いいえ |
| 条件 | ブール式。この条件がfalseと評価された場合、アナリティクス要素全体がスキップされます。 | いいえ |
| 繰り返し | リストを反復処理します。 | いいえ |
| 繰り返し条件 | ブール式。式がfalseと評価された場合、現在の反復はスキップされます。 | いいえ |
| 繰り返し項目 | 現在の反復における項目の名前。 | いいえ |
| 繰り返しインデックス | 現在の反復におけるインデックス値の名前。 | いいえ |
| プロパティ | 分析操作プロパティのリスト。 | はい |
| ターゲット | リスト内のプロパティの1つ。ターゲット式は、NetScalerで構成された仮想サーバーの名前であり、その仮想サーバーの分析が収集されます。 | はい |
| フィルター | リスト内のプロパティの1つ。この属性の値は、分析が収集される仮想サーバー上の | いいえ |

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

| 属性 | 説明 | 必須 |
| --- | --- | --- |
| | リクエストをフィルタリングするために使用されるNetScalerの高度なポリシー式です。デフォルトでは、仮想サーバーを通過するすべてのトラフィックで分析データが収集されます。 | |
| インサイト | リスト内のプロパティの1つ。この属性の値は、ターゲット仮想サーバーから収集されるインサイトデータのタイプです。デフォルトでは、ターゲット仮想サーバーとインサイトタイプで指定されている仮想サーバータイプに基づいて、許可されているすべてのインサイトがターゲット仮想サーバーに構成されます。 | いいえ |
| トランスポートモード | リスト内のプロパティの1つ。この属性の値は`logstream`または`ipfix`です。`logstream`がデフォルト値です。 | いいえ |
| クライアント側測定 | リスト内のプロパティの1つ。この属性の値はENABLEDまたはDISABLEDです。DISABLEDがデフォルト値です。 | いいえ |
| HTTP-X-フォワード・フォー | リスト内のプロパティの1つ。この属性の値はENABLEDまたはDISABLEDです。この属性は、クライアントIP情報をバックエンドサーバーに渡すためのX-Forwarded-Forヘッダーの挿入を有効または無効にしま | いいえ |

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

| 属性 | 説明 | 必須 |
| --- | --- | --- |
| | す。DISABLEDがデフォルト値です。 | |
| HDX Insight の有効化 | リスト内のプロパティの1つ。この属性の値はICAまたはTCPです。この属性は、特定のトラフィックデータに対して`hdxinsight`を有効にします。ICAがデフォルト値です。 | いいえ |

**例1**: 単一の仮想サーバーの分析を構成する

```
operations:


  analytics:
    -
    name: lbvserver-ops-comp
    properties:
        target: $components-basic-lb-comp.outputs.lbvserver-name
        filter: HTTP.REQ.URL.CONTAINS("catalog")
        transport-mode: logstream
        client-side-measurements: ENABLED
        insights:
          -
            type: webinsight
          -
```

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

```
            type: securityinsight
```

**例2**: VPN仮想サーバーのリストの分析を構成する

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

         http-x-forwarded-for: ENABLED

        insights:

          -

            type: hdxinsight

            enable-hdxinsight-for: TCP
```

分析セクションの各属性は、ターゲットプロパティによって識別される仮想サーバー上でAppFlowレコードを収集するようにNetScalerインスタンスを構成します。

### ターゲット仮想サーバーとインサイトタイプ

ターゲット仮想サーバーと、それに対応する許可されるインサイトタイプは次のとおりです。

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

| ターゲット仮想サーバー | インサイトタイプ |
| --- | --- |
| LB仮想サーバー | ウェブインサイト、セキュリティインサイト、ボットインサイト |
| csvサーバー | ウェブインサイト、セキュリティインサイト、ボットインサイト |
| VPNサーバー | HDXインサイト、ゲートウェイインサイト |

**注:**

IPFIX は、StyleBooks で仮想サーバーの分析を設定するために使用されるデフォルトの転送モードです。

## アラーム

オペレーションセクションのアラームサブセクションは、アナリティクスサブセクションと同様の構造と属性を持っています。唯一の違いは、プロパティ属性にあります。すべての属性（プロパティ属性を除く）のリストについては、アナリティクスを参照してください。

アラームサブセクションで利用可能なプロパティは次のとおりです。

| 属性 | 説明 | 必須 |
| --- | --- | --- |
| ターゲット | NetScalerで構成され、アラームが設定されている仮想サーバーの名前に評価される式。 | はい |
| メールプロファイル | NetScaler Console Analytics機能で定義され、アラームがトリガーされたときに通知したいメールアドレスのリストを含むメールプロファイルの名前。 | いいえ (email-profileまたはsms-profileのいずれかを定義する必要があります) |
| SMSプロファイル | NetScaler Console Analytics機能で定義され、アラームがトリガーされたときに通知し | いいえ (email-profileまたはsms-profileのいずれかを定義する必要があります) |

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

| 属性 | 説明 | 必須 |
| --- | --- | --- |
| | たい電話番号のリストを含むSMSプロファイルの名前。 | |
| ルール | ターゲットプロパティで定義された仮想サーバーのアラームをトリガーする条件を定義するルールのリスト。 | はい |
| メトリック | ルールの属性。NetScaler仮想サーバーに関連して追跡したいメトリックの名前。 | はい |
| 演算子 | ルールの属性。メトリックを値と比較するために使用する演算子。有効な演算子は「greaterthan」と「lessthan」です。 | はい |
| 値 | ルールの属性。演算子を使用してメトリックと比較されるしきい値。メトリック値がこのしきい値を超えると、関連するアラームがトリガーされます。 | はい |
| 期間単位 | ルールの属性。アラームルールが満たされた場合にユーザーに警告する頻度。これには、日、時間、または週の値を含めることができます。これは、ルールが満たされた場合、アラームが期間単位で1回送信されることを意味します（例：1日1回）。 | はい |

以下の表は、NetScaler仮想サーバーに関連して追跡されるメトリックのリストを示します。

カウンター|説明|詳細な説明|NetScaler Consoleの計算

| | | | |
| --- | --- | --- | --- |
| VPN仮想サーバーの場合： | | | |

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

| | | | |
|---|---|---|---|
| app_count | VPNアプリ起動数 | ユーザーが指定した時間間隔中に起動された、このVPN仮想サーバー上のユニークなVPNアプリケーションの総数。 | 新しいアプリケーションが起動されるたびに増加する単調増加カウンター |
| app_launch_duration | VPNアプリ起動時間 | アプリケーションの起動にかかる平均時間（ミリ秒） | このVPN仮想サーバーで起動されたすべてのVPNアプリケーションの起動時間から計算された平均値 |
| その他の仮想サーバー（CS、LB、Auth、GSLB） | | | |
| total_requests | リクエスト数 | この仮想サーバーでのクライアントリクエスト数。アプライアンスの最終再起動以降、または仮想サーバーの作成以降のいずれか新しい方。 | この仮想サーバーへの新しいリクエストごとに増加する単調増加カウンター。 |
| total_bytes | バイト | 指定された時間間隔で仮想サーバーからNetScaler Consoleに転送された合計バイト数。 | この仮想サーバーによって処理された合計バイト数をカウントするための単調増加カウンター。 |
| application_response_time | 応答時間 | 仮想サーバーの平均応答時間。 | この仮想サーバーが受信したすべてのリクエストの応答時間の平均値。アプライアンスの最後の再起動以降、または仮想サーバーの作成以降のいずれか遅い方。 |

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

StyleBookにおけるアラームセクションの例:

```
operations:

alarms:

 -

  name:lbvserver_alarm

  properties:

  target: $outputs.lbvserver

  email-profile: $parameters.emailprofile

  sms-profile: "NetScalerSMS"

     rules:

      -

        metric: "total_requests"

        operator: "greaterthan"

        value: 25

        period-unit: weekly

        -

          metric: "total_bytes"

          operator: "lessthan"

          value: 1024

          period-unit: day
```

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

## 式

StyleBookの最も強力な機能の1つは、式の使用です。動的な値を計算するために、さまざまなシナリオでStyleBook式を使用できます。次の例は、パラメーター値とリテラル文字列を連結する式です。

**例**:

```
$parameters.appname + "-mon"
```

この式は、`appname`という名前のパラメーターを取得し、それを文字列`-mon`と連結します。

以下の種類の式がサポートされています:

### 算術式

- 加算 (+)
- 減算 (-)
- 乗算 (*)
- 除算 (/)
- 剰余 (%)

**例**:

- 2つの数値を加算する: $parameters.a + $parameters.b
- 2つの数値を乗算する: $parameters.a * 10
- ある数値を別の数値で除算した後の剰余を求める:

`15%10` は `5` になります

### 文字列式

- 2つの文字列を連結する (+)

**例**:

2つの文字列を連結する: str("app-") + $parameters.appname

### リスト式

2つのリストを結合する (+)

**例**:

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

- 2つのリストを連結する: $parameters.external-servers + $parameters.internal-servers
- もし `$parameters.ports-1` が で、 `$parameters.port-2` が の場合、 `$parameters.ports-1 + $parameters.ports-2` はリスト として表示されます。

### 関係式

- **==** : 2つのオペランドが等しいかどうかをテストし、等しい場合はtrueを返し、そうでない場合はfalseを返します。
- **!=** : 2つのオペランドが異なるかどうかをテストし、異なる場合はtrueを返し、そうでない場合はfalseを返します。
- **\>** : 最初のオペランドが2番目のオペランドより大きい場合はtrueを返し、そうでない場合はfalseを返します。
- **\>=** : 最初のオペランドが2番目のオペランド以上である場合はtrueを返し、そうでない場合はfalseを返します。
- **\<** : 最初のオペランドが2番目のオペランドより小さい場合、trueを返します。それ以外の場合はfalseを返します。
- **\<=** : 最初のオペランドが2番目のオペランド以下の場合、trueを返します。それ以外の場合はfalseを返します。

**例**:

- 等価演算子の使用: `$parameters.name = = "abcd"`
- 不等価演算子の使用: `$parameters.name != "default"`
- その他の関係演算子の例
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

### 論理式 - ブール

- **and**: 論理「and」演算子。両方のオペランドがtrueの場合、結果はtrueになり、それ以外の場合はfalseになります。

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

- **or**: 論理「or」演算子。いずれかのオペランドがtrueの場合、結果はtrueになり、それ以外の場合はfalseになります。
- **not**: 単項演算子。オペランドがtrueの場合、結果はfalseになり、その逆も同様です。
- **in**: 最初の引数が2番目の引数の部分文字列であるかどうかをテストします。
- **in**: 項目がリストの一部であるかどうかをテストします。

**注**

文字列が数値に変換され、数値が文字列に変換される式を型キャストできます。同様に、`tcp-port` を数値にキャストでき、IPアドレスを文字列にキャストできます。

任意の演算子の前後に区切り文字を使用します。次の区切り文字を使用できます。

- 演算子の前: `space`、`tab`、`comma`、`(`、`)`、`[`、`]`
- 演算子の後: `space`、`tab`、`(`、`[`

例:

- `abc + def`
- `100 % 10`
- `10 > 9`

### 逐語的な文字列式

文字列内の特殊文字がリテラル形式を取る必要がある場合に、逐語的な文字列を使用できます。これらの文字列には、エスケープ文字、バックスラッシュ、引用符、括弧、空白、角括弧などが含まれます。逐語的な文字列では、特殊文字の通常の解釈はスキップされます。文字列内のすべての文字はリテラル形式で保持されます。

StyleBooksでは、NetScalerポリシー式を逐語的な文字列を使用してリテラル形式で含めることができます。ポリシー式には通常、特殊文字が含まれています。逐語的な文字列を使用しない場合、文字列を部分文字列に分割して特殊文字をエスケープする必要があります。

逐語的な文字列を作成するには、次のように特殊文字の間に文字列をカプセル化します。

```
~{string}~
```

逐語的な文字列は、StyleBookのどこでも使用できます。

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

**注**

このシーケンスは逐語的な文字列の終わりを示すため、入力文字列で文字シーケンス`}~`を使用しないでください。

例:

```
~{HTTP.REQ.COOKIE.VALUE("jsessionid") ALT
HTTP.REQ.URL.BEFORE_STR("=").AFTER_STR(";jsessionid=") ALT
HTTP.REQ.URL.AFTER_STR(";jsessionid=")}~
```

### ターゲット式

StyleBook定義では、現在のターゲットNetScalerインスタンスを参照するために`$current-target`式を使用できます。ターゲットNetScalerインスタンスのIPアドレスを具体的に参照するには、この式を次のように使用します。

```
$current-target.ip
```

例:

```
components:

 -

  name: lb-comp

  type: ns::lbvserver

  properties:

    name: $current-target.ip + "-lbvserver"
```

この例では、`lbvserver`の名前はターゲットNetScalerインスタンスのIPアドレスで構成されています。

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

### 式の型検証

StyleBookエンジンは、コンパイル時に強力な型チェックを可能にします。つまり、StyleBookの作成中に使用される式は、config packの作成時ではなく、StyleBook自体のインポート中に検証されます。

パラメータ、置換、コンポーネント、コンポーネントのプロパティ、コンポーネントの出力、ユーザー定義変数（repeat-item、repeat-index、置換関数の引数）などへのすべての参照は、その存在と型についてすべて検証されます。

**型チェックの例**:

次の例では、`lbvserver` StyleBookのポートプロパティの予期される型は`tcp-port`です。NetScaler Consoleでは、型検証はコンパイル時（インポート時）に行われます。コンパイラは、文字列と`tcp-port`が互換性のない型であると判断し、そのためStyleBookコンパイラはエラーを表示し、StyleBookのインポートまたは移行に失敗します。

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: str("80")

      servicetype: HTTP
```

このStyleBookを正常にコンパイルするには、コンパイラで以下を数値として宣言します。

`port: 80`

**無効な式のフラグ付けの例**:

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

以前のリリースでは、無効な式がプロパティ名に割り当てられても、コンパイラは無効な式を検出しなかったため、StyleBookをNetScaler Consoleにインポートすることができました。現在、このStyleBookがNetScaler Consoleにインポートされると、コンパイラはそのような無効な式を識別してフラグを付けます。その結果、StyleBookはNetScaler Consoleへのインポートに失敗します。

この例では、`lb-sg-binding-comp`コンポーネントのnameプロパティに割り当てられている式は`$components.lbvserver-comp.properties.lbvservername`です。しかし、`lbvserver-comp`コンポーネントには`lbvservername`というプロパティはありません。以前のNetScaler Consoleリリースでは、コンパイラはこの式を許可し、正常にインポートしていました。実際の失敗は、ユーザーがこのStyleBookを使用して設定パックを作成しようとしたときに発生していました。しかし現在では、このようなエラーはインポート時に識別され、StyleBookはNetScaler Consoleにインポートされません。このようなエラーを手動で修正し、StyleBookをインポートしてください。

```
Components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg
```

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

```
      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: $components.lbvserver-comp.properties.lbvservername

      servicegroupname: $components.sg-comp.properties.servicegroupname
```

### リストのインデックス付け

リストの項目は、直接インデックスを付けてアクセスできるようになりました。

| 式 | 説明 |
| --- | --- |
| `$components.test-lbs[0]` | test-lbsコンポーネントの最初の項目を参照します |
| `$components.test-lbs[0].properties.p1` | test-lbsコンポーネントの最初の項目のプロパティp1を参照します |
| `$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname` | `lbcomps`コンポーネントの最初の項目からの出力である、`servicegroups`コンポーネントの2番目の項目の`servicegroupname`プロパティを参照します |

## インプレース補間

StyleBook式を使用して文字列の一部を置き換えることが可能になりました。これらの文字列式がStyleBookコンパイラによって評価されると、StyleBook式を使用する文字列の部分は、その式の値に置き換えられます。文字列にStyleBook式を含めるには、次の表記法を使用します。

```
"...%{...}%..."
```

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

ここで、「%{」と「}%」で囲まれた文字はStyleBook式を形成します。これらの式は「インプレース補間」として知られています。

例えば、文字列「lb-%{$parameters.appname}%-svc」は、StyleBook式のインプレース補間を含む文字列式です。文字列式の値は、補間式の値に依存します。**$parameters.appname**に「app1」が割り当てられているとします。その場合、文字列式は**lb-app1-svc**と評価されます。これにより、値が文字列式にハードコードされるのではなく、ユーザー定義の値に基づいて評価されるようになります。

インプレース補間の実用的なユースケースは、StyleBookのポリシー式をパラメータ化することです。HTTP URLに特定の単語、例えば「jpeg」が含まれているかどうかをチェックするポリシー式を作成するシナリオを考えてみましょう。

このためには、次のようにポリシー式を記述します。「HTTP.REQ.URL.CONTAINS(\\"jpeg\\")」。

ここで、HTTP URL内のオブジェクトをパラメータ化したい場合、StyleBookに文字列パラメータ（例: $parameters.url-object）を追加できます。ポリシー式はこのパラメータに基づいて記述する必要があります。そのためには、文字列連結を使用して結果を実現します。式は次のようになります。

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
```

$parameter.url-objectに「csv」が割り当てられている場合、上記の式は「HTTP.REQ.URL.CONTAINS(\\"csv\\")」と評価されます。しかし、この式は読みにくいです。このパラメータ化を読みやすく理解しやすくするために、インプレース補間を使用できます。

インプレース補間を使用した式は次のとおりです。

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

上記の式では、$parameters.url-objectの値の周りに内部引用符を追加する補間式を使用しました。この式の結果は上記と同じですが、より直感的で実際の結果に近くなります。

### 補間内で許可される型

補間内で次の型の値を生成する式を使用できます: boolean、number、tcp-port、ipaddress、string。補間が結果に置き換えられると、生成された値は自動的に文字列に変換されます。

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

文字列式には、0個、1個、またはそれ以上の補間を含めることができます。順次補間では、文字列式の異なる部分を異なるStyleBook式で置き換えることができます。例えば、文字列 lb-%{$parameters.appname}%-%{$parameters.vip}% は、$parameters.appname が "app1" で $parameters.vip が "1.1.1.1" の場合、"lb-app1-1.1.1.1" を返します。

文字列式はネストされた補間もサポートしています。つまり、ある補間式を別の補間式の内部にネストして、一方の式の値がもう一方の式の入力となるようにすることができます。

例えば、文字列「%{lb-%{$parameters.port + 1}%}%」を考えてみましょう。

内部文字列「**%{$parameters.port + 1}%**」は、$parameters.port が 80 の場合、「lb-81」を返します。ここで、この式は別の補間式の中にネストされています。

次の表は、さまざまな種類の補間を例と対応する結果とともに示しています。例で使用されているパラメータの値は次のとおりです。

- $parameters.appname: 「lb1」
- $parameters.vip: 「1.1.1.1」
- $parameters.n1: 1
- $parameters.n2: 3

### 単純な補間

| 式 | 結果 |
| --- | --- |
| エルビー-%{$parameters.appname}%-デフ | エルビー-lb1-デフ |

### 自動型変換

| 式 | 結果 |
| --- | --- |
| lb-%{1}% | lb-1 |
| lb-%{$parameters.vip}% | lb-1.1.1.1 |
| lb-%{真}% | lb-真 |

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

### 連続補間

| 式 | 結果 |
| --- | --- |
| %{$parameters.appname}%-%{str($parameters.appname)}% | lb1-lb1 |
| lb-%{1}%-%{2}% | lb-1-2 |

### ネストされた補間

| 式 | 結果 |
| --- | --- |
| %{abc-%{$parameters.n1 + 1}%}% | abc-2 |
| str("%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%") | bc-1-3 |

### quotewrap を使用した補間

| 式 | 結果 |
| --- | --- |
| 文字列("%{引用符で囲む(abcd)}%")str("%{quotewrap(`https://`)}%`+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")` | "テキスト"<`https://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL` |

#### 補間におけるエスケープ文字

「%{" または "}%" の文字が文字列の一部である場合、StyleBookコンパイラがこれらを補間タグとして評価しないように、エスケープ文字として「`\`」を指定する必要があります。

**例**:

str("%{\%\{ + str($parameters.vip) + \}\%}%") は、$parameters.vip が 1.1.1.1 の場合、"%{1.1.1.1}%" を返します。

次の表は、いくつかの式とその結果を示しています。

| カテゴリ | 式 | 結果 |
| --- | --- | --- |
| 補間のエスケープ | str("%{str($parameters.n1) + }\%}%") | 1}% |

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

| カテゴリ | 式 | 結果 |
| --- | --- | --- |
| | ロードバランサー-%{str($parameters.n1) + }\%}% | lb-1}% |
| | "%{str($parameters.n1) + \"\}\%\"}%" | 1}% |

## 組み込み関数

組み込み関数は、StyleBook の式で使用されます。

たとえば、組み込み関数 `str()` を使用して、数値を文字列に変換できます。

```
str($parameters.order)
```

または、組み込み関数 `int()` を使用して、文字列を整数に変換できます。

```
int($parameters.priority)
```

以下は、StyleBook の式でサポートされている組み込み関数と、その使用方法の例です。

### 文字列()

`str()` 関数は、入力引数を文字列値に変換します。

許可される引数タイプ:

- `string`
- `number`
- `TCP-port`
- `boolean`
- `IP address`

**例**:

- `"set-" + str(10)` 関数は `"set-10"` を返します。
- `str(10)` 関数は `10` を返します。
- `str(1.1.1.1)` 関数は `1.1.1.1` を返します。
- `str(T rue)` 関数は `"T rue"` を返します。
- `str(ADM)` 関数は `"mas"` を返します。

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

### int() 関数

`int()` 関数は、文字列、数値、IPアドレス、または `tcpport` を引数として受け取り、整数を返します。

**例**:

- `int("10")` 関数は `10` を返します。
- `int(10)` 関数は `10` を返します。
- `int(ip('0.0.4.1'))` 関数は `1025` を返します。

### bool() 関数

`bool()` 関数は任意の型を引数として受け取ります。引数の値が `false`、空、または存在しない場合、この関数は `false` を返します。

それ以外の場合は、 `true` を返します。

**例**:

- `bool(true)` 関数は `true` を返します。
- `bool(false)` 関数は `false` を返します。
- `bool($parameters.a)` 関数は、 `$parameters.a` が `false`、空、または存在しない場合に `false` を返します。

### len() 関数

`len()` 関数は、文字列またはリストを引数として受け取り、文字列の文字数またはリストの項目数を返します。

**例 1**:

置換を次のように定義した場合:

```
items: ["123", "abc", "xyz"]
```

`len($substitutions.items)` 関数は `3` を返します

**例 2**:

`len("NetScaler Console")` 関数は `10` を返します。

**例 3**:

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

`$parameters.vips` に `['1.1.1.1', '1.1.1.2', '1.1.1.3']` の値がある場合、`len($parameters.vips)` 関数は `3` を返します。

### min() 関数

`min()` 関数は、引数として、リストまたは一連の数値、あるいは `tcp-ports` を受け取り、最小の項目を返します。

**一連の数値/TCPポートの例**:

- `min(80, 100, 1000)` 関数は `80` を返します。
- `min(-20, 100, 400)` 関数は `-20` を返します。
- `min(-80, -20, -10)` 関数は `-80` を返します。
- `min(0, 100, -400)` 関数は `-400` を返します。

**数値/TCPポートのリストの例**:

- サポート `$parameters.ports` は `tcp-ports` のリストであり、値は `[80, 81, 8080]` です。

  `min($parameters.ports)` 関数は `80` を返します。

### max() 関数

`max()` 関数は、引数として、リストまたは一連の数値、あるいは `tcp-ports` を受け取り、最大の項目を返します。

**一連の数値/TCPポートの例**:

- `max(80, 100, 1000)` 関数は `1000` を返します。
- `max(-20, 100, 400)` 関数は `400` を返します。
- `max(-80, -20, -10)` 関数は `-10` を返します。
- The `max(0, 100, -400)` 関数は `100` を返します。

**数値/TCPポートのリストの例**:

- サポート `$parameters.ports` は `tcp-ports` のリストであり、値は `[80, 81, 8080]` です。

  The `max($parameters.ports)` 関数は `8080` を返します。

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

### bin() 関数

The `bin()` 関数は数値を引数として受け取り、その数値をバイナリ形式で表す文字列を返します。

**式の例**:

The `bin(100)` 関数は `0b1100100` を返します。

### oct() 関数

The `oct()` 関数は数値を引数として受け取り、その数値を8進数形式で表す文字列を返します。

**式の例**:

The `oct(100)` 関数は `0144` を返します。

### hex() 関数

The `hex()` 関数は数値を引数として受け取り、その数値を16進数形式で表す小文字の文字列を返します。

**式の例**:

この `hex(100)` 関数は `0x64` を返します。

### ローワー()

`lower()` 関数は文字列を引数として受け取り、その文字列を小文字で返します。

**例**:

この `lower("ADM")` 関数は `adm` を返します。

### アッパー()

`upper()` 関数は文字列を引数として受け取り、その文字列を大文字で返します。

**例**:

この `upper("NetScaler Console")` 関数は `NetScaler Console` を返します。

### サム()

`sum()` 関数は数値のリストまたは `tcpports` を引数として受け取り、リスト内の数値の合計を返します。

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

**例 1**:

置換を次のように定義した場合: substitutions:

`list-of-numbers = [11, 22, 55]`

この `sum($substitutions.list-of-numbers)` 関数は `88` を返します。

**例 2**:

`$parameters.ports` が `[80, 81, 82]` の場合、`sum($parameters.ports)` 関数は `243` を返します。

### pow() 関数

`pow()` 関数は2つの数値を引数として受け取り、最初の引数を2番目の引数の累乗で表す数値を返します。

**例**:

`pow(3,2)` 関数は `9` を返します。

### ip()

`ip()` 関数は、整数、文字列、またはIPアドレスを引数として受け取り、入力値に基づいてIPアドレスを返します。

**例**:

- `ip` 関数でIPアドレスを指定します。

  `ip(3.1.1.1)` 関数は `3.1.1.1` を返します。
- `ip` 関数で文字列を指定します。

  `ip('2.1.1.1')` 関数は `2.1.1.1` を返します。
- `ip` 関数で整数を指定します。
  - `ip(12)` 関数は `0.0.0.12` を返します。
  - `ip` 関数で整数を文字列として指定すると、入力と同等のIPアドレスを返します。

    `ip('1025')` 関数は `0.0.4.1` を返します。

  この関数は、整数の加算および減算操作もサポートしており、結果のIPアドレスを返します。

  - 加算: `ip(1025) + ip(12)` 関数は `0.0.4.13` を返します。

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

- 減算: `ip('1025') - ip(12)` 関数は `0.0.3.245` を返します。
- 加算と減算の組み合わせ: `ip('1.1.1.1') + ip('1.1.1.1') – ip(2)` は `2.2.2.0` を返します。

### base64.encode()

`base64.encode()` 関数は文字列引数を受け取り、base64エンコードされた文字列を返します。

**例**:

`base64.encode("abcd")` 関数は `YWJjZA==` を返します。

### base64.decode()

`base64.decode` 関数はbase64エンコードされた文字列を引数として受け取り、デコードされた文字列を返します。

**例**:

`base64.decode("YWJjZA==")` 関数は `abcd` を返します。

### イグジスツ()

`exists()`関数は任意の型の引数を取り、ブール値を返します。入力に何らかの値がある場合、戻り値は `True` です。入力引数に値がない場合（つまり、値がない場合）、戻り値は `False` です。

`$parameters.monitor`がオプションのパラメーターであるとします。コンフィグパックの作成時にこのパラメーターに値を指定すると、`($parameters.monitor)`関数は `True`を返します。

それ以外の場合は、`False`を返します。

### フィルター()

`filter()`関数は2つの引数を取ります。

引数1：1つの引数を取り、ブール値を返す置換関数。

引数2：リスト。

この関数は、最初の 引数にある置換関数に渡されたときに、各要素が `True` と評価される元のリストのサブセットを返します。

**例**:

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

置換関数を次のように考えます。

置換:

```
x(a): $a != 81
```

この関数は、入力値が `81` と等しくない場合にTrueを返します。それ以外の場合は、`False` を返します。

仮に、`$parameters.ports` が `[81, 80, 81, 89]` であるとします。

`filter($substitutions.x, $parameters.ports)` は、リストから `81` のすべての出現を削除して `[80, 89]` を返します。

### if-then-else() 関数

関数 `if-then-else()` は3つの引数を取ります。

引数1：ブール式

引数2：任意の式

引数3：任意の式（オプション）

引数1の式が `True` と評価される場合、関数は引数2として提供された式の値を返します。

それ以外の場合、引数3が指定されている場合、関数は引数3の式の値を返します。

引数3が指定されていない場合、関数は `no` を返します。

**例1：**

`if-then-else($parameters.servicetype == HTTP, 80, 443)` 関数は、`$parameters.servicetype` が `HTTP` の値を持つ場合、`80` を返します。それ以外の場合、関数は `443` を返します。

**例2：**

`if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` 関数は、`$parameters.servicetype` が `HTTP` の値を持つ場合、`$parameters.hport` の値を返します。

それ以外の場合、関数は `$parameters.sport` の値を返します。

**例3：**

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

`if-then-else($parameters.servicetype == HTTP, 80)` は、`$parameters.servicetype` が `HTTP` の値を持つ場合、`80` を返します。

それ以外の場合、関数は値を返しません。

### join() 関数

`join()` 関数は2つの引数を取ります。

引数1: 数値、`tcp-ports`、文字列、またはIPアドレスのリスト

引数2: 区切り文字列 (オプション)

この関数は、引数1として提供されたリストの要素を文字列に結合します。各要素は引数2として提供された区切り文字列で区切られます。引数2が提供されない場合、リスト内の要素は1つの文字列として結合されます。

**例**:

- `$parameters.ports` は `[81, 82, 83]` です。
  - 区切り文字引数を使用する場合:

    `join($parameters.ports, '-')` 関数は `81-82-83` を返します。
  - 区切り文字引数を使用しない場合:

    `join($parameters.ports)` 関数は `818283` を返します。

### split()関数

`split()` 関数は、指定された区切り文字に応じて入力文字列を複数のリストに分割します。区切り文字が指定されていないか、空白 (`''`) の場合、この関数はスペースを区切り文字と見なし、文字列をリストに分割します。

**例:**

- `split('Example_string_split', 's')` 関数は `['Example_','tring_','plit']` を返します。
- `split('Example string split')` 関数は `['Example','string','split']` を返します。
- `split('Example string split', '')` 関数は `['Example','string','split']` を返します。
- `split('Example string')` 関数は `['Example','string']` を返します。

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

この関数は、連続するスペースを1つのスペースとして扱います。

### マップ()

`map()` 関数は2つの引数を取ります。

引数1：任意の関数

引数2：要素のリスト。

この関数は、リスト内の各要素が、`map()` 関数（引数1）を引数2の対応する要素に適用した結果であるリストを返します。

引数1で許可される関数：

- 1つの引数を取る組み込み関数：

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`

- 少なくとも1つの引数を取る置換関数。

**例：**

$parameters.nums が `[81, 82, 83]` であるとします。

- 組み込み関数 str を使用したマップ

  `map(str, $parameters.nums)` 関数は `["81", "82", "83"]` を返します

  マップ関数の結果は文字列のリストであり、各要素は入力リスト ($parameters.nums) の対応する要素に str 関数を適用することによって計算されます。

- 置換関数を使用したマップ

  - 置換:

    `add-10(port): $port + 10`

  - 式:

    `map($substitutions.add-10, $parameters.nums)` 関数は数値のリストを返します: `[ 91, 92, 93 ]`

このマップ関数の結果は数値のリストです。各要素は、入力リスト `($parameters.nums)` の対応する要素に置換関数 `$substitutions.add-10` を適用することによって計算されます。

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

### quotewrap() 関数

`quotewrap()` 関数は文字列を引数として受け取り、入力値の前後に二重引用符文字を追加した文字列を返します。

**例**:

`quotewrap("ADM")` 関数は `"mas"` を返します

### replace() 関数

`replace()` 関数は3つの引数を取ります。

引数1: 次の組み込み型の`string`またはリスト:

- `string`
- `number`
- `ipaddress`
- `tcp-port`
- `boolean`

引数2: 引数1で指定された型と一致する単一の値または値のリスト

引数3: 引数1で指定された型と同じ型の単一の値 (オプション)

`replace()` 関数は、引数1内の引数2のすべての出現箇所を引数3に置き換えます。

引数3が指定されていない場合、引数1から引数2のすべての出現箇所が削除されます。

**例**:

- `replace('abcdef', 'def', 'xyz')` 関数は `abcxyz` を返します。

  `def` のすべての出現箇所が `xyz` に置き換えられます。
- `replace('abcdefabc', 'def')` は `abcabc` を返します。

  引数3がないため、結果の文字列から`def`が削除されます。
- `replace('An#example@to%replace!characters', ['@', '#', '!', '%'], '_')`関数は `An_example_to_replace_characters`を返します。

  出力文字列には、`['@', '#', '!', '%']`で指定された文字の代わりにアンダースコア (_) があります。

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

- `replace([10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4], [10.10.10.2, 10.10.10.4])` 関数は `[10.10.10.1, 10.10.10.3]` を返します。

  引数3がないため、結果のIPアドレスリストから `10.10.10.2` と `10.10.10.4` が削除されます。

- `replace([8080, 8081, 8082, 8083, 8084], 8083, 80)` 関数は `[8080, 8081, 8082, 80, 8084]` を返します。

  `8083` のすべての出現箇所は `80` に置き換えられます。

### trim()関数

`trim()` 関数は、入力文字列から先頭と末尾の空白が削除された文字列を返します。

**例**:

`trim(' abc ')` 関数は `abc` を返します。

### truncate() 関数

`truncate()` 関数は2つの引数を取ります。

引数1: 文字列

引数2: 数値

この関数は、引数1の入力文字列が引数2で指定された長さに切り詰められた文字列を返します。

**例**:

`truncate('NetScaler Console', 6)` は `Citrix` を返します。

### distinct() 関数

`distinct()` 関数は、リスト入力から一意の項目を抽出します。

**例:** `$parameters.input_list` が `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']` の場合、`distinct($parameters.input_list)` 関数は `['ADM', 'ADC', 'VPX', 'CPX']` を返します。

### url.encode()

`url.encode()` 関数は、RFC 3986に従って文字がASCII文字セットを使用して変換された文字列を返します。

**例**:

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

`url.encode("a/b/c")`関数は`a%2Fb%2Fc`を返します。

### url.decode()

`url.decode()`関数は、RFC 3986に従ってURLエンコードされた引数が通常の文字列にデコードされた文字列を返します。

**例**:

`url.decode("a%2Fb%2Fc")`関数は`a/b/c`を返します。

### is-ipv4() 関数

The `is-ipv4()` 関数は IP アドレスを引数として受け取り、その IP アドレスが IPv4 形式である場合にブール値 `True` を返します。

The `is-ipv4(10.10.10.10)` 関数は `True` を返します

### is-ipv6() 関数

The `is-ipv6()` 関数は IP アドレスを引数として受け取り、その IP アドレスが IPv6 形式である場合にブール値 `True` を返します。

The `is-ipv6(2001:DB8::)` 関数は `True` を返します

### startswith() 関数

The `startswith()` 関数は、文字列が指定されたプレフィックスで始まるかどうかを判断します。この関数には、2つの必須文字列引数が必要です。

`startswith(str, sub_str)`

この関数は、文字列 ( `str` ) が部分文字列 ( `sub_str` ) で始まる場合に `True` を返します。

**例**：

- The `startswith('Citrix', 'Ci')` 関数は `True` を返します。
- The `startswith('Citrix', 'iC')` 関数は `False` を返します
- The `startswith('Citrix', 'Ab')` 関数は `False` を返します

### endswith() 関数

The `endswith()` 関数は、文字列が指定されたサフィックスで終わるかどうかを判断します。この関数には、2つの必須文字列引数が必要です。

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

`endswith(str, sub_str)`

この関数は、文字列 ( `str` ) が部分文字列 ( `sub_str` ) で終わる場合に `True` を返します。

**例**:

- `endswith('Citrix', 'ix')` 関数は `True` を返します。
- `endswith('Citrix', 'Ix')` 関数は `False` を返します。
- `endswith('Citrix', 'ab')` 関数は `False` を返します。

### contains() 関数

`contains()` 関数は、文字列が指定された部分文字列を含むかどうかを判断します。この関数には、2つの必須の文字列引数が必要です。

`contains(str, sub_str)`

この関数は、部分文字列 ( `sub_str` ) が文字列 ( `str` ) 内のどこかに含まれている場合に `True` を返します。

例:

- `contains('Citrix', 'tri')` 関数は `True` を返します。
- `contains('Citrix', 'Ci')` 関数は `True` を返します。
- `contains('Citrix', 'ti')` 関数は `False` を返します

### substring() 関数

`substring()`関数を使用して、文字列から部分文字列を抽出します。

`substring(str, start_index, end_index)`

この関数は、2つの必須引数と1つのオプションの整数引数を必要とします。

- `str` (必須)
- `start_index` (必須)
- `end_index` (オプション)

この関数は、指定されたインデックス位置の間にある文字列 ( `str` ) から部分文字列を返します。終了インデックス位置を指定しない場合、関数は開始インデックスから文字列の末尾まで部分文字列を抽出します。

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

**注**

`end_index`を指定すると、部分文字列は`end_index`位置の文字を除外します。

例:

- `substring('Citrix', 2)`関数は`trix`を返します
- `substring('Citrix', 10)`関数は ( `''` ) を返します

  この例では、無効な`start_index`位置があるため、関数は空の文字列を返します。
- `substring('Citrix', 2, 4)`関数は`tr`を返します

  この例では、関数は2番目と4番目のインデックス位置の間の文字を抽出します。
- 「`substring('Citrix', -3)`」関数は「`rix`」を返します。

  文字列の末尾にある文字を抽出したい場合は、`start_index`引数に負の値を指定します。

  この例では、関数は文字列の最後の3文字を含む部分文字列を抽出します。

### 複数()

「`multiple()`」関数は2つの引数を取ります。

引数1: `number`、`string`、`boolean`、`ipaddress`、`tcp-port`、または`password`

引数2: `number`

「`multiple(argument1, argument2)`」関数は、引数1の多くのコピーを含むリストを返します。コピーの数は、引数2に渡された数と等しくなります。

例:

- 「`multiple(10.10.10.10, 3)`」関数は「`[10.10.10.10, 10.10.10.10, 10.10.10.10]`」を返します。
- 「`multiple(8080, 4)`」関数は「`[8080, 8080, 8080, 8080]`」を返します。

### 反転()

reverse() 関数は、項目のリストを引数として受け取り、同じ項目を逆順に並べたリストを返します。

引数には、以下の組み込み型のリストを指定できます。

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

- `string`
- `number`
- `ipaddress`
- `ipnetwork`
- `tcp-port`
- `boolean`
- `password`
- `object`
- `file`
- `certfile`
- `keyfile`
- `certkey`

**例**:

- reverse() は を返します。
- reverse() は を返します。
- reverse() は を返します。

## 依存関係の検出

StyleBook内のコンポーネントは、同じStyleBook内の他のコンポーネントのプロパティまたはセクションを参照できます。コンポーネントはそれ自体で完結したブロックであり、実行される順序と同じ順序で記述されているとは限りません。StyleBookコンパイラは、コンポーネントが記述されている順序をチェックし、論理的な順序で実行します。

**例**:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:
```

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

```
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
```

上記の例では、**lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp** の3つのコンポーネントが定義されています。このStyleBookが実行されると、まずlbvserver-compが作成されます。lb-sg-binding-compはlbvserver-compのプロパティを参照しますが、StyleBookで2番目に定義されているコンポーネントであるにもかかわらず、次に作成することはできません。これは、lb-sg-binding-compがまだ作成されていないsg-compにも依存しているためです。その結果、コンパイラはコンポーネントが作成されるまでにそのコンポーネントの依存関係が解決されるようにコン

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

ポーネントを並べ替え、この並べ替えられたコンポーネントのリストを実行します。上記のStyleBookの実行順序は、lbvserver-comp、sg-comp、lb-sg-binding-compです。

したがって、StyleBookの作成者はコンポーネントの正しい順序について心配する必要はありません。コンポーネントは任意の順序で記述できます。コンパイラは、コンポーネントが互いをどのように参照しているかに基づいて、コンポーネントの正しい実行順序を計算します。この依存関係の検出と並べ替えは、置換セクションと出力セクションにも適用されることに注意してください。

### 循環依存関係

コンポーネントが別のコンポーネントを参照する可能性があるため、StyleBookの定義に依存関係の循環が導入される可能性があります。たとえば、コンポーネントAがコンポーネントBで定義されたプロパティを参照し、そのコンポーネントBが再びコンポーネントAで定義されたプロパティを参照する場合などです。この種の依存関係は循環依存関係と呼ばれます。循環依存関係は自動的に解決できません。StyleBookの作成者は、このような循環依存関係を排除するために、StyleBookの定義を手動で修正する必要があります。コンパイラは、循環依存関係が存在する場合、それを特定して報告できます。

次の例は、コンポーネントの循環依存関係を示しています。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
```

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

```
    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

     name: mylb

      servicegroupname: $components.sg-comp.properties.servicegroupname

-

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: $components.lbvserver-comp.properties.servicetype
```

上記の例では、**lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp** の3つのコンポーネントがあります。lbvserver-compはlb-sg-binding-compに依存し、lb-sg-binding-compはsg-compに依存し、sg-compはlbvserver-compに依存します。ここでは、これらのコンポーネント間に依存関係の循環が形成されており、これは自動的に解決できません。その結果、このStyleBookは実行できません。StyleBookコンパイラはこれを検出し、StyleBookがNetScaler Consoleにインポートされるのを防ぎます。

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

# セキュリティ

NetScaler Consoleのセキュリティ分析は、アプリケーションへの脅威を監視、検出、軽減するのに役立ちます。以下のトピックは、セキュリティに関する洞察を表示し、それに基づいて行動するのに役立ちます。

- アプリケーションセキュリティダッシュボード
- セキュリティ違反
- APIセキュリティ

## アプリケーションセキュリティダッシュボード

**App Security**ダッシュボードは、検出/ライセンスされたアプリケーションのセキュリティメトリックの概要を提供します。このダッシュボードには、同期攻撃、スモールウィンドウ攻撃、DNSフラッド攻撃など、検出/ライセンスされたアプリケーションのセキュリティ攻撃情報が表示されます。

アプリケーションセキュリティダッシュボードでセキュリティメトリックを表示するには：

1. **Security** > **Security Dashboard**に移動します。
2. インスタンスリストからインスタンスIPアドレスを選択します。

   レポートには、各アプリケーションに関する以下の情報が含まれます。

   - **脅威インデックス**。アプリケーションに対する攻撃の重要度を示す1桁の評価システムです。アプリケーションに対する攻撃が重要であるほど、そのアプリケーションの脅威インデックスは高くなります。値は1から7の範囲です。

     脅威インデックスは攻撃情報に基づいています。違反タイプ、攻撃カテゴリ、場所、クライアントの詳細などの攻撃関連情報は、アプリケーションに対する攻撃に関する洞察を提供します。違反情報は、違反または攻撃が発生した場合にのみNetScaler Consoleに送信されます。多数の侵害と脆弱性により、脅威インデックス値が高くなります。
   - **安全インデックス**。外部の脅威や脆弱性からアプリケーションを保護するために、NetScalerインスタンスをどれだけ安全に構成しているかを示す1桁の評価システムです。アプリケーションのセキュリティリスクが低いほど、安全インデックスは高くなります。値は1から7の範囲です。

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

安全インデックスは、アプリケーションファイアウォール構成とNetScalerシステムセキュリティ構成の両方を考慮します。高い安全インデックス値を得るには、両方の構成が強力である必要があります。たとえば、厳格なアプリケーションファイアウォールチェックが実施されていても、`nsroot`ユーザーの強力なパスワードなどのNetScalerシステムセキュリティ対策が提供されていない場合、アプリケーションには低い安全インデックス値が割り当てられます。

**App Security Investigator**で報告された不一致を表示できます。

## 脅威インデックスの詳細



**1** - 詳細を表示できるNetScalerインスタンスのIPアドレスを表示します。

**2** - 脅威インデックススコア、発生した違反の総数、ブロックされた違反の総数などの詳細を表示します。

**3** - 選択したインスタンスの仮想サーバーを表示します。

**4** - クライアントに基づいたセキュリティ違反を表示します。各クライアントに対してApp Security Investigatorグラフが表示されます。各クライアントIPをクリックして結果を表示できます。

**5** - マップビューと表形式ビューで違反を表示します。

**6** - 違反の詳細を表示します。グラフにマウスポインターを合わせると、違反タイプ、攻撃時間、合計イベントなどの詳細が表示されます。

バブルグラフをクリックすると、**App Security Violation Details**ページに詳細が表示されます。たとえば、クロスサイトスクリプティング（cross-site script）違反の詳細をさらに表示したい場合は、**App Security Investigator**の**XSS**に表示されているグラフをクリックします。

**App Security Violation Details**には、攻撃時間、攻撃カテゴリ、重大度、URLなどの違反詳細が表示されます。



表示したいオプションを選択するには、**Settings**オプションをクリックすることもできます。

## 安全性インデックスの詳細

アプリケーションの脅威エクスポージャーを確認した後、そのアプリケーションにどのようなアプリケーションセキュリティ構成が設定されており、どのような構成が不足しているかを判断した

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

いと考えるでしょう。この情報は、アプリケーションの安全性インデックスの概要をドリルダウンすることで取得できます。

安全性インデックスの概要は、以下のセキュリティ構成の有効性に関する情報を提供します。

- **アプリケーションファイアウォール構成**。設定されていないシグネチャとセキュリティエンティティの数を示します。
- **NetScaler Consoleシステムセキュリティ**。設定されていないシステムセキュリティ設定の数を示します。

**Safety Index**の詳細を表示するには、仮想サーバー/アプリケーションを選択し、**Safety Index**タブをクリックします。



詳細が表示されます。



**1** - アプリケーションファイアウォール構成の詳細情報を表示します。

**2** - システムセキュリティの詳細情報を表示します。各セキュリティグループをクリックすると、現在のステータスとCitrixの推奨事項に関する詳細が表示されます。

**3** - セキュリティチェックとシグネチャ違反の概要を表示します。

仮想サーバーの**WAF Security Violations**を有効にし、**Security** > **Security Violations**に移動することで、脅威環境の概要も表示できます。

## 統合セキュリティダッシュボード

「**統合セキュリティ**」ダッシュボードは、保護を設定し、分析を有効にし、アプリケーションに保護を展開できる単一ペインのダッシュボードです。このダッシュボードでは、さまざまなテンプレートオプションから選択し、単一のワークフローで構成プロセス全体を完了できます。開始するには、**セキュリティ > セキュリティダッシュボード**に移動し、**アプリケーションの管理**をクリックします。「**アプリケーションの管理**」ページでは、保護されたアプリケーションと保護されていないアプリケーションの詳細を表示できます。

**注:**

- 新規ユーザーの場合、またはStyleBooksを介して、あるいはNetScaler®インスタンスで直接保護を設定していない場合は、**セキュリティ > セキュリティダッシュボード**をクリックすると、次のページが表示されます。

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

セキュリティダッシュボード(/en-us/netscaler-application-delivery-management-software/media/get-started-sec-dashboard.png)

- 保護が必要な仮想サーバーの総数を表示できます。「**開始**」をクリックして、「**保護されていないアプリケーション**」で詳細を表示します。
- 保護を設定するための対象となる仮想サーバータイプは、負荷分散とコンテンツスイッチングです。

### 保護されたアプリケーション

統合セキュリティダッシュボードを使用して保護を設定した後、詳細を表示できます。詳細については、「保護されていないアプリケーションの保護を設定する」を参照してください。

NetScalerインスタンスで直接、またはStyleBooksを介して保護をすでに設定している場合は、「**保護されたアプリケーション**」タブで、「**プロファイル**」の下に「**その他**」とマークされたアプリケーションを表示できます。

保護されたアプリケーション(/en-us/netscaler-application-delivery-management-software/media/secured-applications.png)

### 保護されていないアプリケーションの保護を設定する

**注:**

ブロックリストでサポートされる最大構成エンティティ（ルール）は32です。

「**保護されていないアプリケーション**」タブで、アプリケーションを選択し、「**アプリケーションの保護**」をクリックします。

保護されていないアプリケーション(/en-us/netscaler-application-delivery-management-software/media/unsecured-applications.png)

アプリケーションを保護するために、以下のいずれかのオプションを選択できます。

- **WAFレコメンデーションスキャナー** - このオプションを使用すると、アプリケーションでスキャンを実行できます。スキャンの特定のパラメーターに基づいて、結果はアプリケーションの保護を提案します。これらの推奨事項を適用することを検討してください。
- **保護の選択とカスタマイズ** - このオプションを使用すると、さまざまなテンプレートオプションから選択したり、保護をカスタマイズして展開したりできます。

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

保護のカスタマイズ(/en-us/netscaler-application-delivery-management-software/media/customize-protections.png)

- **OWASP Top 10** - OWASPトップ10のセキュリティリスクに対する業界標準の保護を備えた事前定義されたテンプレートです。詳細については、`https://owasp.org/www-project-top-ten/`を参照してください。
- **CVE保護** - 既知の脆弱性カテゴリに分類された事前設定された署名ルールの一覧から署名セットを作成できます。署名パターンが受信トラフィックと一致した場合に、ログまたはブロックアクションを設定するために署名を選択できます。ログメッセージには脆弱性の詳細が含まれています。
- **カスタム保護** - 要件に基づいて保護を選択し、展開します。

- **既存の保護を選択** - このオプションは、既存のアプリケーションに展開されている保護を複製します。同じ保護を別のアプリケーションに展開したい場合は、このオプションを選択して、そのまま別のアプリケーションに展開できます。このオプションをテンプレートとして選択し、保護を変更してから展開することもできます。

**WAFレコメンデーションスキャナー**

**注:**

- アプリケーションに対して一度に実行できるスキャンは1つだけです。同じアプリケーションまたは別のアプリケーションで新しいスキャンを開始するには、前のスキャンが完了するまで待つ必要があります。
- **履歴の表示**をクリックして、過去のスキャンの履歴とステータスを表示できます。**レポートの表示**をクリックして、後で推奨事項を適用することもできます。

**前提条件:**

- NetScalerインスタンスは、13.0 41.28以降（セキュリティチェック用）および13.0以降（署名用）である必要があります。
- プレミアムライセンスが必要です。
- ロードバランシング仮想サーバーである必要があります。

WAF推奨スキャンを開始するには、以下の情報を提供する必要があります。

1. **スキャンパラメータ**の下：

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

- **ドメイン名** – アプリケーションに関連付けられている、有効でアクセス可能なIPアドレスまたは公開アクセス可能なドメイン名を指定します。例: `www.example.com`。
- **HTTP/HTTPSプロトコル** – アプリケーションのプロトコルを選択します。
- **トラフィックタイムアウト** – スキャン中の単一リクエストの待機時間（秒単位）。値は0より大きい必要があります。
- **スキャン開始URL** – スキャンを開始するアプリケーションのホームページ。例: `https://www.example.com/home`。URLは有効なIPv4アドレスである必要があります。IPアドレスがプライベートである場合、NetScaler Consoleオンプレミス管理IPからプライベートIPアドレスにアクセスできることを確認する必要があります。
- **ログインURL** – 認証のためにログインデータが送信されるURL。HTMLでは、このURLは一般的にアクションURLとして知られています。
- **認証方法** – アプリケーションでサポートされている認証方法（フォームベースまたはヘッダーベース）を選択します。
  - フォームベース認証では、ログイン資格情報を含むフォームをログインURLに送信する必要があります。これらの資格情報は、フォームフィールドとその値の形式である必要があります。その後、アプリケーションはスキャン中にセッションを維持するために使用されるセッションCookieを共有します。
  - ヘッダーベース認証では、ヘッダーセクションに認証ヘッダーとその値が必要です。認証ヘッダーは有効な値を持つ必要があり、スキャン中にセッションを維持するために使用されます。ヘッダーベースの場合、フォームフィールドは空のままにする必要があります。
- **リクエストメソッド** – ログインURLにフォームデータを送信する際に使用されるHTTPメソッドを選択します。許可されるリクエストメソッドは、**POST**、**GET**、**PUT**です。
- **フォームフィールド** – ログインURLに送信するフォームデータを指定します。フォームフィールドは、フォームベース認証を選択した場合にのみ必要です。**フィールド名**がキーで**フィールド値**が値となるキーと値のペアで指定する必要があります。パスワードを含む、ログインに必要なすべてのフォームフィールドが正しく追加されていることを確認してください。値はデータベースに保存される前に暗号化されます。複数のフォームフィールドを追加するには、**追加**をクリックします。例: **フィールド名** – ユーザー名、**フィールド値** – admin。
- **ログアウトURL** – アクセス後にセッションを終了するURLを指定します。例: `https://www.example.com/customer/logout`。

2. 「**スキャン構成**」の下で：

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

- 「**チェックする脆弱性**」 – スキャナーが検出する脆弱性を選択します。現在、これはSQLインジェクションとクロスサイトスクリプティングの違反に対して行われます。デフォルトでは、すべての違反が選択されています。脆弱性を選択すると、アプリケーションでこれらの攻撃をシミュレートし、潜在的な脆弱性を報告します。本番環境ではない環境でこの検出を有効にすることをお勧めします。他のすべての脆弱性も、アプリケーションでこれらの攻撃をシミュレートすることなく報告されます。
- 「**応答サイズ制限**」 – 応答サイズの最大制限。指定された値を超える応答はスキャンされません。推奨される制限は10 MB (1000000バイト) です。
- 「**リクエストの同時実行数**」 – Webアプリケーションに並行して送信されるリクエストの総数。

3. WAFスキャン設定の構成が完了しました。「**スキャン開始**」をクリックしてスキャンプロセスを開始し、進行状況が完了するまで待ちます。スキャンが完了したら、「**レポートの表示**」をクリックします。

   スキャンレポート(/en-us/netscaler-application-delivery-management-software/media/scan-result.png)
4. スキャン結果ページで、「**推奨事項の確認**」をクリックします。

   推奨事項の確認(/en-us/netscaler-application-delivery-management-software/media/review-recommendation.png)
5. 保護を確認するか、他の保護を編集/追加し、「**展開**」をクリックします。

   保護の展開(/en-us/netscaler-application-delivery-management-software/media/deploy-waf-protection.png)

   セキュリティチェックを正常に適用すると：

- 構成は、バージョンに応じて、StyleBookを介してNetScalerインスタンスに適用されます。
  - NetScaler 13.0の場合、`unified-appsec-protection-130` StyleBookが使用されます。
  - NetScaler 13.1の場合、`unified-appsec-protection-131` StyleBookが使用されます。
  - NetScaler 14.1の場合、`unified-appsec-protection-141` StyleBookが使用されます。
- NetScaler上に`Appfw`プロファイルが作成され、`policylabel`を使用してアプリケーションにバインドされます。
- 推奨される署名がすでに適用されている場合、署名はappfwプロファイルにバインドされます。

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

**注**

セキュリティチェックは、NetScaler 13.0 41.28以降のバージョンでサポートされています。

**Applications > Configuration > Config Packs**に移動して、WAFプロファイルと署名がデフォルトのStyleBooksを通じて適用されていることを確認できます。

### WAFスキャナーレポートのエクスポート

WAFスキャナーレポートをエクスポートするには、次の手順に従います。

1. **セキュリティ > ダッシュボード > アプリケーションの管理** に移動します。
2. **Unsecured Applications**タブで、**View History**をクリックします。
3. **Scan History**ページで、目的のスキャンを選択し、**View Report**をクリックします。
4. **Scan Results**ページで、**Export**アイコンをクリックします。
5. **Exports Now**ページで、エクスポートタイプを選択します。

**Snapshot**エクスポートタイプの場合:

1. エクスポートファイル形式を選択します: PDF、JPG、またはPNG
2. レポートのタイトルを入力します。
3. **エクスポート**をクリックします。

スナップショットのエクスポート(/en-us/netscaler-application-delivery-management-software/media/snapshot-export.png)

**表形式**のエクスポートタイプの場合：

リリース14.1ビルド25.x以降、WAFスキャナーレポートを表形式でエクスポートできます。

1. CSVファイル形式を選択します。
2. リストからエクスポートするデータレコードの数を選択します。
3. レポートのタイトルを入力します。
4. **エクスポート**をクリックします。

スナップショットの表形式(/en-us/netscaler-application-delivery-management-software/media/tabular-export.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 保護を選択してカスタマイズする

#### OWASP TOP 10

OWASP Top 10(/en-us/netscaler-application-delivery-management-software/media/owasp-top.png)

**1** - IPアドレス、仮想サーバータイプ、ライセンスタイプ、アプリケーションが構成されているインスタンスなど、アプリケーションに関する情報を提供します。

**2** - 選択したテンプレートを表示します。選択に基づいて名前を変更できます。

**3** - 保護を表示します。一部の保護には追加情報が必要です。

**4** - 詳細ログタイプを表示します。次のオプションを選択できます。

- **パターン**。違反パターンのみをログに記録します。
- **パターンペイロード**。違反パターンと150バイトの追加JSONペイロードをログに記録します。
- **パターン、ペイロード、ヘッダー**。違反パターン、150バイトの追加JSONペイロード、およびHTTPヘッダー情報をログに記録します。

**5** - モニターモードを有効にできます。モニターモードを有効にすると、トラフィックはログに記録されるだけで、軽減策はアクティブになりません。

**6** - 保護を追加できます。「**保護の追加**」をクリックし、追加する保護を確認します。

**7** - 「テンプレートの変更」オプションを使用して、新しいテンプレートを選択できます。

**8** - 保護を編集または削除できます。

**9** - 選択した保護の分析を有効にします。このオプションはデフォルトで選択されています。構成された保護の分析は、**セキュリティ > セキュリティ違反**で表示できます。

保護を設定したら、「**展開**」をクリックします。

#### CVE保護

CVE保護を展開するには、「**CVE保護の作成**」をクリックします。「**署名セットの作成**」ページで、リストから署名を選択してログまたはブロックアクションを設定し、「**保存**」をクリックします。

▢
**保存**をクリックすると、構成ページに追加された署名を表示できます。

▢
アプリケーションに保護を追加するには、 をクリックすることもできます。すべての保護を設定したら、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#### カスタム保護

要件に基づいて保護を展開するには、 をクリックします。 ページで、展開する保護を選択し、 をクリックします。



をクリックした後、構成ページで選択した保護を確認し、 をクリックします。

#### 既存の保護を選択

あるアプリケーションから別のアプリケーションに既存の保護を展開するには、リストから既存の保護を選択します。



保護を選択すると、既存の保護が複製され、構成ページに表示されます。要件に基づいて変更し、をクリックできます。

# アプリケーションセキュリティ違反の詳細を表示

インターネットに公開されているWebアプリケーションは、攻撃に対して著しく脆弱になっています。NetScaler Consoleは、アプリケーションを攻撃から保護するために、実用的な違反の詳細を視覚化することを可能にします。次の単一ペインソリューションについては、**セキュリティ** > **セキュリティ違反** に移動してください。

- WAFセキュリティ違反とボットセキュリティ違反の両方に関連する脅威の詳細を完全に可視化して、アプリケーションを視覚化します
- **ネットワーク**、**ボット**、**WAF** などのカテゴリに基づいてアプリケーションセキュリティ違反にアクセスします
- アプリケーションを保護するための是正措置を講じます

**セキュリティ違反** ページには、次のオプションがあります。

- **アプリケーション概要** – 総違反数、WAFおよびボットの総違反数、国別の違反など、アプリケーションの概要を表示します。詳細については、「アプリケーション概要」を参照してください。
- **すべての違反** – アプリケーションセキュリティ違反の詳細を表示します。詳細については、「すべての違反」を参照してください。

## 前提条件

**メトリクスコレクター** が有効になっていることを確認してください。詳細については、「インテリジェントアプリ分析の構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# APIセキュリティ

NetScaler Console APIセキュリティは、アプリケーションによって処理されるAPIトラフィックの可視性を提供し、使用状況を分析し、公開されているAPIエンドポイントを検出するのに役立ちます。以下のトピックは、開始するのに役立ちます。

- API分析を表示
- APIエンドポイントを検出

## API分析を表示

API分析により、APIトラフィックの可視性が向上します。この分析により、IT管理者はAPIゲートウェイによって提供されるAPIインスタンスとエンドポイントを監視できます。APIリクエストの統合された定期的な監視を提供します。

API分析を監視する前に、APIインスタンスでWeb Insightを有効にしてください。詳細については、「仮想サーバーでの分析の構成」を参照してください。

**API分析**では、API定義の一部として追加されたAPIインスタンスとエンドポイントの応答時間を監視できます。また、APIインスタンスとエンドポイントによって消費された帯域幅も表示されます。

デフォルトでは、ダッシュボードには過去1時間のAPI分析が表示されます。その期間のAPI分析を表示するために期間を選択できます。各タイルで**詳細を表示**をクリックすると、リスト全体が表示されます。このビューでは、**地理的位置**タイルを除き、APIインスタンスとエンドポイントを部分名で検索できます。

### APIエンドポイントの分布

このグラフは、APIエンドポイントのアプリケーションおよびサーバー応答時間の分布を表示します。応答時間が非常に長いAPIエンドポイントを特定し、必要な措置を講じることができます。

APIエンドポイントは、応答時間の制限に応じて、次のいずれかの色で表示されます。

- **緑** – 応答時間が30ミリ秒未満の場合。
- **オレンジ** – 応答時間が30〜100ミリ秒の場合。
- **赤** – 応答時間が100ミリ秒を超える場合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### APIインスタンス

**APIインスタンス**タイルには、アプリケーションおよびサーバー応答時間が高い上位のAPIインスタンスが表示されます。

APIインスタンス(/en-us/netscaler-application-delivery-management-software/media/api-instances.png)

APIインスタンスを選択して、そのパフォーマンス、使用状況、セキュリティの詳細を表示します。選択したAPIインスタンスには、次の情報が表示されます。

- APIエンドポイント数
- リクエスト数
- アプリケーションおよびサーバー応答時間
- 消費帯域幅
- 認証失敗

APIインスタンスダッシュボード(/en-us/netscaler-application-delivery-management-software/media/api-instance-dashboard.png)

### APIエンドポイント

**APIエンドポイント**タイルには、アプリケーションおよびサーバー応答時間が高い上位のエンドポイントが表示されます。

APIエンドポイント(/en-us/netscaler-application-delivery-management-software/media/api-endpoints.png)

APIエンドポイントを選択して、パフォーマンス、使用状況、セキュリティの詳細を表示します。

### 認証失敗

**認証失敗**タイルには、認証失敗が多い上位のAPIエンドポイントが表示されます。認証の失敗または成功は、API定義に追加されたポリシーに基づいて発生します。

認証失敗(/en-us/netscaler-application-delivery-management-software/media/auth-failures-endpoint.png)

APIエンドポイントでの認証の失敗率と成功率を表示したい場合は、次の手順を実行します。

1. **APIエンドポイント**からエンドポイントを選択します。
2. **セキュリティ**タブを選択します。このタブには、選択したエンドポイントでの認証の失敗と成功が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証失敗エンドポイント(/en-us/netscaler-application-delivery-management-software/media/auth-failures-instance.png)

インスタンスのAPIエンドポイントでの認証の失敗率と成功率を表示したい場合は、次の手順を実行します。

1. **APIインスタンス**からインスタンスを選択します。
2. **セキュリティ**タブを選択します。このタブには、選択したインスタンスのエンドポイントでの認証の失敗と成功が表示されます。

### さまざまなAPIインサイトを表示する

APIアナリティクスを移動して、以下の特定の情報を表示します。

- インスタンス内の上位APIエンドポイント
- 最もアクセスされたAPI
- エンドポイントの地理的位置
- HTTPS応答ステータス
- APIリクエストの傾向
- エンドポイントの帯域幅消費量
- SSLエラーと使用状況

#### インスタンス内の上位APIエンドポイントを表示する

**API Analytics**ページには、応答時間が長い上位のエンドポイントが表示されます。インスタンスの類似エンドポイントを表示したい場合は、**API Instances**からインスタンスを選択します。

**Top API Endpoints**タイルには、アプリケーションおよびサーバーの応答時間が長いエンドポイントが表示されます。



#### 最もアクセスされたAPIを表示する

**API Analytics**で、APIインスタンスからAPIインスタンスを選択します。**Most Accessed APIs**タイルには、リクエストと帯域幅が多い上位のエンドポイントが表示されます。



#### エンドポイントの地理的位置を表示する

1. **API Analytics**で、次のいずれかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **API Instances**からインスタンスを選択して、選択したインスタンスのエンドポイントがリクエストを受信した場所を表示します。
- **API Endpoints**からエンドポイントを選択して、そのエンドポイントがリクエストを受信した場所を表示します。

2. **Performance and Usage**で、**Geo Locations**タイルが表示されます。

   応答時間、帯域幅、およびリクエストに基づいて場所を並べ替えることができます。

### HTTPS応答ステータスを表示

「**HTTPS応答ステータス**」タイルには、応答ステータスとその理由および発生回数が表示されます。HTTPS応答ステータスは、次のいずれかの方法で表示できます。

- 「**APIインスタンス**」からインスタンスを選択します。
- 「**APIエンドポイント**」からエンドポイントを選択します。

このタイルは、「**パフォーマンスと使用状況**」タブに表示されます。

HTTPS応答ステータス(/en-us/netscaler-application-delivery-management-software/media/https-response-status-apis.png)

### APIリクエストの傾向を表示

「**APIエンドポイント**」からエンドポイントを選択します。「**パフォーマンスと使用状況**」で、「**合計リクエスト**」タイルには、エンドポイントが受信した合計リクエスト数の傾向が表示されます。

合計APIリクエスト(/en-us/netscaler-application-delivery-management-software/media/total-requests-endpoint.png)

レート制限のためにドロップされたリクエストの傾向を表示する場合は、「**APIインスタンス**」からインスタンスを選択します。「**セキュリティ**」で、「**レート制限**」タイルには、ドロップされたリクエストの傾向が表示されます。また、エンドポイントが受信した合計リクエストの傾向も表示されます。

レート制限(/en-us/netscaler-application-delivery-management-software/media/rate-limit-instance.png)

この比較により、合計リクエストのうち、レート制限のためにドロップされたリクエストの数を特定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### エンドポイントの帯域幅消費量を表示

エンドポイントによる帯域幅消費の傾向を表示するには、APIエンドポイントからエンドポイントを選択します。「**帯域幅**」タイルには、帯域幅消費グラフが表示されます。

帯域幅消費量(/en-us/netscaler-application-delivery-management-software/media/bandwidth-consumption-endpoint.png)

### SSLエラーと使用状況を表示

**APIインスタンス**からインスタンスを選択します。**セキュリティ**には、次のタイルが表示されます。

- **SSLエラー** – クライアントおよびアプリケーションサーバーで発生したSSL障害を表示します。
- **SSL使用状況** – SSL証明書、プロトコル、暗号、およびキーの強度とそれらの発生回数を表示します。

SSLエラーと使用状況(/en-us/netscaler-application-delivery-management-software/media/ssl-errors-usage-instance.png)

エンドポイントでSSL使用状況を表示するには、APIエンドポイントからエンドポイントを選択します。**セキュリティ**タブに**SSL使用状況**タイルが表示されます。

SSL使用状況(/en-us/netscaler-application-delivery-management-software/media/ssl-usage-apis.png)

## APIエンドポイントを検出する

APIセキュリティを使用して、組織内で検出されたAPIエンドポイントを表示します。NetScaler Consoleは、NetScalerインスタンスで受信したAPIトラフィックに基づいてAPIエンドポイントを検出します。

NetScaler Consoleでは、**Security > API Security > API Discovery** ページに検出されたAPIエンドポイントが表示されます。

**VServers** タブには、NetScalerインスタンスからの仮想サーバーが表示されます。仮想サーバーは、指定された期間にAPIリクエストを受信するとこのタブに表示されます。

**注:**

分析を設定し、仮想サーバーでWeb Insightsを有効にしてください。参照: APIインスタンスでWeb Insightを有効にする。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### APIエンドポイントを表示する

**API Discovery** で仮想サーバーを選択すると、NetScaler Console GUI にAPIエンドポイントとその詳細が表示されます。例えば、:

- **Method** - APIエンドポイントで使用されるメソッドが表示されます。例えば、`GET` および `POST` メソッドなどです。
- **Total requests** - APIエンドポイントでのAPIリクエストの数が表示されます。
- **Response statuses** - 各応答ステータスの数が表示されます。例えば、`2xx`、`3xx`、`4xx`、および `5xx` などです。

仮想サーバー内のAPIエンドポイントは次のとおりです。

必要なAPIエンドポイントを選択して、その詳細な分析レポートを表示することもできます。

各セクションの詳細については、「API分析の表示」(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/security/api-security/api-analytics.html)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# ゲートウェイ

NetScaler Console は、NetScaler Gateway を介して提供されるトラフィックのパフォーマンスとユーザーエクスペリエンスを可視化するゲートウェイ分析を提供します。以下のトピックは、ゲートウェイトラフィックの監視とトラブルシューティングに役立ちます。

- ゲートウェイインサイト
- HDXインサイト

## Gateway Insight

NetScaler Gatewayの展開において、ユーザーのアクセス詳細の可視性は、アクセス障害のトラブルシューティングに不可欠です。ネットワーク管理者として、ユーザーがNetScaler Gatewayにログオンできない場合や、ユーザーのアクティビティ、ログオン失敗の理由を知りたいと思うでしょう。この情報は通常、ユーザーが解決を要求しない限り利用できません。

Gateway Insightは、アクセスモードに関係なく、NetScaler Gatewayへのログオン時にすべてのユーザーが遭遇した障害を可視化します。任意の時点で、利用可能なすべてのユーザーのリスト、アクティブユーザー数、アクティブセッション数、およびすべてのユーザーが使用したバイト数とライセンスを表示できます。ユーザーのエンドポイント分析 (EPA)、認証、シングルサインオン (SSO)、およびアプリケーション起動の失敗を表示できます。また、ユーザーのアクティブセッションと終了したセッションの詳細も表示できます。

Gateway Insightは、仮想アプリケーションのアプリケーション起動失敗の理由も可視化します。これにより、あらゆる種類のログオンまたはアプリケーション起動の失敗の問題をトラブルシューティングする能力が向上します。起動されたアプリケーションの数、合計およびアクティブなセッションの数、合計バイト数、およびアプリケーションによって消費された帯域幅を表示できます。アプリケーションのユーザー、セッション、帯域幅、および起動エラーの詳細を表示できます。

任意の時点で、NetScaler Gatewayアプライアンスに関連付けられているすべてのゲートウェイによって使用されているゲートウェイの数、アクティブセッション数、合計バイト数、および帯域幅を表示できます。ゲートウェイのエンドポイント分析 (EPA)、認証、シングルサインオン、およびアプリケーション起動の失敗を表示できます。また、ゲートウェイに関連付けられているすべてのユーザーとそのログオンアクティビティの詳細も表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

すべてのログメッセージはNetScaler Consoleデータベースに保存されるため、任意の期間のエラー詳細を表示できます。また、ログオン失敗の概要を表示し、ログオンプロセスのどの段階で失敗が発生したかを特定することもできます。

## 注意点

- Gateway Insightは、以下の展開でサポートされています。
  - Access Gateway
  - 統合ゲートウェイ
- NetScaler Consoleのリリースとビルドは、NetScaler Gatewayアプライアンスのリリースとビルドと同じか、それ以降である必要があります。
- Advancedライセンスを持つNetScalerインスタンスでは、1時間分のGateway Insightレポートを表示できます。1時間を超えるGateway Insightレポートを表示するには、Premiumライセンスが必須です。

## 制限事項

- 認証方法が証明書ベースの認証として構成されている場合、NetScaler GatewayはGateway Insightをサポートしません。
- Gateway Insightレポートの場合、NetScalerアプライアンスから地理位置情報が提供されません。
- 仮想ICAアプリケーションおよびデスクトップのユーザーログオンの成功、遅延、およびアプリケーションレベルの詳細は、HDX™ Insight Usersダッシュボードでのみ表示されます。
- ダブルホップモードでは、2番目のDMZにあるNetScaler Gatewayアプライアンスでの障害の可視性は利用できません。
- リモートデスクトッププロトコル（RDP）デスクトップアクセスに関する問題は報告されません。
- Gateway Insightは、次の認証タイプをサポートしています。これら以外の認証タイプを使用すると、Gateway Insightでいくつかの不一致が発生する可能性があります。
  - ローカル
  - LDAP
  - RADIUS
  - TACACS
  - SAML

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ネイティブOTP
- オーオース-オープンIDコネクト

  OAuth-OpenID Connect認証の場合、NetScalerはOAuth-OpenID Connectリライングパーティ（RP）またはOAuth-OpenID Connectアイデンティティプロバイダー（IdP）として機能できます。認証が成功すると、ユーザー名はGateway Insightレポートのタブに報告されます。ただし、セッションがIdPまたはRPのどちらで作成されたかを特定することはできません。

  **注：** OAuth-OpenID Connect認証は、NetScaler Consoleリリース13.1ビルド4.xx以降でサポートされています。

## Gateway Insightを有効にする

NetScaler GatewayアプライアンスでGateway Insightを有効にするには、まずNetScaler Gatewayアプライアンスを NetScaler Consoleに追加する必要があります。次に、VPNアプリケーションを表す仮想サーバーに対してAppFlowを有効にする必要があります。NetScaler Consoleへのデバイスの追加については、「デバイスの追加」を参照してください。

**注**

NetScaler Consoleでエンドポイント分析 (EPA) の失敗を表示するには、NetScaler GatewayアプライアンスでAppFlow認証、承認、および監査ユーザー名(#enable-appflow-aaa-user-name-logging-on-a-citrix-gateway-appliance-by-using-the-gui)ロギングを有効にする必要があります。

ゲートウェイインサイトを有効にする以下の手順は、NetScaler Consoleが**13.0 Build 36.27**である場合に適用されます。

1. **インフラストラクチャ > インスタンス**に移動し、AppFlowを有効にするインスタンスを選択します。
2. **アクションの選択**リストから、**分析の構成**を選択します。
3. **インサイトの構成**ページで、**分析の構成**の下にある**NetScaler Gateway**を選択します。
4. 仮想サーバーを選択し、**AppFlowを有効にする**をクリックします。
5. **AppFlowを有効にする**画面で、**式の選択**リストのtrueをクリックします。
6. **転送モード**の横にある**Logstream**チェックボックスをオンにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注**
>
> 転送モードとして**IPFIX**または**Logstream**のいずれかを選択できます。

**IPFIX**および**Logstream**の詳細については、**Logstreamの概要**を参照してください。

7. **OK**をクリックします。

### NetScaler Consoleバージョン13.0 Build 41.x以降の場合

1. **インフラストラクチャ > インスタンス**に移動し、インスタンスを選択します。
2. **Select Action**リストから、**Configure Analytics**を選択します。
3. 仮想サーバーを選択し、**Enable Analytics**をクリックします。
4. **Advanced Options**で、次の操作を行います。
   a. **Logstream**を選択します。
   b. **NetScaler Gateway**を選択します。
5. **OK**をクリックします。

### GUIを使用してNetScaler GatewayアプライアンスでAppFlow認証、承認、および監査ユーザー名ログを有効にする

1. **Configuration > System > AppFlow > Settings**に移動し、**Change AppFlow Settings**をクリックします。
2. **Configure AppFlow Settings**画面で、**AAA Username**を選択し、**OK**をクリックします。

## Gateway Insightレポートの表示

NetScaler Consoleでは、NetScaler Gatewayアプライアンスに関連付けられているすべてのユーザー、アプリケーション、およびゲートウェイのレポートを表示でき、特定のユーザー、アプリケーション、またはゲートウェイの詳細を表示できます。**Overview**セクションでは、EPA、SSO、認証、およびアプリケーション起動の失敗を表示できます。また、ユーザーがログオンするために使用したさまざまなセッションモード、クライアントの種類、および毎時ログオンしたユーザー数の概要も表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

グループを作成するときに、グループにロールを割り当て、グループにアプリケーションレベルのアクセスを提供し、グループにユーザーを割り当てることができます。NetScaler Consoleアナリティクスは、仮想IPアドレスベースの承認をサポートするようになりました。ユーザーは、承認されているアプリケーション（仮想サーバー）のみのすべてのインサイトのレポートを表示できるようになりました。グループとグループへのユーザーの割り当ての詳細については、「Configure Groups」を参照してください。

### EPA、SSO、認証、承認、およびアプリケーション起動の失敗を表示するには

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. ユーザーの詳細を表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。「**Go**」をクリックします。
3. EPA (エンドポイント分析)、認証、承認、SSO (シングルサインオン)、またはアプリケーション起動のタブをクリックして、失敗の詳細を表示します。



### セッションモード、クライアント、およびユーザー数の概要を表示するには

NetScaler Consoleで、**Gateway > Gateway Insight**に移動し、下にスクロールしてレポートを表示します。



## ユーザーのGateway Insightレポートを表示する

次のレポートを表示できます。

- NetScaler Gatewayアプライアンスに関連付けられているすべてのユーザー。
- ユーザーのEPA、認証、SSO、およびアプリケーション起動の失敗。
- ユーザーのアクティブセッションと終了セッションの詳細。
- フルトンネル、クライアントレスVPN、ICA®プロキシなどのセッションモードの種類。

### ユーザーの詳細を表示するには

1. NetScaler Consoleで、**Gateway > Gateway Insight > Users**に移動します。
2. ユーザーの詳細を表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。「**Go**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. その期間中にすべてのユーザーが使用したアクティブユーザー数、アクティブセッション数、バイト数、ライセンス数を表示できます。

   Gateway Insightユーザーレポート(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-users.png)

下にスクロールして、利用可能なユーザーとアクティブユーザーのリストを表示します。

アクティブユーザー(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-active-users.png)

「**Users**」または「**Active Users**」タブでユーザーをクリックすると、以下のユーザー詳細が表示されます。

- **ユーザー詳細** - NetScaler Gatewayアプライアンスに関連付けられている各ユーザーのインサイトを表示できます。「**Gateway**」>「**Gateway Insight**」>「**Users**」に移動し、ユーザーをクリックすると、セッションモード、オペレーティングシステム、ブラウザなど、選択したユーザーのインサイトが表示されます。

  ユーザー詳細(/en-us/netscaler-application-delivery-management-software/media/gw-user-details.png)
- **選択したゲートウェイのユーザーとアプリケーション** - 「**Gateway**」>「**Gateway Insight**」>「**Gateway**」に移動し、ゲートウェイドメイン名をクリックすると、選択したゲートウェイに関連付けられている上位10のアプリケーションと上位10のユーザーが表示されます。

  ユーザーとアプリケーション(/en-us/netscaler-application-delivery-management-software/media/gw-user-app.png)
- **アプリケーションとユーザーのその他のオプションを表示** – 10を超えるアプリケーションとユーザーの場合、「Applications and Users」のその他アイコンをクリックすると、選択したゲートウェイに関連付けられているすべてのユーザーとアプリケーションの詳細を表示できます。
- **棒グラフをクリックして詳細を表示** – 棒グラフをクリックすると、関連する詳細を表示できます。たとえば、**Gateway > Gateway Insight > Gateway** に移動し、ゲートウェイの棒グラフをクリックすると、ゲートウェイの詳細が表示されます。

  棒グラフ(/en-us/netscaler-application-delivery-management-software/media/bar-graph.png)
- ユーザーの**アクティブセッション**と**終了セッション**。

  Gateway Insightのアクティブセッションと終了セッション(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-active-terminated-session.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**アクティブセッション**」におけるゲートウェイドメイン名とゲートウェイIPアドレス。
- ユーザーのログイン期間。

  Gateway Insightのログイン期間(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-login-duration.png)
- ユーザーログアウトセッションの理由。ログアウトの理由は次のとおりです。
  - セッションがタイムアウトしました
  - 内部エラーのためログアウトしました
  - 非アクティブセッションのタイムアウトによりログアウトしました
  - ユーザーがログアウトしました
  - 管理者がセッションを停止しました

## アプリケーションのGateway Insightレポートを表示する

起動されたアプリケーションの数、合計セッション数とアクティブセッション数、アプリケーションによって消費された合計バイト数と帯域幅を表示できます。アプリケーションのユーザー、セッション、帯域幅、起動エラーの詳細を表示できます。

### アプリケーションの詳細を表示するには

1. NetScaler Consoleで、**ゲートウェイ > Gateway Insight > アプリケーション**に移動します。
2. アプリケーションの詳細を表示する期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。「**Go**」をクリックします。

起動されたアプリケーションの数、合計セッション数とアクティブセッション数、アプリケーションによって消費された合計バイト数と帯域幅を表示できるようになりました。

アプリケーションの詳細(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-apps.png)

ICAおよびその他のアプリケーションによって消費されたセッション数、帯域幅、および合計バイト数を表示するには、下にスクロールします。

その他のアプリケーションの詳細(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-other-apps.png)

タブで、 列のアプリケーションをクリックすると、そのアプリケーションの詳細が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ゲートウェイのGateway Insightレポートを表示する

NetScaler Gatewayアプライアンスに関連付けられているすべてのゲートウェイによって使用されているゲートウェイの数、アクティブセッションの数、合計バイト数、および帯域幅をいつでも表示できます。ゲートウェイのEPA、認証、シングルサインオン、およびアプリケーション起動の失敗を表示できます。また、ゲートウェイに関連付けられているすべてのユーザーの詳細と、そのログオンアクティビティも表示できます。

### ゲートウェイの詳細を表示するには

1. **NetScaler Console**で、 **> >** の順に移動します。
2. ゲートウェイの詳細を表示する期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズします。 をクリックします。

これで、NetScaler Gatewayアプライアンスに関連付けられているすべてのゲートウェイによって使用されているゲートウェイの数、アクティブセッションの数、合計バイト数、および帯域幅をいつでも表示できます。

ゲートウェイアクティビティの詳細(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-gatways.png)

ゲートウェイドメイン名、仮想サーバー名、NetScaler® IPアドレス、セッションモード、合計バイト数などのゲートウェイの詳細を表示するには、下にスクロールします。

その他のゲートウェイの詳細(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-gatway-domains.png)

列のゲートウェイをクリックすると、そのゲートウェイのEPA、認証、シングルサインオン、アプリケーション起動の失敗、およびその他の詳細が表示されます。

## レポートのエクスポート

GUIに表示されるすべての詳細を含むGateway Insightレポートを、PDF、JPEG、PNG、またはCSV形式でローカルコンピューターに保存できます。また、レポートのエクスポートを、指定されたメールアドレスにさまざまな間隔でスケジュールすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

- 読み取り専用アクセス権を持つユーザーは、レポートをエクスポートできません。
- 地理マップレポートは、NetScaler Consoleにインターネット接続がある場合にのみエクスポートされます。

### レポートをエクスポートするには

1. **ダッシュボード**タブの右ペインで、**エクスポート**ボタンをクリックします。
2. **今すぐエクスポート**で、必要な形式を選択し、**エクスポート**をクリックします。

### エクスポートをスケジュールするには：

1. **ダッシュボード**タブの右ペインで、**エクスポート**ボタンをクリックします。
2. **エクスポートのスケジュール**で、詳細を指定し、**スケジュール**をクリックします。

### メールサーバーまたはメール配布リストを追加するには：

1. **構成**タブで、**設定 > 通知 > メール**に移動します。
2. 右ペインで、メールサーバーを追加するには**メールサーバー**を選択し、メール配布リストを作成するには**メール配布リスト**を選択します。
3. 詳細を指定し、**作成**をクリックします。

### Gateway Insightダッシュボード全体をエクスポートするには：

1. 「**ダッシュボード**」タブの右ペインで、「**エクスポート**」ボタンをクリックします。
2. 「**今すぐエクスポート**」の下で、「**PDF**」形式を選択し、「**エクスポート**」をクリックします。

## Gateway Insight のユースケース

次のユースケースは、Gateway Insight を使用して、NetScaler Gateway アプライアンス上のユーザーのアクセス詳細、アプリケーション、およびゲートウェイを可視化する方法を示しています。

### ユーザーが NetScaler Gateway アプライアンスまたは内部 Web サーバーにログインできない

あなたは NetScaler Console を介して NetScaler Gateway アプライアンスを監視している NetScaler Gateway 管理者であり、ユーザーがログインできない理由、またはログインプロセスのどの段階で障害が発生したかを確認したいと考えています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console を使用すると、ログインプロセスの次の段階でユーザーログインエラーの詳細を表示できます。

- 認証
- エンドポイント分析 (EPA)
- シングルサインオン

NetScaler Console では、特定のユーザーを検索し、そのユーザーのすべての詳細を表示できます。

**ユーザーを検索するには：**

NetScaler Console で、**Gateway > Gateway Insight** に移動し、「**ユーザーを検索**」テキストボックスに検索したいユーザーを指定します。

### 認証の失敗

認証情報の誤りや認証サーバーからの応答がないなどの認証エラーを表示できます。また、認証が失敗した要因も確認できます。

**認証失敗の詳細を表示するには：**

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. **概要**セクションで、認証エラーを表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。**Go**をクリックします。

   
3. **認証**タブをクリックします。**失敗**グラフで、任意の時点での認証エラーの数を確認できます。

   

同じタブのテーブルから、**ユーザー名、クライアントIPアドレス、エラー時刻、認証タイプ、認証サーバーIPアドレス**など、各認証エラーの詳細を表示するには下にスクロールします。テーブルの**エラーの説明**列にはログオン失敗の理由が表示され、**状態**列には失敗が発生したn番目の要素が表示されます。



**ユーザー名**列のユーザーをクリックすると、そのユーザーの認証エラーやその他の詳細が表示されます。設定アイコンを使用して、テーブルをカスタマイズし、列を追加または削除できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要：**

OAuth-OpenID Connect認証が失敗した場合、一部の失敗（例：「トークン検証失敗」）では、Gateway Insightレポートでユーザー名が**NA**と表示されます。この失敗では、OAuth-OpenID Connectリライングパーティでの「トークン検証失敗」による認証失敗の場合、ユーザー名は利用できません。



### EPAの失敗

EPAの失敗は、事前認証または事後認証の段階で確認できます。

**重要：**

NetScaler Gatewayは、クラシック式と高度な式の両方について、EPA障害をNetScaler Consoleに報告します。高度な式の場合、ポリシー名はGateway Insightダッシュボードに表示されません。EPAがnFactor認証フローの要素の1つとして構成されている場合、障害が報告されます。

**EPA障害の詳細を表示するには：**

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. 概要セクションで、EPAエラーを表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。**Go**をクリックします。

   
3. **EPA (エンドポイント分析)**タブをクリックします。**障害**グラフで、任意の時点でのEPAエラーの数を表示できます。

   

スクロールダウンして、同じタブのテーブルから、**ユーザー名、NetScaler IPアドレス、Gateway IPアドレス、VPN、エラー時刻、ポリシー名、Gatewayドメイン名**など、各EPAエラーの詳細を表示します。

テーブルの**エラーの説明**列には、EPA障害の理由が表示されます。例えば、nFactor EPA障害が原因でEPAチェックが失敗した場合、「EPA事前認証チェックの失敗」というエラーメッセージが表示されます。

**ポリシー名**列には、障害の原因となったポリシーが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



**ユーザー名**列のユーザーをクリックすると、そのユーザーのEPAエラーやその他の詳細が表示されます。下向き矢印を使用して列を追加または削除することで、テーブルをカスタマイズできます。EPAがnFactor認証フローの要素として使用されている場合、ユーザー名が割り当てられていないエントリにはケースIDが表示されます。

**注**

「clientSecurity」式がVPNセッションポリシー規則として構成されている場合、NetScaler GatewayはEPA障害を報告しません。

### SSO障害

NetScaler Gatewayアプライアンスを介してアプリケーションにアクセスするユーザーの、あらゆる段階でのSSO失敗をすべて表示できます。

**SSO失敗の詳細を表示するには：**

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. 概要セクションで、SSOエラーを表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。**Go**をクリックします。

   
3. **SSO (Single Sign On)** タブをクリックします。失敗グラフで、任意の時点でのSSOエラーの数を表示できます。

   

同じタブのテーブルから、**ユーザー名、NetScaler IPアドレス、エラー発生時刻、エラーの説明、リソース名**などの各SSOエラーの詳細を表示するには、下にスクロールします。



**ユーザー名**列のユーザーをクリックすると、そのユーザーのSSOエラーやその他の詳細が表示されます。下向き矢印を使用して、テーブルをカスタマイズし、列を追加または削除できます。

### NetScaler Gatewayに正常にログオンした後、ユーザーが仮想アプリケーションを起動できない

アプリケーション起動の失敗については、アクセスできないSecure Ticket Authority (STA) またはCitrix Virtual Appサーバー、あるいは無効なSTAチケットなどの原因を可視化できます。エラーが発生した時刻、エラーの詳細、およびSTA検証が失敗したリソースを表示できます。

**アプリケーション起動失敗の詳細を表示するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. **概要**セクションで、SSOエラーを表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。**Go**をクリックします。

   「アプリケーション起動失敗ビュー」(/en-us/netscaler-application-delivery-management-software/media/use-cases-app-launch-failure-overview.png)
3. 「**Application Launch**」タブをクリックします。「**Failures**」グラフで、任意の時点でのアプリケーション起動失敗の数を確認できます。

   「アプリケーション起動失敗グラフ」(/en-us/netscaler-application-delivery-management-software/media/use-cases-app-launch-failure-graph.png)

同じタブのテーブルから、**NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name** など、各アプリケーション起動エラーの詳細を表示するには、下にスクロールします。テーブルの**Error Description**列にはSTAサーバーのIPアドレスが表示され、**Resource Name**列にはSTA検証が失敗したリソースの詳細が表示されます。

**Username**列のユーザーをクリックすると、そのユーザーのアプリケーション起動エラーやその他の詳細が表示されます。下向き矢印を使用して、列を追加または削除するようにテーブルをカスタマイズできます。

### 新しいアプリケーションを正常に起動した後、ユーザーはそのアプリケーションによって消費された合計バイト数と帯域幅を表示したいと考えています

新しいアプリケーションを正常に起動した後、NetScaler Consoleで、そのアプリケーションによって消費された合計バイト数と帯域幅を表示できます。

**アプリケーションによって消費された合計バイト数と帯域幅を表示するには：**

NetScaler Consoleで、**Gateway > Gateway Insight > Applications** に移動し、下にスクロールして、**Other Applications**タブで詳細を表示したいアプリケーションをクリックします。

「バイトと帯域幅の消費ビュー」(/en-us/netscaler-application-delivery-management-software/media/use-cases-bytes-bandwidth-consumed.png)

そのアプリケーションによって消費されたセッション数と合計バイト数を表示できます。

「セッションとバイトの合計数ビュー」(/en-us/netscaler-application-delivery-management-software/media/use-cases-bytes-consumed.png)

そのアプリケーションによって消費された帯域幅も表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「アプリケーションによって消費されたバイト数ビュー」(/en-us/netscaler-application-delivery-management-software/media/use-cases-bandwidth-consumed.png)

### ユーザーはNetScaler Gatewayに正常にログオンしましたが、内部ネットワーク内の特定のネットワークリソースにアクセスできません

Gateway Insightを使用すると、ユーザーがネットワークリソースにアクセスできるかどうかを判断できます。また、失敗の原因となったポリシーの名前も表示できます。

**リソースのユーザーアクセスを表示するには:**

1. NetScaler Consoleで、**ゲートウェイ > ゲートウェイインサイト > アプリケーション** に移動します。
2. 表示される画面で下にスクロールし、**Other Applications** タブで、ユーザーがログオンできなかったアプリケーションを選択します。

   
3. 下にスクロールすると、**Users** テーブルに、そのアプリケーションにアクセスできるすべてのユーザーが表示されます。

### 異なるユーザーが異なるNetScaler Gateway展開を使用しているか、または異なるアクセスモードでNetScaler Gatewayにログオンしている可能性があります。管理者は、展開タイプとアクセスモードに関する詳細を表示できる必要があります

Gateway Insightを使用すると、ユーザーがログオンに使用したさまざまなセッションモード、クライアントの種類、および1時間あたりのログオンユーザー数の概要を表示できます。また、ユーザーの展開が統合ゲートウェイ展開であるか、従来のNetScaler Gateway展開であるかを判断することもできます。統合ゲートウェイ展開の場合、コンテンツスイッチング仮想サーバー名とIPアドレス、およびVPN仮想サーバー名を表示できます。

**セッションモード、クライアントの種類、およびログオンユーザー数の概要を表示するには**:

1. NetScaler Consoleで、**Gateway > Gateway Insight** に移動します。
2. **概要**セクションで下にスクロールすると、**セッションモード、オペレーティングシステム、ブラウザ**、および**ユーザーログオンアクティビティ**のグラフが表示され、ユーザーがログオンに使用したさまざまなセッションモード、クライアントの種類、および1時間あたりのログオンユーザー数が示されます。

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Gateway Insight の問題のトラブルシューティング

Gateway Insight ソリューションが期待どおりに機能しない場合、問題は以下のいずれかにある可能性があります。トラブルシューティングについては、それぞれのセクションのチェックリストを参照してください。

- Gateway Insight の構成。
- NetScaler と NetScaler Console 間の接続の問題。
- NetScaler でのレコードの生成。
- NetScaler Console での検証。

## Gateway Insight 構成チェックリスト

- NetScaler アプライアンスで AppFlow 機能が有効になっていることを確認してください。詳細については、「AppFlow の有効化」を参照してください。
- NetScaler の実行中の構成で Gateway Insight の構成を確認します。

  `show running | grep -i <appflow_policy>` コマンドを実行して Gateway Insight の構成を確認します。バインドタイプが REQUEST であることを確認してください。例:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  バインドタイプ OTHERTCP_REQUEST も Gateway Insight に必要です。

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type
  OTHERTCP_REQUEST
  ```

- シングルホップ、Access Gateway、または Unified Gateway の展開の場合、VPN トラフィックが流れている VPN 仮想サーバーに Gateway Insight AppFlow ポリシーがバインドされていることを確認してください。詳細については、「HDX Insight データ収集の有効化」を参照してください。
- ダブルホップの場合、Gateway Insight は両方のホップで構成する必要があります。
- NetScaler Gateway/VPN 仮想サーバーで `appflowlog` パラメーターを確認します。詳細については、「仮想サーバーの AppFlow を有効にする」を参照してください。

## NetScaler と NetScaler Console 間の接続チェックリスト

- NetScalerでAppFlowコレクターのステータスを確認します。詳細については、NetScalerとAppFlowコレクター間の接続ステータスを確認する方法を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Gateway Insight AppFlow®ポリシーのヒット数を確認します。

  コマンド `show appflow policy <policy_name>` を実行して、AppFlowポリシーのヒット数を確認します。

  GUIで**Settings > AppFlow > Policies**に移動して、AppFlowポリシーのヒット数を確認することもできます。
- AppFlowポート4739または5557をブロックしているファイアウォールがないか確認します。

### NetScalerチェックリストでのレコード生成

- `nsconmsg -d stats -g ai_tot` コマンドを実行し、NetScalerでの統計情報の増加を確認します。
- `nstrace logs` をキャプチャし、CFLOWパケットを確認して、NetScalerがAppFlowレコードをエクスポートしていることを確認します。

  **注:**

  `nstrace logs` はIPFIXにのみ必要です。Logstreamの場合、nstraceログではNetScalerアプライアンスがAppFlowレコードをエクスポートしたかどうかは確認できません。

### NetScaler Consoleでのレコードの検証

- `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` コマンドを実行してログを確認し、NetScaler ConsoleがAppFlowレコードを受信していることを確認します。
- NetScalerインスタンスがNetScaler Consoleに追加されていることを確認します。
- NetScaler Gateway/VPN仮想サーバーがNetScaler Consoleでライセンスされていることを確認します。

### NetScaler ConsoleでのLogstreamログの検証

NetScaler Console で受信した Logstream データの検証は、次の方法で行うことができます。

- **NetScaler Console でのデータレコードロギングの有効化**

  有効にすると、ログは /var/mps/log/mps_afdecoder.log で確認できます。
- **ULFD ライブラリロギングの有効化**

  コマンド `/mps/decoder_enable_debug` を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ログは `/var/ulflog/libulfd.log` にキャプチャされます。

コマンド `/mps/decoder_disable_debug` を使用してロギングを無効にできます。

### Gateway Insight カウンター

次の Gateway Insight カウンターが利用可能です。

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

### NetScalerログのAppFlowレコード

リリース13.0ビルド71.x以降、AppFlowレコードがエクスポートされているかどうかをNetScalerログで確認できます。`syslogparams`のデフォルトのログレベルは、すべてのエラーログと情報ログをキャプチャします。エラーの手がかりが見つからない場合は、`syslogparams`でDEBUGを含むすべてのログレベルを有効にして、DEBUGログもキャプチャしてください。

#### サンプルログ

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "GwInsight:
Sent auth record Func=ns_sslvpn_export_auth_data Username=<name>
Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid> Gwip=<ip>:443
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<vpnfqdn> Authtype=3
EPAid=(null) AuthStage=1 AuthDuration=309 AuthAgent=<auth_server_ip>
Groupname= Policyname=<name> CurfactorPolname=<name> NextfactorPolname=
CSecExpr= Devicetype=16777219 Deviceid=0 email="

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight:
Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is zero"

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight:
Func=update_session_appflow_collector pcb or session is NULL"

<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record Username=<>
Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=1 Sessid=<sessid>
Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn>
SSOAuthMethod=0 SessState=2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/
Citrix/Store

Web BackendServername= SSOurl= email="

SSO logs:
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=1 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=3 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
VPNfqdn=<fqdn> SSOAuthMethod=2 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:443 SessSeq=c
Sessid=<sessid> Gwip=<ip>:443 StatusCode=155 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=6 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

### Citrixテクニカルサポートへのお問い合わせ

迅速な解決のために、Citrixテクニカルサポートに連絡する前に以下の情報を用意してください。

- 展開とネットワークトポロジの詳細。
- NetScalerおよびNetScaler Consoleのバージョン。
- NetScalerおよびNetScaler Consoleのテクニカルサポートバンドル。
- 問題発生時の`nstrace`キャプチャ。

### 既知の問題

Gateway Insightの既知の問題については、NetScalerのリリースノートを参照してください。

## HDX™ インサイト

HDX インサイトは、NetScalerを介してCitrix Virtual Apps and Desktopに渡されるHDXトラフィックのエンドツーエンドの可視性を提供します。また、管理者はリアルタイムのクライアントおよびネットワーク遅延メトリック、履歴レポート、エンドツーエンドのパフォーマンスデータを確認し、パフォーマンスの問題をトラブルシューティングできます。リアルタイムと履歴の両方の可視性データが利用可能であるため、NetScaler Consoleは幅広いユースケースをサポートできます。

データが表示されるようにするには、NetScaler Gateway仮想サーバーでAppFlowを有効にする必要があります。AppFlowはIPFIXプロトコルまたはLogStreamメソッドによって配信できます。

**注**

ICA®ラウンドトリップ時間の計算がログに記録されるようにするには、次のポリシー設定を有効にします。

- ICAラウンドトリップ計算

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ICAラウンドトリップ計算間隔
- アイドル接続のICAラウンドトリップ計算

個々のユーザーをクリックすると、選択した期間内にユーザーが行った、アクティブまたは終了した各HDXセッションを確認できます。その他の情報には、いくつかの遅延統計とセッション中に消費された帯域幅が含まれます。また、オーディオ、プリンターマッピング、クライアントドライブマッピングなどの個々の仮想チャネルから帯域幅情報を取得することもできます。

**注**

グループを作成すると、グループに役割を割り当て、グループにアプリケーションレベルのアクセスを提供し、ユーザーをグループに割り当てることができます。NetScaler Consoleアナリティクスは、仮想IPアドレスベースの承認をサポートするようになりました。ユーザーは、承認されているアプリケーション（仮想サーバー）のみのすべてのインサイトのレポートを表示できるようになりました。グループとグループへのユーザーの割り当ての詳細については、「グループの構成」を参照してください。

**Gateway > HDX Insight > Applications** に移動し、**Launch Duration** をクリックして、アプリケーションの起動にかかった時間を表示することもできます。また、**Gateway > HDX Insight > Users** に移動して、接続されているすべてのユーザーのユーザーエージェントを表示することもできます。

**注**

HDXインサイトは、ソフトウェアバージョン12.0で実行されているNetScalerインスタンスで構成された管理者パーティションをサポートしています。

次のシンクライアントはHDXインサイトをサポートしています。

- WYSE Windowsベースのシンクライアント
- WYSE Linuxベースのシンクライアント
- WYSE ThinOSベースのシンクライアント
- 10ZiG Ubuntuベースのシンクライアント

## パフォーマンス低下の根本原因の特定

### シナリオ1

ユーザーはCitrix Virtual Apps and Desktopsへのアクセス中に遅延を経験しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

遅延は、サーバーネットワークの遅延、サーバーネットワークによって引き起こされるICAトラフィックの遅延、またはクライアントネットワークの遅延が原因である可能性があります。

問題の根本原因を特定するには、次のメトリックを分析します。

- WAN遅延
- DC遅延
- ホスト遅延

**クライアントメトリックを表示するには：**

1. **Gateway > HDX Insight > Users** に移動します。
2. 下にスクロールしてユーザー名を選択し、リストから期間を選択します。期間は1日、1週間、1か月、またはデータを表示したい期間をカスタマイズすることもできます。
3. チャートには、指定された期間のユーザーのICA RTTとDC遅延値がグラフとして表示されます。



4. 「**現在のセッション**」テーブルで、「**RTT**」値にマウスを合わせ、ホスト遅延、DC遅延、WAN遅延の各値をメモします。
5. 「**現在のセッション**」テーブルで、ホップ図記号をクリックして、クライアントとサーバー間の接続に関する情報（遅延値を含む）を表示します。



**概要**

この例では、「**DC遅延**」は751ミリ秒、「**WAN遅延**」は52ミリ秒、「**ホスト遅延**」は6秒です。これは、ユーザーがサーバーネットワークによって引き起こされる平均遅延のために遅延を経験していることを示しています。

### シナリオ2

ユーザーがCitrix Virtual AppまたはDesktopでアプリケーションを起動する際に遅延が発生しています

遅延は、サーバーネットワーク上の遅延、サーバーネットワークによって引き起こされるICAトラフィックの遅延、クライアントネットワーク上の遅延、またはアプリケーションの起動にかかる時間によって発生する可能性があります。

問題の根本原因を特定するには、次のメトリックを分析します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WAN遅延
- DC遅延
- ホスト遅延

**ユーザーメトリックを表示するには：**

1. **Gateway > HDX Insight > Users** に移動します。
2. 下にスクロールしてユーザー名をクリックします。
3. グラフィカル表示で、特定のセッションのWAN Latency、DC Latency、およびRTT値に注目してください。
4. **Current Sessions** テーブルで、ホスト遅延が高いことに注目してください。



**概要**

この例では、**DC Latency** は1ミリ秒、**WAN latency** は12ミリ秒ですが、**Host Delay** は517ミリ秒です。DCおよびWANの遅延が低いにもかかわらずRTTが高い場合は、ホストサーバー上のアプリケーションエラーを示しています。

**注** HDX Insightは、ソフトウェア11.1ビルド51.21以降を実行しているNetScaler Consoleを使用している場合、WANジッターやサーバー側再送信などのより多くのユーザーメトリックも表示します。これらのメトリックを表示するには、**Gateway > HDX Insight > Users** に移動し、ユーザー名を選択します。ユーザーメトリックはグラフの横のテーブルに表示されます。



## HDX Insightのジオマップ

NetScaler Consoleのジオマップ機能は、さまざまな地理的場所でのアプリケーションの使用状況をマップ上に表示します。管理者はこの情報を使用して、さまざまな地理的場所でのアプリケーション使用状況の傾向を把握できます。

NetScaler Consoleを構成して、特定の地理的場所またはLANのジオマップを表示するには、その場所のプライベートIP範囲（開始IPアドレスと終了IPアドレス）を指定します。

HDX Insightの地理的位置マップから、過去およびアクティブなユーザーの詳細を表示することもできます。**Gateway > HDX Insight** に移動し、マップの **World** セクションで、詳細を表示したい国または地域をクリックします。さらにドリルダウンして、都市や州ごとの情報を表示できます。

**データセンターのジオマップを構成するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

特定の場所のジオマップを構成するには、**Settings > Analytics Settings > IP Blocks** に移動します。

### ユースケース

ABC社が2つの支社（1つはサンタクララ、もう1つはインド）を持っているシナリオを考えてみましょう。

サンタクララのユーザーはSClara.x.comにあるNetScaler Gatewayアプライアンスを使用してVPNトラフィックにアクセスします。インドのユーザーはIndia.x.comにあるNetScaler Gatewayアプライアンスを使用してVPNトラフィックにアクセスします。

特定の時間帯、例えば午前10時から午後5時の間に、サンタクララのユーザーはSClara.x.comに接続してVPNトラフィックにアクセスします。ほとんどのユーザーが同じNetScaler Gatewayにアクセスするため、VPNへの接続に遅延が発生し、一部のユーザーはSClara.x.comの代わりにIndia.x.comに接続します。

トラフィックを分析するNetScaler管理者は、地理マップ機能を使用してサンタクララオフィスのトラフィックを表示できます。マップは、サンタクララオフィスの応答時間が高いことを示しています。これは、サンタクララオフィスにはユーザーがVPNトラフィックにアクセスできるNetScaler Gatewayアプライアンスが1つしかないためです。したがって、管理者は別のNetScaler Gatewayをインストールすることを決定し、ユーザーがVPNにアクセスするためのローカルNetScaler Gatewayアプライアンスを2つ持つようにするかもしれません。

## 制限事項

NetScalerインスタンスがAdvancedライセンスを持っている場合、分析データは1時間しか収集されないため、NetScaler ConsoleでHDX Insightに設定されたしきい値はトリガーされません。

## HDX™ Insight データ収集の有効化

HDX Insightは、NetScalerインスタンスを通過するICAトラフィックに対する前例のないエンドツーエンドの可視性を提供することで、IT部門が優れたユーザーエクスペリエンスを提供できるようにします。また、NetScaler Console Analyticsの一部でもあります。HDX Insightは、ネットワーク、仮想デスクトップ、アプリケーション、およびアプリケーションファブリック向けに、魅力的で強力なビジネスインテリジェンスと障害分析機能を提供します。HDX Insightは、ユーザーの問題を即座にトリアージし、仮想デスクトップ接続に関するデータを収集し、AppFlowレコードを生成して視覚的なレポートとして提示することができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerでデータ収集を有効にするための構成は、展開トポロジにおけるアプライアンスの位置によって異なります。

### LANユーザーモードで展開されたNetScalerを監視するためのデータ収集の有効化

Citrix Virtual App and Desktopアプリケーションにアクセスする外部ユーザーは、NetScaler Gatewayで認証する必要があります。ただし、内部ユーザーはNetScaler Gatewayにリダイレクトされる必要がない場合があります。また、透過モード展開では、管理者はルーティングポリシーを手動で適用して、要求がNetScalerアプライアンスにリダイレクトされるようにする必要があります。

これらの課題を克服し、LANユーザーがCitrix Virtual App and Desktopアプリケーションに直接接続できるように、NetScaler Gatewayアプライアンス上でSOCKSプロキシとして機能するキャッシュリダイレクション仮想サーバーを構成することで、NetScalerアプライアンスをLANユーザーモードで展開できます。

NetScalerをLANユーザーモードで展開(/en-us/netscaler-application-delivery-management-software/media/lan-console.png)

**注:**

NetScaler ConsoleとNetScaler Gatewayアプライアンスは同じサブネット内に存在します。

このモードで展開されたNetScalerアプライアンスを監視するには、まずNetScalerアプライアンスをNetScaler Insightインベントリに追加し、AppFlowを有効にしてから、ダッシュボードでレポートを表示します。

NetScalerアプライアンスをNetScaler Consoleインベントリに追加した後、データ収集のためにAppFlowを有効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

- NetScalerインスタンスでは、**Settings > AppFlow > Collectors** に移動して、コレクター(つまりNetScaler Console) が稼働しているかどうかを確認できます。NetScalerインスタンスは、NSIPを使用してAppFlowレコードをNetScaler Consoleに送信します。しかし、インスタンスはSNIPを使用してNetScaler Consoleとの接続性を検証します。したがって、SNIPがインスタンスに構成されていることを確認してください。
- NetScaler Console構成ユーティリティを使用して、LANユーザーモードで展開されたNetScalerでデータ収集を有効にすることはできません。
- コマンドとその使用方法の詳細については、コマンドリファレンスを参照してください。
- ポリシー式に関する情報については、ポリシーと式を参照してください。

**コマンドラインインターフェイスを使用してNetScalerアプライアンスでデータ収集を構成するには：**

コマンドプロンプトで、以下を実行します。

1. アプライアンスにログオンします。
2. プロキシIPとポートを使用してフォワードプロキシキャッシュリダイレクション仮想サーバーを追加し、サービスタイプをHDXとして指定します。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

例

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

**注：**

NetScaler Gatewayアプライアンスを使用してLANネットワークにアクセスしている場合は、VPNトラフィックに一致するポリシーによって適用されるアクションを追加します。

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add vpn trafficPolicy <name> <rule> <action>
```

例

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. NetScalerアプライアンスにNetScaler ConsoleをAppFlowコレクターとして追加します。

```
add appflow collector <name> -IPAddress <ip_addr>
```

例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. AppFlow®アクションを作成し、コレクターをそのアクションに関連付けます。

```
add appflow action <name> -collectors <string>
```

例：

```
add appflow action act -collectors MyInsight
```

5. トラフィックを生成するためのルールを指定するAppFlowポリシーを作成します。

```
add appflow policy <policyname> <rule> <action>
```

例：

```
add appflow policy pol true act
```

6. AppFlowポリシーをグローバルバインドポイントにバインドします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global <policyname> <priority> -type <type>
```

例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

**注記**

ICA®トラフィックに適用するには、typeの値はICA_REQ_OVERRIDEまたはICA_REQ_DEFAULTである必要があります。

7. AppFlowのflowRecordIntervalパラメーターの値を60秒に設定します。

```
set appflow param -flowRecordInterval 60
```

例:

```
set appflow param -flowRecordInterval 60
```

8. 構成を保存します。タイプ: `save ns config`

### シングルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする

NetScaler Gatewayをシングルホップモードで展開すると、ネットワークのエッジに配置されます。Gatewayインスタンスは、デスクトップ配信インフラストラクチャへのプロキシICA接続を提供します。シングルホップは最もシンプルで一般的な展開です。シングルホップモードは、外部ユーザーが組織内の内部ネットワークにアクセスしようとした場合にセキュリティを提供します。シングルホップモードでは、ユーザーは仮想プライベートネットワーク（VPN）を介してNetScalerアプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler GatewayアプライアンスをNetScaler Consoleインベントリに追加し、NetScaler ConsoleでAppFlowを有効にする必要があります。

**NetScaler ConsoleからAppFlow機能を有効にするには:**

1. Webブラウザーで、NetScaler ConsoleのIPアドレスを入力します（例: `<http://192.168.100.1>`）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。
3. **インフラストラクチャ > インスタンス**に移動し、分析を有効にするNetScalerインスタンスを選択します。
4. **アクションの選択**リストから、**分析の構成**を選択します。
5. VPN仮想サーバーを選択し、**分析を有効にする**をクリックします。
6. **HDX Insight**を選択し、次に**ICA**を選択します。
7. 「**OK**」をクリックします。

「

**注**

」

シングルホップモードでAppFlowを有効にすると、以下のコマンドがバックグラウンドで実行されます。これらのコマンドは、トラブルシューティングの目的でここに明示的に指定されています。

```
-  add appflow collector <name> -IPAddress <ip_addr>


-  add appflow action <name> -collectors <string>


-  set appflow param -flowRecordInterval <secs>


-  disable ns feature AppFlow


-  enable ns feature AppFlow


-  add appflow policy <name> <rule> <expression>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  set appflow policy <name> -rule <expression>


-  bind vpn vserver <vsname> -policy <string> -type <type> -priority
<positive_integer>


-  set vpn vserver <name> -appflowLog ENABLED


-  save ns config
```

EUEM仮想チャネルデータは、NetScaler ConsoleがGatewayインスタンスから受信するHDX Insightデータの一部です。EUEM仮想チャネルはICA RTTに関するデータを提供します。EUEM仮想チャネルが有効になっていない場合でも、残りのHDX InsightデータはNetScaler Consoleに表示されます。

### ダブルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする

NetScaler Gatewayのダブルホップモードは、攻撃者がセキュアなネットワーク内のサーバーに到達するために複数のセキュリティゾーンまたは非武装地帯（DMZ）を突破する必要があるため、組織の内部ネットワークに追加の保護を提供します。ICA接続が通過するホップ数（NetScaler Gatewayアプライアンス）と、各TCP接続の遅延の詳細、およびそれがクライアントによって認識される総ICA遅延に対してどの程度であるかを分析したい場合は、NetScaler Consoleをインストールして、NetScaler Gatewayアプライアンスがこれらの重要な統計情報を報告するようにする必要があります。

分析を有効にする(/en-us/netscaler-application-delivery-management-software/media/double-hop-2.png)

最初のDMZにあるNetScaler Gatewayは、ユーザー接続を処理し、SSL VPNのセキュリティ機能を実行します。このNetScaler Gatewayは、ユーザー接続を暗号化し、ユーザーがどのように認証されるかを決定し、内部ネットワーク内のサーバーへのアクセスを制御します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2番目のDMZにあるNetScaler Gatewayは、NetScaler Gatewayプロキシデバイスとして機能します。このNetScaler Gatewayは、ICAトラフィックが2番目のDMZを通過して、サーバーファームへのユーザー接続を完了できるようにします。

NetScaler Consoleは、最初のDMZにあるNetScaler Gatewayアプライアンスに属するサブネット、または2番目のDMZにあるNetScaler Gatewayアプライアンスに属するサブネットのいずれかに展開できます。上記の画像では、NetScaler Consoleと最初のDMZにあるNetScaler Gatewayは同じサブネットに展開されています。

ダブルホップモードでは、NetScaler Consoleは一方のアプライアンスからTCPレコードを収集し、もう一方のアプライアンスからICAレコードを収集します。NetScaler Gatewayアプライアンスを NetScaler Consoleインベントリに追加し、データ収集を有効にすると、各アプライアンスはホップカウントと接続チェーンIDを追跡してレポートをエクスポートします。

NetScaler ConsoleがどのNetScaler Gatewayアプライアンスがレコードをエクスポートしているかを識別できるように、各アプライアンスにはホップカウントが指定され、各接続には接続チェーンIDが指定されます。ホップカウントは、クライアントからサーバーへのトラフィックが流れるNetScaler Gatewayアプライアンスの数を表します。接続チェーンIDは、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler Consoleは、ホップカウントと接続チェーンIDを使用して、両方のNetScaler Gatewayアプライアンスからのデータを関連付け、レポートを生成します。

このモードで展開されたNetScaler Gatewayアプライアンスを監視するには、まずNetScaler GatewayをNetScaler Consoleインベントリに追加し、NetScaler ConsoleでAppFlowを有効にしてから、NetScaler Consoleダッシュボードでレポートを表示する必要があります。

### Optimal Gatewayに使用される仮想サーバーでHDX Insightを構成する

Optimal Gatewayで使用される仮想サーバーでHDX Insightを構成する手順：

1. **Infrastructure > Instances** に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. **Select Action** リストから、**Configure Analytics** を選択します。
3. 認証用に構成されたVPN仮想サーバーを選択し、**Enable Analytics** をクリックします。
4. **HDX Insight** を選択し、次に **ICA** を選択します。
5. 必要に応じて、その他の詳細オプションを選択します。
6. **OK** をクリックします。
7. 他のVPN仮想サーバーで手順3から6を繰り返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Consoleでのデータ収集を有効にする

NetScaler Consoleで両方のアプライアンスからICA詳細の収集を開始するように設定すると、収集される詳細は冗長になります。つまり、両方のアプライアンスが同じメトリックを報告します。この状況を回避するには、最初のNetScaler Gatewayアプライアンスの1つでICAのAppFlowを有効にし、次に2番目のアプライアンスでTCPのAppFlowを有効にする必要があります。これにより、一方のアプライアンスはICA AppFlowレコードをエクスポートし、もう一方のアプライアンスはTCP AppFlowレコードをエクスポートします。これにより、ICAトラフィックの解析にかかる処理時間も節約されます。

### NetScaler ConsoleからAppFlow機能を有効にするには：

1. Webブラウザで、NetScaler ConsoleのIPアドレスを入力します（例：`<http://192.168.100.1>`）。
2. **User Name** と **Password** に、管理者資格情報を入力します。
3. **Infrastructure > Instances** に移動し、分析を有効にするNetScalerインスタンスを選択します。
4. **Select Action** リストから、**Configure Analytics** を選択します。
5. VPN仮想サーバーを選択し、 をクリックします。
6. を選択し、ICAトラフィックまたはTCPトラフィックに対してそれぞれ または を選択します。

   **注**

   NetScalerアプライアンスでそれぞれのサービスまたはサービスグループに対してAppFlowロギングが有効になっていない場合、Insight列に「Enabled」と表示されていても、NetScaler Consoleダッシュボードにはレコードが表示されません。

7. をクリックします。

### NetScaler Gatewayアプライアンスのデータエクスポート設定

NetScaler Gatewayアプライアンスをインストールしたら、レポートをNetScaler Consoleにエクスポートするために、NetScaler Gatewayアプライアンスで次の設定を行う必要があります。

- 最初のDMZと2番目のDMZにあるNetScaler Gatewayアプライアンスの仮想サーバーが相互に通信するように構成します。
- 2番目のDMZにあるNetScaler Gateway仮想サーバーを、最初のDMZにあるNetScaler Gateway仮想サーバーにバインドします。
- 2番目のDMZにあるNetScaler Gatewayでダブルホップを有効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 2番目のDMZにあるNetScaler Gateway仮想サーバーで認証を無効にします。
- いずれかのNetScaler Gatewayアプライアンスで ICAレコードのエクスポートを有効にします
- もう一方のNetScaler Gatewayアプライアンスで TCPレコードのエクスポートを有効にします。
- 両方のNetScaler Gatewayアプライアンスで接続チェイニングを有効にします。

**コマンドラインインターフェイスを使用したNetScaler Gatewayの構成:**

1. 最初のDMZにあるNetScaler Gateway仮想サーバーが、2番目のDMZにあるNetScaler Gateway仮想サーバーと通信するように構成します。

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON or
OFF)] [-imgGifToPng]



add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. 2番目のDMZにあるNetScaler Gateway仮想サーバーを、最初のDMZにあるNetScaler Gateway仮想サーバーにバインドします。最初のDMZにあるNetScaler Gatewayで次のコマンドを実行します。

```
bind vpn vserver <name> -nextHopServer <name>



bind vpn vserver vs1 -nextHopServer nh1
```

3. 2番目のDMZにあるNetScaler Gatewayで、ダブルホップとAppFlowを有効にします。

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
 appflowLog ( ENABLED or DISABLED )]



set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. 2番目のDMZにあるNetScaler Gateway仮想サーバーで認証を無効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn vserver <name> [-authentication (ON or OFF)]



set vpn vserver vs -authentication OFF
```

5. いずれかのNetScaler Gatewayアプライアンスで TCPレコードのエクスポートを有効にします。

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
OTHERTCP_REQUEST
```

6. もう一方のNetScaler Gatewayアプライアンスで ICAレコードのエクスポートを有効にします。

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA_REQUEST
```

7. 両方のNetScaler Gatewayアプライアンスで接続チェーンを有効にします。

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]



set appflow param -connectionChaining ENABLED
```

**構成ユーティリティを使用してNetScaler Gatewayを構成する:**

1. 最初のDMZにあるNetScaler Gatewayが2番目のDMZにあるNetScaler Gatewayと通信するように構成し、2番目のDMZにあるNetScaler Gatewayを最初のDMZにあるNetScaler Gatewayにバインドします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 「**構成**」タブで「**NetScaler Gateway**」を展開し、「**仮想サーバー**」をクリックします。
b. 右側のペインで仮想サーバーをダブルクリックし、Advancedグループで「**公開済みアプリケーション**」を展開します。
c. 「**ネクストホップサーバー**」をクリックし、ネクストホップサーバーを2番目のNetScaler Gatewayアプライアンスにバインドします。

2. 2番目のDMZにあるNetScaler Gatewayでダブルホップを有効にします。
   a. 「**構成**」タブで「**NetScaler Gateway**」を展開し、「**仮想サーバー**」をクリックします。
   b. 右側のペインで仮想サーバーをダブルクリックし、「**基本設定**」グループで編集アイコンをクリックします。
   c. 「その他」を展開し、「**Double Hop**」を選択して「**OK**」をクリックします。
3. 2番目のDMZにあるNetScaler Gatewayの仮想サーバーで認証を無効にします。
   a. 「**Configuration**」タブで「**NetScaler Gateway**」を展開し、「**Virtual Servers**」をクリックします。
   b. 右ペインで仮想サーバーをダブルクリックし、「**Basic Settings**」グループで編集アイコンをクリックします。
   c. 「**More**」を展開し、「**Enable Authentication**」のチェックを外します。
4. いずれかのNetScaler GatewayアプライアンスでTCPレコードをエクスポートできるようにします。
   a. 「**Configuration**」タブで「**NetScaler Gateway**」を展開し、「**Virtual Servers**」をクリックします。
   b. 右ペインで仮想サーバーをダブルクリックし、「Advanced」グループで「Policies」を展開します。
   c. 「+」アイコンをクリックし、「**Choose Policy**」リストから「**AppFlow**」を、「**Choose Type**」リストから「**Other TCP Request**」を選択します。
   d. 「**Continue**」をクリックします。
   e. ポリシーバインディングを追加し、「**Close**」をクリックします。
5. もう一方のNetScaler GatewayアプライアンスでICAレコードをエクスポートできるようにします。
   a. 「**Configuration**」タブで「**NetScaler Gateway**」を展開し、「**Virtual Servers**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 右ペインで仮想サーバーをダブルクリックし、「**Advanced**」グループで、「**Policies**」を展開します。

c. 「+」アイコンをクリックし、「**Choose Policy**」リストから「AppFlow」を、「Choose Type」リストから「**Other TCP Request**」を選択します。

d. 「**続行**」をクリックします。

e. ポリシーバインディングを追加し、「**閉じる**」をクリックします。

6. 両方のNetScaler Gatewayアプライアンスで接続チェイニングを有効にします。

a. 「**Configuration**」タブで、「**System**」>「**Appflow**」の順に移動します。

b. 右ペインの「**Settings**」グループで、「**Change Appflow Settings**」をダブルクリックします。

c. 「**Connection Chaining**」を選択し、「**OK**」をクリックします。

7. 最初のDMZにあるNetScaler Gatewayを、2番目のDMZにあるNetScaler Gatewayと通信するように構成し、2番目のDMZにあるNetScaler Gatewayを最初のDMZにあるNetScaler Gatewayにバインドします。

a. Configurationタブで、「**NetScaler Gateway**」を展開し、「**Virtual Servers**」をクリックします。

b. 右ペインで仮想サーバーをダブルクリックし、「**Advanced group**」で「**Published Applications**」を展開します。

c. 「**Next Hop Server**」をクリックし、2番目のNetScaler Gatewayアプライアンスにネクストホップサーバーをバインドします。

8. 2番目のDMZにあるNetScaler Gatewayでダブルホップを有効にします。

a. Configurationタブで、「**NetScaler Gateway**」を展開し、「**Virtual Servers**」をクリックします。

b. 右ペインで仮想サーバーをダブルクリックし、「**Basic Settings**」グループで編集アイコンをクリックします。

c. 「More」を展開し、「**Double Hop**」を選択して「**OK**」をクリックします。

9. 2番目のDMZにあるNetScaler Gatewayの仮想サーバーで認証を無効にします。

a. 「構成」タブで NetScaler Gateway を展開し、**仮想サーバー**をクリックします。

b. 右側のペインで仮想サーバーをダブルクリックし、**基本設定**グループで編集アイコンをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **詳細**を展開し、**認証を有効にする**のチェックを外します。

10. いずれかの NetScaler Gateway アプライアンスで TCP レコードのエクスポートを有効にします。

a. 「構成」タブで **NetScaler Gateway** を展開し、**仮想サーバー**をクリックします。

b. 右側のペインで仮想サーバーをダブルクリックし、詳細グループで**ポリシー**を展開します。

c. **+**アイコンをクリックし、「ポリシーの選択」リストから「AppFlow」を選択し、「**種類の選択**」リストから「**その他の TCP 要求**」を選択します。

d. **続行**をクリックします。

e. ポリシーバインディングを追加し、**閉じる**をクリックします。

11. もう一方の NetScaler Gateway アプライアンスで ICA レコードのエクスポートを有効にします。

a. 「構成」タブで **NetScaler Gateway** を展開し、**仮想サーバー**をクリックします。

b. 右側のペインで仮想サーバーをダブルクリックし、詳細グループで**ポリシー**を展開します。

c. **+**アイコンをクリックし、「**ポリシーの選択**」リストから「AppFlow」を選択し、「**種類の選択**」リストから「**その他の TCP 要求**」を選択します。

d. **続行**をクリックします。

e. ポリシーバインディングを追加し、**閉じる**をクリックします。

12. 両方のNetScaler Gatewayアプライアンスで接続チェイニングを有効にします。

### トランスペアレントモードで展開されたNetScalerを監視するためのデータ収集を有効にする

NetScalerがトランスペアレントモードで展開されている場合、クライアントは介在する仮想サーバーなしでサーバーに直接アクセスできます。NetScalerアプライアンスがCitrix Virtual Apps and Desktop環境でトランスペアレントモードで展開されている場合、ICAトラフィックはVPN経由で送信されません。

NetScalerをNetScaler Consoleインベントリに追加した後、データ収集のためにAppFlowを有効にする必要があります。データ収集の有効化は、デバイスとモードによって異なります。その場合、各NetScalerアプライアンスにAppFlowコレクターとしてを追加し、アプライア

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンスを通過するすべてのICAトラフィックまたは特定のICAトラフィックを収集するように AppFlowポリシーを構成する必要があります。

**注**

- NetScaler Console構成ユーティリティを使用して、トランスペアレントモードで展開されたNetScalerでデータ収集を有効にすることはできません。
- コマンドとその使用法に関する詳細については、コマンドリファレンスを参照してください。
- ポリシー式に関する情報については、ポリシーと式を参照してください。

次の図は、NetScalerがトランスペアレントモードで展開されている場合のNetScaler Consoleのネットワーク展開を示しています。

**コマンドラインインターフェイスを使用してNetScalerアプライアンスでデータ収集を構成するには：**

コマンドプロンプトで、次の操作を行います。

1. アプライアンスにログオンします。
2. NetScalerアプライアンスがトラフィックをリッスンするICAポートを指定します。

```
set ns param --icaPorts <port>...
```

**例：**

```
set ns param -icaPorts 2598 1494
```

**注**

- このコマンドで最大10個のポートを指定できます。
- デフォルトのポート番号は2598です。必要に応じてポート番号を変更できます。

3. NetScalerアプライアンスにAppFlowコレクターとしてNetScaler Insight Centerを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow collector <name> -IPAddress <ip_addr>
```

**例:**

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

**注** NetScalerアプライアンスで構成されているAppFlowコレクターを表示するには、**show appflow collector**コマンドを使用します。

4. AppFlowアクションを作成し、コレクターをそのアクションに関連付けます。

```
add appflow action <name> -collectors <string> ...
```

**例:**

AppFlow アクション act-collectors MyInsight を追加

5. トラフィックを生成するためのルールを指定するAppFlowポリシーを作成します。

```
add appflow policy <policyname> <rule> <action>
```

**例:**

```
add appflow policy pol true act
```

6. AppFlowポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global <policyname> <priority> -type <type>
```

**例:**

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

**注**

ICAトラフィックに適用するには、**type**の値はICA_REQ_OVERRIDEまたはICA_REQ_DEFAULTである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. AppFlow の flowRecordInterval パラメータの値を 60 秒に設定します。

```
set appflow param -flowRecordInterval 60
```

**例:**

```
set appflow param -flowRecordInterval 60
```

8. 設定を保存します。入力: `save ns config`

### シングルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする

NetScaler Gateway をシングルホップモードで展開すると、ネットワークのエッジに配置されます。Gateway インスタンスは、デスクトップ配信インフラストラクチャへのプロキシ ICA 接続を提供します。シングルホップは最もシンプルで一般的な展開です。シングルホップモードは、外部ユーザーが組織内の内部ネットワークにアクセスしようとした場合にセキュリティを提供します。シングルホップモードでは、ユーザーは仮想プライベートネットワーク (VPN) を介して NetScaler アプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler GatewayアプライアンスをNetScaler Consoleインベントリに追加し、NetScaler ConsoleでAppFlowを有効にする必要があります。

シングルホップ(/en-us/netscaler-application-delivery-management-software/media/single-hop-2.png)

**NetScaler ConsoleからAppFlow機能を有効にするには：**

1. **Infrastructure** \> **Instances** に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. **Action** リストから、**Enable/Disable Insight** を選択します。
3. **VPN virtual servers** を選択し、**Enable AppFlow®** をクリックします。
4. **Enable AppFlow** フィールドに「**true**」と入力し、**ICA®** を選択します。
5. **OK** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

シングルホップモードでAppFlowを有効にすると、以下のコマンドがバックグラウンドで実行されます。これらのコマンドは、トラブルシューティングの目的でここに明示的に記載されています。

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

EUEM仮想チャネルデータは、NetScaler ConsoleがGatewayインスタンスから受信するHDX Insightデータの一部です。EUEM仮想チャネルは、ICA RTTに関するデータを提供します。EUEM仮想チャネルが有効になっていない場合でも、残りのHDX InsightデータはNetScaler Consoleに引き続き表示されます。

### トランスペアレントモードで展開されたNetScalerを監視するためのデータ収集を有効にする

NetScalerがトランスペアレントモードで展開されている場合、クライアントは仮想サーバーを介さずに直接サーバーにアクセスできます。Citrix Virtual Apps and Desktops環境でNetScalerがトランスペアレントモードで展開されている場合、ICAトラフィックはVPN経由で送信されません。

NetScalerをNetScaler Consoleインベントリに追加した後、データ収集のためにAppFlowを有効にする必要があります。データ収集の有効化は、デバイスとモードによって異なります。その場合、各NetScalerインスタンスにNetScaler ConsoleをAppFlowコレクターとして追加し、アプライアンスを通過するすべてのICAトラフィックまたは特定のICAトラフィックを収集するようにAppFlowポリシーを構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

- NetScaler Console構成ユーティリティを使用して、トランスペアレントモードで展開されたNetScalerでデータ収集を有効にすることはできません。
- コマンドとその使用法に関する詳細については、「コマンドリファレンス」を参照してください。
- ポリシー式に関する情報については、「ポリシーと式」を参照してください。

次の図は、NetScalerがトランスペアレントモードで展開されている場合のNetScaler Consoleのネットワーク展開を示しています。



**コマンドラインインターフェイスを使用してNetScalerアプライアンスでデータ収集を構成するには：**

コマンドプロンプトで、次の操作を行います。

1. アプライアンスにログオンします。
2. NetScalerアプライアンスがトラフィックをリッスンするICAポートを指定します。

   ```
   set ns param --icaPorts \<port\>...
   ```

   **例：**

   ```
   set ns param -icaPorts 2598 1494
   ```

   **注**

   - このコマンドで最大10個のポートを指定できます。
   - デフォルトのポート番号は2598です。必要に応じてポート番号を変更できます。

3. NetScalerインスタンスにNetScaler Insight CenterをAppFlowコレクターとして追加します。

   ```
   add appflow collector <name> -IPAddress <ip_addr>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**例:**

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

**注:** NetScalerインスタンスで構成されているAppFlowコレクターを表示するには、**show appflow collector**コマンドを使用します。

4. AppFlow®アクションを作成し、コレクターをそのアクションに関連付けます。

```
add appflow action <name> -collectors <string> ...
```

**例:**

```
add appflow action act -collectors MyInsight
```

5. トラフィック生成のルールを指定するAppFlowポリシーを作成します。

```
add appflow policy <policyname> <rule> <action>
```

**例:**

```
add appflow policy pol true act
```

6. AppFlowポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global <policyname> <priority> -type <type>
```

**例:**

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

**注**

ICA®トラフィックに適用するには、**type**の値がICA_REQ_OVERRIDEまたはICA_REQ_DEFAULTである必要があります。

7. AppFlowのflowRecordIntervalパラメーターの値を60秒に設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set appflow param -flowRecordInterval 60
```

8. 構成を保存します。

```
save ns config
```

### ダブルホップモードで展開されたNetScaler Gatewayアプライアンスのデータ収集を有効にする

NetScaler Gatewayのダブルホップモードは、組織の内部ネットワークに追加の保護を提供します。これは、攻撃者がセキュアなネットワーク内のサーバーに到達するために、複数のセキュリティゾーンまたは非武装地帯（DMZ）を突破する必要があるためです。ICA接続が通過するホップ数（NetScaler Gatewayアプライアンス）を分析し、各TCP接続の遅延の詳細と、それがクライアントによって認識される総ICA遅延に対してどのように機能するかを知りたい場合は、NetScaler Gatewayアプライアンスがこれらの重要な統計情報を報告できるように、NetScaler Consoleをインストールする必要があります。

図3. ダブルホップモードで展開されたNetScaler Console



最初のDMZにあるNetScaler Gatewayは、ユーザー接続を処理し、SSL VPNのセキュリティ機能を実行します。このNetScaler Gatewayは、ユーザー接続を暗号化し、ユーザーがどのように認証されるかを決定し、内部ネットワーク内のサーバーへのアクセスを制御します。

2番目のDMZにあるNetScaler Gatewayは、NetScaler Gatewayプロキシデバイスとして機能します。このNetScaler Gatewayは、ICAトラフィックが2番目のDMZを通過して、サーバーファームへのユーザー接続を完了できるようにします。

NetScaler Consoleは、最初のDMZにあるNetScaler Gatewayアプライアンスに属するサブネット、または2番目のDMZにあるNetScaler Gatewayアプライアンスに属するサブネットのいずれかに展開できます。上の画像では、NetScaler Consoleと最初のDMZにあるNetScaler Gatewayは同じサブネットに展開されています。

ダブルホップモードでは、NetScaler Consoleは一方のアプライアンスからTCPレコードを収集し、もう一方のアプライアンスからICAレコードを収集します。NetScaler GatewayアプライアンスをNetScaler Consoleインベントリに追加し、データ収集を有効にすると、各アプライアンスはホップ数と接続チェーンIDを追跡してレポートをエクスポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ConsoleがどのNetScaler Gatewayアプライアンスがレコードをエクスポートしているかを識別できるように、各アプライアンスにはホップ数が指定され、各接続には接続チェーンIDが指定されます。ホップ数は、クライアントからサーバーへのトラフィックが流れるNetScaler Gatewayアプライアンスの数を表します。接続チェーンIDは、クライアントとサーバー間のエンドツーエンド接続を表します。

NetScaler Consoleは、ホップ数と接続チェーンIDを使用して、両方のNetScaler Gatewayアプライアンスからのデータを関連付け、レポートを生成します。

このモードで展開されたNetScaler Gatewayアプライアンスを監視するには、まずNetScaler GatewayをNetScaler Consoleインベントリに追加し、NetScaler ConsoleでAppFlowを有効にし、その後、NetScaler Consoleダッシュボードでレポートを表示する必要があります。

### NetScaler Consoleでデータ収集を有効にする

両方のアプライアンスからICA詳細の収集を開始するようにNetScaler Consoleを有効にすると、収集される詳細は冗長になります。つまり、両方のアプライアンスが同じメトリックを報告します。この状況を克服するには、最初のNetScaler GatewayアプライアンスのいずれかでTCPのAppFlowを有効にし、次に2番目のアプライアンスでICAのAppFlowを有効にする必要があります。そうすることで、一方のアプライアンスはICA AppFlowレコードをエクスポートし、もう一方のアプライアンスはTCP AppFlowレコードをエクスポートします。これにより、ICAトラフィックの解析にかかる処理時間も節約されます。

### NetScaler ConsoleからAppFlow機能を有効にするには：

1. **>** に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. 「**アクション**」リストから、「**Insight の有効化/無効化**」を選択します。
3. VPN仮想サーバーを選択し、「**AppFlow® を有効にする**」をクリックします。
4. 「**AppFlow を有効にする**」フィールドに「**true**」と入力し、ICAトラフィックとTCPトラフィックに対してそれぞれ「**ICA/TCP**」を選択します。

   **注**

   NetScalerアプライアンス上のサービスまたはサービスグループでAppFlowロギングが有効になっていない場合、Insight列に「有効」と表示されていても、NetScaler Consoleダッシュボードにはレコードが表示されません。

5. 「**OK**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### データをエクスポートするようにNetScaler Gatewayアプライアンスを構成する

NetScaler Gatewayアプライアンスをインストールした後、レポートをNetScaler Consoleにエクスポートするには、NetScaler Gatewayアプライアンスで次の設定を構成する必要があります。

- 最初のDMZと2番目のDMZにあるNetScaler Gatewayアプライアンスの仮想サーバーが相互に通信するように構成します。
- 2番目のDMZにあるNetScaler Gateway仮想サーバーを、最初のDMZにあるNetScaler Gateway仮想サーバーにバインドします。
- 2番目のDMZにあるNetScaler Gatewayでダブルホップを有効にします。
- 2番目のDMZにあるNetScaler Gateway仮想サーバーで認証を無効にします。
- いずれかのNetScaler GatewayアプライアンスでICAレコードのエクスポートを有効にします
- もう一方のNetScaler GatewayアプライアンスでTCPレコードのエクスポートを有効にします。
- 両方のNetScaler Gatewayアプライアンスで接続チェイニングを有効にします。

### コマンドラインインターフェイスを使用してNetScaler Gatewayを構成する:

1. 最初のDMZにあるNetScaler Gateway仮想サーバーが、2番目のDMZにあるNetScaler Gateway仮想サーバーと通信するように構成します。

   **VPNネクストホップサーバーを追加** \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure**(ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

2. 2番目のDMZにあるNetScaler Gateway仮想サーバーを、最初のDMZにあるNetScaler Gateway仮想サーバーにバインドします。最初のDMZにあるNetScaler Gatewayで次のコマンドを実行します。

   **VPN仮想サーバーをバインド** \<name\> **-nextHopServer** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. 2番目のDMZにあるNetScaler Gatewayで、ダブルホップとAppFlowを有効にします。

   **set vpn vserver** \<name\> \[**- doubleHop** ( 有効 |無効 )\] \[**- appflowLog** ( 有効 |無効 )\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 2番目のDMZにあるNetScaler Gateway仮想サーバーで認証を無効にします。

   **set vpn vserver**\<name\> \[**-authentication** (オン|オフ)\]

   ```
   set vpn vserver vs -authentication OFF
   ```

5. いずれかのNetScaler Gatewayアプライアンスで TCPレコードのエクスポートを有効にします。

   **bind vpn vserver**\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \
   [**-type**\<type\>\]

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
   ```

6. もう一方のNetScaler Gatewayアプライアンスで ICAレコードのエクスポートを有効にします。

   **bind vpn vserver**\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \
   [**-type**\<type\>\]

   ```
   bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA\_REQUEST
   ```

7. 両方のNetScaler Gatewayアプライアンスで接続チェーンを有効にします。

   **appFlow パラメータを設定** \[**-connectionChaining** (ENABLED|DISABLED)\]

   ```
   set appflow param -connectionChaining ENABLED
   ```

**構成ユーティリティを使用したNetScaler Gatewayの構成：**

1. 最初のDMZにあるNetScaler Gatewayを、2番目のDMZにあるNetScaler Gatewayと通信するように構成し、2番目のDMZにあるNetScaler Gatewayを最初のDMZにあるNetScaler Gatewayにバインドします。

   a. **Configuration**タブで**NetScaler Gateway**を展開し、**Virtual Servers**をクリックします。

   b. 右側のペインで仮想サーバーをダブルクリックし、Advancedグループで**Published Applications**を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **Next Hop Server**をクリックし、2番目のNetScaler Gatewayアプライアンスにネクストホップサーバーをバインドします。

2. 2番目のDMZにあるNetScaler Gatewayでダブルホップを有効にします。

a. **Configuration**タブで**NetScaler Gateway**を展開し、**Virtual Servers**をクリックします。

b. 右側のペインで仮想サーバーをダブルクリックし、**Basic Settings**グループで編集アイコンをクリックします。

c. **More**を展開し、**Double Hop**を選択して**OK**をクリックします。

3. 2番目のDMZにあるNetScaler Gatewayの仮想サーバーで認証を無効にします。

a. **Configuration**タブで**NetScaler Gateway**を展開し、**Virtual Servers**をクリックします。

b. 右側のペインで仮想サーバーをダブルクリックし、**Basic Settings**グループで編集アイコンをクリックします。

c. **More**を展開し、**Enable Authentication**のチェックを外します。

4. いずれかのNetScaler GatewayアプライアンスでTCPレコードのエクスポートを有効にします。

a. **Configuration**タブで**NetScaler Gateway**を展開し、**Virtual Servers**をクリックします。

b. 右ペインで仮想サーバーをダブルクリックし、グループでを展開します。

c. +アイコンをクリックし、リストからを選択し、ドロップダウンリストからを選択します。

d. をクリックします。

e. ポリシーバインディングを追加し、をクリックします。

5. 他のNetScaler GatewayアプライアンスでICAレコードのエクスポートを有効にします。

a. タブでを展開し、をクリックします。

b. 右ペインで仮想サーバーをダブルクリックし、グループでを展開します。

c. +アイコンをクリックし、ドロップダウンリストからを選択し、ドロップダウンリストからを選択します。

d. をクリックします。

e. ポリシーバインディングを追加し、をクリックします。

6. 両方のNetScaler Gatewayアプライアンスで接続チェーンを有効にします。

a. タブで、に移動します。

b. 右ペインのグループで、をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. を選択し、をクリックします。

### LANユーザーモードで展開されたNetScalerを監視するためのデータ収集を有効にする

Citrix Virtual AppまたはDesktopアプリケーションにアクセスする外部ユーザーは、NetScaler Gatewayで認証する必要があります。ただし、内部ユーザーはNetScaler Gatewayにリダイレクトされる必要がない場合があります。また、透過モード展開では、リクエストがNetScalerアプライアンスにリダイレクトされるように、管理者はルーティングポリシーを手動で適用する必要があります。

これらの課題を克服し、LANユーザーがCitrix Virtual Apps and Desktopsアプリケーションに直接接続できるように、NetScaler GatewayアプライアンスでSOCKSプロキシとして機能するキャッシュリダイレクション仮想サーバーを構成することで、NetScalerアプライアンスをLANユーザーモードで展開できます。

図4. LANユーザーモードで展開されたNetScaler Console

LANユーザーモード(/en-us/netscaler-application-delivery-management-software/media/lan-console.png)

**注** NetScaler ConsoleとNetScaler Gatewayアプライアンスは同じサブネットに存在します。

このモードで展開されたNetScalerアプライアンスを監視するには、まずNetScalerアプライアンスをNetScaler Insightインベントリに追加し、AppFlowを有効にしてから、ダッシュボードでレポートを表示します。

NetScalerアプライアンスをNetScaler Consoleインベントリに追加した後、データ収集のためにAppFlowを有効にする必要があります。

**注**

- NetScaler Console構成ユーティリティを使用して、LANユーザーモードで展開されたNetScalerでデータ収集を有効にすることはできません。
- コマンドとその使用法に関する詳細情報については、「コマンドリファレンス」を参照してください。
- ポリシー式に関する情報については、「ポリシーと式」を参照してください。

**コマンドラインインターフェイスを使用してNetScalerアプライアンスでデータ収集を構成するには:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コマンドプロンプトで、次の操作を行います:

1. アプライアンスにログオンします。
2. プロキシIPとポートを持つフォワードプロキシキャッシュリダイレクション仮想サーバーを追加し、サービスタイプをHDXとして指定します。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

**例:**

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

**注:**

NetScaler Gatewayアプライアンスを使用してLANネットワークにアクセスしている場合は、VPNトラフィックに一致するポリシーによって適用されるアクションを追加します。

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]



add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

**例:**

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. NetScalerアプライアンスにAppFlowコレクターとしてNetScaler Consoleを追加します。

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
```

**例:**

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. AppFlow®アクションを作成し、コレクターをそのアクションに関連付けます。

```
add appflow action** \<name\> **-collectors** \<string\> ...
```

**例:**

```
add appflow action act -collectors MyInsight
```

5. トラフィックを生成するためのルールを指定するAppFlowポリシーを作成します。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

**例:**

```
add appflow policy pol true act
```

6. AppFlowポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global** \<policyname\> \<priority\> **-type** \<type\>
```

**例:**

```
bind appflow global pol 1 -type ICA\_REQ\_DEFAULT
```

**注:**

ICAトラフィックに適用するには、typeの値がICA_REQ_OVERRIDEまたはICA_REQ_DEFAULTである必要があります。

7. AppFlowのflowRecordIntervalパラメーターの値を60秒に設定します。

```
set appflow param -flowRecordInterval 60
```

**例：**

```
set appflow param -flowRecordInterval 60
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 設定を保存します。

```
save ns config
```

## HDX™ Insight のしきい値を作成し、アラートを設定する

NetScaler Console の HDX Insight を使用すると、NetScaler インスタンスを通過する HDX トラフィックを監視できます。NetScaler Console では、Insight トラフィックの監視に使用されるさまざまなカウンタにしきい値を設定できます。また、NetScaler Console でルールを設定し、アラートを作成することもできます。

HDX トラフィックタイプは、アプリケーション、デスクトップ、ゲートウェイ、ライセンス、ユーザーなど、さまざまなエンティティに関連付けられています。各エンティティには、それぞれに関連付けられた異なるメトリックを含めることができます。たとえば、アプリケーションエンティティは、さまざまなヒット数、アプリケーションによって消費される帯域幅、およびサーバーの応答時間に関連付けられています。ユーザーエンティティは、WAN レイテンシ、DC レイテンシ、ICA® RTT、およびユーザーによって消費される帯域幅に関連付けることができます。

NetScaler Console の HDX Insight のしきい値管理により、設定されたしきい値が侵害されたときに、プロアクティブにルールを作成し、アラートを設定できました。現在、このしきい値管理は、しきい値ルールのグループを設定するように拡張されています。個々のルールではなく、グループを監視できるようになりました。しきい値ルールグループは、ユーザー、アプリケーション、デスクトップなどのエンティティから選択されたメトリックに対する1つ以上のユーザー定義のしきい値ルールで構成されます。各ルールは、ルール作成時に入力する期待値に対して監視されます。ユーザーエンティティの場合、しきい値グループは地理的位置にも関連付けることができます。

NetScaler Console でアラートが生成されるのは、設定されたしきい値グループ内のすべてのルールが侵害された場合のみです。たとえば、合計セッション起動数とアプリケーション起動数の両方でアプリケーションを1つのしきい値グループとして監視できます。両方のルールが侵害された場合にのみアラートが生成されます。これにより、エンティティに対してより現実的なしきい値を設定できます。

いくつかの例を次に示します。

- しきい値ルール1：ユーザー（エンティティ）のICA RTT（メトリック）は \<= 100 ms である必要があります
- しきい値ルール2：ユーザー（エンティティ）のWANレイテンシ（メトリック）は \<= 100 ms である必要があります

© 1997–2026 Citrix Systems, Inc. All rights reserved.

しきい値グループの例は次のとおりです：{しきい値ルール1 + しきい値ルール2}

ルールを作成するには、まず監視するエンティティを選択する必要があります。次に、ルール作成時にメトリックを選択します。たとえば、アプリケーションエンティティを選択し、合計セッション起動数またはアプリ起動数を選択できます。エンティティとメトリックのすべての組み合わせに対して1つのルールを作成できます。提供されている比較演算子 (\>、\<、\>=、および \<=) を使用し、各メトリックのしきい値を入力します。

**注**

単一のグループで複数のエンティティを監視したくない場合は、各エンティティに対して個別のしきい値ルールグループを作成する必要があります。

カウンタの値がしきい値を超えると、NetScaler Console はしきい値違反を示すイベントを生成し、各イベントに対してアラートが作成されます。

アラートの受信方法を設定する必要があります。NetScaler Console にアラートを表示したり、モバイルデバイスで電子メールまたはSMSとしてアラートを受信したりできます。後者の2つのアクションについては、NetScaler Console で電子メールサーバーまたはSMSサーバーを設定する必要があります。

しきい値グループは、ユーザーエンティティの地理固有の監視のために、地理的位置にバインドすることもできます。

### 使用例

ABC Inc.は50か国以上にオフィスを持つグローバル企業です。同社はシンガポールとカリフォルニアにそれぞれ1つずつ、Citrix Virtual Apps and Desktopsをホストする2つのデータセンターを所有しています。同社の従業員は、NetScaler GatewayとCitrix GSLBベースのリダイレクトを使用して、世界中のどこからでもCitrix Virtual Apps and Desktopsにアクセスします。ABC Inc.のCitrix Virtual Apps and Desktops管理者であるEricは、いつでもどこからでもアプリとデスクトップの配信を最適化するために、すべてのオフィスのユーザーエクスペリエンスを追跡したいと考えています。Ericはまた、ICA RTT、遅延などのユーザーエクスペリエンスメトリックをチェックし、逸脱をプロアクティブに提起したいと考えています。

ABC Inc.のユーザーは分散した場所に存在します。一部のユーザーはデータセンターの近くにいますが、一部のユーザーはデータセンターから遠く離れた場所にいます。ユーザーベースが広範囲に分散しているため、メトリックとそれに対応するしきい値もこれらの場所によって異なります。たとえば、データセンターに近い場所のICA RTTは5〜10ミリ秒ですが、リモートロケーションの場合は約100ミリ秒になることがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX Insightのしきい値ルールグループ管理により、Ericは各ロケーションに地理固有のしきい値ルールグループを設定し、エリアごとの違反についてメールまたはSMSでアラートを受け取ることができます。Ericはまた、しきい値ルールグループ内で複数のメトリックの追跡を組み合わせ、容量の問題がある場合はその根本原因を絞り込むこともできます。Ericは、すべてのCitrix Virtual Apps and Desktopsポートフォリオメトリックを手動で確認する複雑さを心配することなく、逸脱をプロアクティブに追跡できるようになりました。

**NetScaler Consoleを使用してHDX Insightのしきい値ルールグループを作成し、アラートを設定するには：**

1. NetScaler Consoleで、**Settings > Analytics Settings > Thresholds**に移動します。開いた**Thresholds**ページで、**Add**をクリックします。
2. **Create Thresholds and Alerts**ページで、次の詳細を指定します。

   a. **名前**。NetScaler Consoleがアラートを生成するイベントの名前を入力します。

   b. **トラフィックタイプ**。リストボックスからHDXを選択します。

   c. **エンティティ**。リストボックスからカテゴリまたはリソースタイプを選択します。エンティティは、以前に選択したトラフィックタイプごとに異なります。

   d. **参照キー**。参照キーは、選択したトラフィックタイプとエンティティに基づいて自動的に生成されます。

   e. **期間**。リストボックスから、エンティティを監視する時間間隔を選択します。エンティティを1時間、1日、または1週間の期間で監視できます。

   しきい値の設定(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-1.png)

3. すべてのエンティティのしきい値ルールグループを作成する：

   HDXトラフィックの場合、**Add Rule**をクリックしてルールを作成する必要があります。開いた**Add Rules**ポップアップウィンドウに値を入力します。

   「ルールを追加」(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-2.png)

   各エンティティを監視するために複数のルールを作成できます。1つのグループに複数のルールを作成することで、個別のルールではなく、しきい値ルールのグループとしてエンティティを監視できます。ウィンドウを閉じるには、**OK**をクリックします。

   「SLA管理」(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-3.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ユーザーエンティティの地理位置情報タグ付けの構成

   オプションで、**地理詳細の構成**セクションでユーザーエンティティの場所ベースのアラートを作成できます。次の図は、米国西海岸のユーザーのWAN遅延パフォーマンスを監視するための地理位置情報ベースのタグ付けを作成する例を示しています。

   「地理詳細」(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-4.png)

5. **しきい値を有効にする**をクリックして、NetScaler Consoleがエンティティの監視を開始できるようにします。
6. オプションで、電子メール通知やSMS通知などのアクションを構成します。
7. しきい値ルールグループを作成するには、**作成**をクリックします。

## HDX™ Insight レポートとメトリクスの表示

HDX Insight は、NetScaler インスタンス上の HDX トラフィックに関するレポートとメトリクスを完全に可視化します。

選択したエンティティの HDX メトリクスを表示できます。ビューには、次のエンティティカテゴリが含まれます。

- **ユーザー**: 選択した時間間隔内に Citrix Virtual App または Desktop にアクセスしているすべてのユーザーのレポートを表示します。
- **アプリケーション**: アプリケーションの総数、および指定された時間間隔内にアプリケーションが起動された合計回数など、関連するすべての情報に関するレポートを表示します。
- **インスタンス**: 受信トラフィックのゲートウェイとして機能する NetScaler インスタンスに関するレポートを表示します。
- **Gateway Virtual Servers**: すべての仮想サーバーのレポートを表示します。
- **デスクトップ**: 選択した期間に使用されたデスクトップのレポートを表示します。
- **ライセンス**: 指定された時間枠内で使用された SSL VPN ライセンスの総数に関するレポートを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

リリース 14.1 ビルド 51.x 以降、VPN 仮想サーバーレベルでアクティブセッション、デスクトップ、起動されたアプリケーションなどの主要なメトリクスを監視できます。すべての仮想サーバーのリストは、**Gateway > HDX Insight > Gateway Virtual Servers** で表示できます。

## ユーザービューのレポートとメトリクス

このビューのレポートとメトリクスは、Citrix Virtual Apps and Desktops ユーザーごとに表示されます。

**ユーザービューに移動するには:**

1. **Gateway > HDX Insight > Users** に移動します。

   ユーザーグラフ(/en-us/netscaler-application-delivery-management-software/media/analytics-hgx-users-graph.png)

ユーザービューレポートとメトリクスは、以下のセクションで構成されています。

- 概要ビュー
- ユーザー別ビュー
- ユーザーセッション別ビュー

### 概要ビュー

概要ビューには、選択したタイムライン中にログインしたすべてのユーザーのレポートが表示されます。このビューのすべてのメトリクス/レポートは、特に指定がない限り、選択した期間に対応する値を表示します。

**選択した期間を変更するには：**

1. 期間リストまたはタイムスライダーを使用して、目的の時間間隔を設定します。
2. **Go**をクリックします。

折れ線グラフ

| メトリクス | 説明 |
| --- | --- |
| アクティブセッション | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリクス | 説明 |
| --- | --- |
| アクティブなアプリ | この数値は、アクティブなCitrix Virtual App セッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDIまたはCVADまたはStoreFrontサーバー間の遅延です。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンドの通信にかかった1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリクス | 説明 |
| --- | --- |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-line-chart.png)

### ユーザーサマリーレポート

このレポートに固有のメトリックは次のとおりです。

| メトリック | 説明 |
| --- | --- |
| アクティブセッション | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| アクティブなアプリ | この数値は、アクティブなCitrix Virtual Appセッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションやデスクトップを操作する際に、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| 帯域幅 | 選択された時間間隔中にエンドツーエンドの通信にかかった1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありません |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| | が、再送信による高い帯域幅使用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| アプリ起動総数 | 選択した期間中にユーザーが起動したアプリの総数。 |
| 総バイト数 | 選択した期間中にユーザーが消費した総バイト数。 |
| アクティブなデスクトップ | 指定された時間間隔におけるアクティブなCitrix Virtual Desktopsの総数。 |

サマリーレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-user-summary-report.png)

### チャネル

チャネルは、ドーナツグラフの形式で、各ICA®仮想チャネルによって消費される全体的な帯域幅または総バイト数を表します。帯域幅または総バイト数でメトリックを並べ替えることもできます。

「チャネル」(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-channel-1.png)

### ユーザーエージェント

ユーザーエージェントは、各ワークスペースクライアントが消費する全体の帯域幅/合計バイト数をドーナツチャート形式で表します。チャート内の色付きの各セグメントは、1つのワークスペースクライアントを表します。セグメントの長さは、そのワークスペースクライアントでアプリケー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ションを起動しているユーザーの数によって異なります。メトリックを帯域幅または合計バイト数で並べ替えることもできます。

「ユーザーエージェント」(/en-us/netscaler-application-delivery-management-software/media/hdx-user-agents.png)

各セグメントをクリックすると、そのワークスペースクライアントを使用しているユーザーの詳細が表示されます。

「ユーザーエージェント1」(/en-us/netscaler-application-delivery-management-software/media/hdx-user-agents-1.png)

#### しきい値違反数

しきい値違反数メトリックは、選択した期間内に違反したしきい値の数を表します。

#### 世界地図

HDX Insightの「世界地図」ビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者は、システムの世界地図ビューを表示し、地域をクリックするだけで特定の国、さらに都市へとドリルダウンできます。管理者は、さらに都市や州ごとの情報を表示するためにドリルダウンできます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightの「世界地図」では、以下の詳細を表示でき、各メトリックの密度はヒートマップ形式で表示されます。

- ICA RTT
- WAN遅延
- DC遅延
- 帯域幅
- 合計バイト数

世界地図(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

### ユーザーごとの表示

ユーザーごとの表示では、選択した特定のユーザーの詳細なエンドユーザーエクスペリエンスレポートが提供されます。

**特定のユーザーのメトリックに移動するには：**

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Gateway > HDX Insight > Users**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ユーザーサマリーレポートから特定のユーザーを選択します。

### 折れ線グラフ

折れ線グラフには、選択した期間における特定の選択ユーザーのすべてのメトリックの概要が表示されます。

現在/終了したセッションレポート

このレポートは、選択したユーザーの現在/終了したすべてのユーザーセッションに関連しています。これらのメトリックは、開始時刻、セッション再接続、およびACRカウントでソートできます。

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | サーバーネットワークによって引き起こされる、NetScalerを通過するICAトラフィックの平均遅延。 |
| 間隔あたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| 間隔あたりのバイト数 | その特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッション開始時刻。 |
| 稼働時間 | セッションの継続時間。 |
| クライアントIPアドレス | エンドユーザーのIP。 |
| サーバーIPアドレス | バックエンド/Citrix Virtual Appsサーバーの IP。 |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| クライアントタイプ | ワークスペースタイプ - Citrix Windows Client など |
| クライアントバージョン | ワークスペースのバージョン。 |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッションの再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gatewayユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 市 | セッションが確立された市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー回数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。例：ICAセッションタイムアウト、ユーザーによるセッション終了。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppsまたはCitrix Virtual Desktopsでホストされているアプリ |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| | ケーションやデスクトップを操作する際に、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDIまたはCVADまたはStoreFrontサーバー間の遅延です。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### HDX InsightにおけるEDTのサポート

NetScaler Consoleは、HDX Insightの分析を表示するために、Enlightened Data Transport (EDT)をサポートするようになりました。つまり、NetScaler ConsoleはUDPとTCPの両方のプロトコルをサポートしています。NetScaler GatewayのEDTサポートにより、Citrix Workspaceを実行しているユーザーに対して、仮想デスクトップのセッション内ユーザーエクスペリエンスが高精細に保証されます。

HDX Insightは、アクティブセッションレポートの一部として、EDTセッションと非EDTセッションの数を表示するようになりました。ユーザーテーブルには、システム内のすべてのユーザーの詳細レポートが表示されます。このテーブルには、WAN遅延、DC遅延、再送信、RTOなどのメトリックが表示されますが、これらのメトリックの一部は、現在TCPスタックから計算されているため、EDTセッションを持つユーザーには利用できません。したがって、それらは「NA」と表示されます。

- ユーザーが消費した帯域幅と、ユーザーが使用したプロトコルの種類に基づいた合計バイト数を確認できる新しいドーナツチャートが導入されました。

**注**

HDX InsightにおけるEDTは、NetScaler Consoleではリリース12.1ビルド50.28以降でサポートされており、ADCインスタンスではリリース12.1ビルド49.23以降で利用可能です。

### NetScaler Console 12.0以降で利用可能なHDX Insightメトリック:

| L7クライアント側遅延 | ICAクライアントとNETSCALERインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCITRIX以外のデバイスが存在する場合に役立ちます。 |
|---|---|
| L7サーバー側遅延 | NetScalerデバイスとCitrix Virtual App間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。 |
| 最大違反遅延 | 設定された時間間隔で定義されたしきい値の違反が発生した場合のL7遅延の最高値。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| L7クライアント側遅延 | ICAクライアントとNETSCALERインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCITRIX以外のデバイスが存在する場合に役立ちます。 |
| --- | --- |
| 平均違反遅延 | システムが「L7遅延違反」状態にある場合のL7遅延の平均値。 |
| L7しきい値違反回数 | L7しきい値違反が発生した回数。 |

現在のセッション(/en-us/netscaler-application-delivery-management-software/media/hdx-current-sessions-1.png)

終了したセッション(/en-us/netscaler-application-delivery-management-software/media/hdx-teminated-sessions-1.png)

### デスクトップユーザー

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する洞察を提供します。これらのメトリックは、デスクトップ起動回数と帯域幅でソートできます。

| メトリック | 説明 |
| --- | --- |
| 名前 | シトリックス バーチャル デスクトップの名前。 |
| デスクトップ起動回数 | デスクトップが起動された回数。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信で使用された1秒あたりの合計バイト数。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。 |
| ICA RTT | ICA RTTは、ユーザーがCitrix Virtual AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作しているときに発生する画面の遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デスクトップユーザー(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)
アプリケーション
アクティブ、セッション起動総数、アプリ起動総数、起動期間でソートされたアプリを表す棒グラフ。

アプリケーショングラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-application-graph.png)
インスタンス
アクティブなアプリと合計アプリでソートされたNetScalerインスタンスを表す棒グラフ

インスタンス(/en-us/netscaler-application-delivery-management-software/media/hdx-instances-graph.png)
チャネル
チャネルは、各ICA仮想チャネルによって消費される全体的な帯域幅または合計バイト数をドーナツチャートの形式で表します。メトリックを帯域幅または合計バイト数で並べ替えることもできます。

ユーザーエージェント
ユーザーエージェントは、各エンドポイントによって消費される全体的な帯域幅/合計バイト数をドーナツチャートの形式で表します。メトリックを帯域幅または合計バイト数で並べ替えることもできます。

### ユーザーセッションごとのビュー

ユーザーセッションごとのビューでは、特定の選択されたユーザーのセッションに関するレポートが提供されます。

**選択したユーザーのセッションのメトリックを表示するには：**

1. **Gateway > HDX Insight > Users** に移動します。
2. **User Summary Report** セクションから特定のユーザーを選択します。
3. **Current Sessions** または **Terminated Sessions** 列からセッションを選択します。

タイムラインチャート

| メトリック | 説明 |
| --- | --- |
| セッションの再接続 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| ACRカウント | この数値は、アクティブなCitrix Virtual App セッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppsまたはDesktops でホストされているアプリケーションまたは デスクトップを操作する際にユーザーが経験 する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起 こされる遅延。つまり、NetScalerからエンド ユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こ される遅延。NetScaler GatewayとVDI、 CVAD、またはStoreFrontサーバー間の遅延で す。 |
| セッション帯域幅 | 時間間隔に関係なく、セッションによって消 費される帯域幅。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で 再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信 されたパケットの数。このメトリックの値が 高いからといって、ユーザーエクスペリエンス がシームレスでなくなるわけではありません が、再送信による高い帯域幅使用率を示しま す。 |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信 タイムアウトが発生した回数。 |
| サーバー側の高速RTO | NetScalerとバックエンドサーバー間の接続で 再送信タイムアウトが発生した回数。 |
| 間隔あたりの帯域幅 | その特定の時間間隔中にセッションによって 消費された帯域幅。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィ ンドウをアドバタイズした回数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |

アクティブなアプリケーション

「**アクティブなアプリケーション**」セクションには、選択したユーザーのアクティブなアプリケーションが表示されます。これらのアプリケーションは、アクティブなセッション数と起動期間で並べ替えることもできます。

関連セッション

関連セッションセクションには、選択したユーザーのセッションの関連セッションが表示されます。関係は、共通サーバーまたは共通NetScalerとして選択できます。

関連セッション(/en-us/netscaler-application-delivery-management-software/media/hdx-related-sessions.png)

### アプリケーションビューのレポートとメトリック

このビューのレポートとメトリックは、Citrix Virtual Appsに焦点を当てています。

**アプリケーションビューに移動するには：**

1. **Gateway > HDX Insight > Applications** に移動します。

**概要ビュー**

概要ビューには、選択したタイムライン中にログインしたすべてのアプリケーションのレポートが表示されます。

明示的に言及されていない限り、すべてのメトリック/レポートには、選択した期間に対応する値が設定されます。

#### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # セッション | 指定された時間間隔におけるセッションの総数。 |
| 起動時間 | アプリケーションの起動にかかる平均時間。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart.png)

### アプリケーション概要レポート

| メトリック | 説明 |
| --- | --- |
| 名前 | Citrix Virtual App の名前。 |
| 合計セッション起動数 | 指定された時間間隔におけるアクティブな Citrix Virtual App セッションの合計数。 |
| 合計アプリ起動数 | 指定された時間間隔に起動された Citrix Virtual App アプリケーションの合計数。 |
| 起動時間 | Citrix Virtual App の起動にかかる平均時間。 |

概要レポート(/en-us/netscaler-application-delivery-management-software/media/hdx-application-summary-report.png)

### アクティブアプリケーションレポート

| メトリック | 説明 |
| --- | --- |
| 名前 | Citrix Virtual Appの名前。 |
| 状態 | アプリケーションの状態を表示します: 緑 - アクティブ、赤 - 非アクティブ |
| アクティブなセッション数 | 指定された時間間隔でこのアプリを使用しているアクティブなユーザーセッションの数。 |
| アクティブなアプリ数 | このアプリケーションのアクティブなセッション数。 |

アクティブレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-active-applications.png)

### しきい値レポート

しきい値レポートは、選択した期間にアプリケーションとして*エンティティ*が選択された場合に、違反したしきい値の数を表します。詳細については、しきい値の作成方法を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # アクティブセッション数 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| 起動時間 | アプリケーションの起動にかかる平均時間。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart-1.png)

### 現在のセッションレポート

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | NetScalerを通過するICAトラフィックにおいて、サーバーネットワークによって引き起こされる平均遅延。 |
| インターバルあたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| インターバルあたりのバイト数 | その特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッションの開始時刻。 |
| アップタイム | セッション期間。 |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンド/Citrix Virtual Appサーバーの IPアドレス。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |
| クライアントの種類 | ワークスペースの種類 - Citrix Windows Client など |
| クライアントのバージョン | ワークスペースのバージョン。 |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッションの再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gateway ユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 都市 | セッションが確立された都市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。たとえば、ICAセッションタイムアウト、ユーザーによるセッション終了など。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| ICA RTT | ICA RTTは、Citrix Virtual AppsまたはDesktopsでホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延。 |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側の再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示しています。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側の高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| ユーザー名 | この特定のCitrix Virtual Appにアクセスしているユーザーのユーザー名。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| セッションID | Citrix Virtual Appセッションの一意の識別子。 |
| セッションタイプ | 「アプリケーション」になります。 |
| 状態 | セッション状態: アクティブは緑、非アクティブは赤。 |
| 最大違反遅延 | 設定された時間間隔で定義されたしきい値の違反が発生したときのL7遅延の最高値。 |
| 平均違反遅延 | システムが「L7遅延違反」状態にあるときのL7遅延の平均値。 |
| L7しきい値違反回数 | L7しきい値違反が発生した回数。 |
| L7クライアント側遅延 | ICAクライアントとNetScalerインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。 |
| L7サーバー側遅延 | NetScalerデバイスとCitrix Virtual App間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。 |

セッションレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-current-sessions-report.png)

### アプリケーションごとのセッションビュー

アプリケーションごとのセッションビューには、特定の選択されたアプリケーションセッションのレポートが表示されます。

### セッションレポートを表示するには：

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Gateway > HDX Insight > Applications**に移動します。
3. アプリケーションサマリーレポートから特定のユーザーを選択します。
4. 現在のセッションレポートからセッションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| セッションの再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppsおよびDesktopsでそれぞれホストされているアプリケーションまたはデスクトップと対話する際にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| サーバー側のゼロウィンドウサイズイベント | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 間隔あたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| サーバー側の再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側の再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅利用率を示します。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |



ユーザー棒グラフ

ユーザーの棒グラフは、この特定のアプリにログインしているユーザーを表します。



## デスクトップビューのレポートとメトリクス

このビューのレポートとメトリクスは、Citrix Virtual Desktopsに焦点を当てています。

**デスクトップビューに移動するには：**

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Gateway > HDX Insight > Desktop**に移動します。

### サマリービュー

概要ビューには、選択した期間中にログインしたすべてのCitrix Virtual Desktopsのレポートが表示されます。

明示的に記載されていない限り、すべてのメトリック/レポートには、選択した期間に対応する値が表示されます。

折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # アクティブセッション数 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| # アクティブアプリ数 | この数値は、アクティブなCitrix Virtual Appセッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktopsでホストされているアプリケーションまたは |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| | デスクトップを操作する際にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信に要した1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅利用率を示しています。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-line-chart.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デスクトップサマリーレポート

| メトリック | 説明 |
| --- | --- |
| アクティブセッション | 指定された時間間隔におけるアクティブなCitrix Virtual Desktopセッションの総数。 |
| アクティブデスクトップ | 指定された時間間隔におけるアクティブなCitrix Virtual Desktopの総数。 |
| ICA RTT | ICA RTTは、ユーザーがCitrix Virtual Apps and Desktopsでホストされているアプリケーションまたはデスクトップを操作する際に経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| 帯域幅 | 選択された時間間隔におけるエンドツーエンド通信にかかる1秒あたりの総バイト数。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |

しきい値レポート

しきい値レポートは、選択した期間に*エンティティ*がデスクトップとして選択された場合に違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

### デスクトップごとのビュー

デスクトップごとのビューは、選択したCitrix Virtual Desktopの詳細なエンドユーザーエクスペリエンスレポートを提供します。

**特定のデスクトップビューに移動するには：**

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Analytics \> HDX Insight \> Desktop**に移動します。
3. **Desktop Summary Report**から特定の**Desktop**を選択します。

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # アクティブセッション数 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| # アクティブなアプリ | この数値は、アクティブなCitrix Virtual App セッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたは デスクトップを操作しているときにユーザー が経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信に要した1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送タイムアウトが発生した回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-line-chart.png)

### デスクトップユーザーレポート

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する洞察を提供します。これらのメトリックは、デスクトップ起動数と帯域幅で並べ替えることができます。

| メトリック | 説明 |
| --- | --- |
| 名前 | シトリックス バーチャル デスクトップの名前。 |
| デスクトップ起動回数 | デスクトップが起動された回数。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信に費やされた1秒あたりの合計バイト数。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktopsでホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デスクトップユーザー(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)

### ユーザーデスクトップのアクティブ/非アクティブレポート

これらの以下のメトリックは、間隔あたりの帯域幅、セッション再接続、およびACRカウントでソートできます。

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | NetScalerを通過するICAトラフィックにおける、サーバーネットワークによって引き起こされる平均遅延。 |
| インターバルあたりの帯域幅 | 特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| インターバルあたりのバイト数 | 特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッション開始時刻。 |
| アップタイム | セッション期間。 |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンド/シトリックス バーチャル アプリサーバーのIPアドレス。 |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |
| クライアントタイプ | ワークスペースタイプ - Citrix Windows Client など |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| クライアントバージョン | ワークスペースバージョン。 |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッション再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gatewayユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 市 | セッションが確立された市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー回数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。たとえば、ICAセッションタイムアウト、ユーザーによるセッション終了などです。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktopsでホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| 合計バイト | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケット数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅利用率を示します。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| VDIイメージ名 | ユーザーが接続しているCitrix Virtual Desktopの名前 |
| 図 | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

非アクティブなユーザー(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive.png)

### デスクトップセッションごとのビュー

デスクトップセッションごとのビューは、特定の選択されたCitrix Virtual Desktopセッションのレポートを提供します。

**デスクトップセッションビューに移動するには：**

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Analytics \> HDX Insight \> Desktop**に移動します。
3. **デスクトップサマリーレポート**から特定のデスクトップを選択します。
4. 現在のセッションレポートからセッションを選択します。

タイムラインチャート

ユーザーセッションごとのビューは、特定の選択されたユーザーのセッションのレポートを提供します。

**選択したユーザーのセッションのメトリックを表示するには：**

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Gateway > HDX Insight > Users** に移動します。
3. **User Summary Report** セクションから特定のユーザーを選択します。
4. **Current Sessions** または **Terminated Sessions** 列からセッションを選択します。

| メトリック | 説明 |
| --- | --- |
| セッションの再接続 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| ACRカウント | この数値は、アクティブなCitrix Virtual App セッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktops でそれぞれホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| セッション帯域幅 | 時間間隔に関係なく、セッションによって消費される帯域幅。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| 間隔あたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |

タイムラインチャート(/en-us/netscaler-application-delivery-management-software/media/hdx-timeline-chart.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 関連するデスクトップセッションレポート

これらの以下のメトリックは、間隔あたりの帯域幅、セッション再接続、およびACRカウントでソートできます。

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | NetScalerを通過するICAトラフィックにおける、サーバーネットワークによって引き起こされる平均遅延。 |
| 期間ごとの帯域幅 | 特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| 期間ごとのバイト数 | 特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッション開始時刻。 |
| 稼働時間 | セッション期間。 |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンド/Citrix Virtual AppサーバーのIPアドレス。 |
| NetScaler IPアドレス | NetScaler 管理 IP (NSIP)。 |
| クライアントタイプ | ワークスペースタイプ - Citrix Windows Client など |
| クライアントバージョン | ワークスペースバージョン。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリーム ICA であるかどうかを示します。 |
| セッションの再接続 | セッションが再接続された回数。 |
| ACR カウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICA セッションのアクセスモードを表示します。例: NetScaler Gateway ユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 都市 | セッションが確立された都市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。たとえば、ICAセッションタイムアウト、ユーザーによるセッション終了などです。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktopsでホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側の高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |

非アクティブユーザー(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive.png)

### インスタンスビューのレポートとメトリック

インスタンスビューのレポートとメトリックは、NetScalerインスタンスに焦点を当てています。

**インスタンスビュー**に移動するには：

1. サポートされているWebブラウザーを使用してNetScaler Consoleにログオンします。
2. **Analytics \> HDX Insight \> Instances** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスビューのレポートとメトリックは、次のセクションで構成されています。

- 「インスタンス概要ビュー」(#instance-summary-view)
- 「インスタンス別ビュー」(#per-instance-view)

### インスタンス概要ビュー

このビューは、NetScaler Consoleに追加されたすべてのNetScalerインスタンスのレポートを表示するため、概要ビューと呼ばれます。

明示的に記載されていない限り、以下のすべてのメトリック/レポートには、選択された期間に対応する値が表示されます。

#### インスタンス棒グラフ

このグラフは、インスタンスと合計セッション起動数 | 合計アプリを表示します。これらは、グラフキャンバスの右上にあるリストから選択できます。



#### インスタンス/アクティブインスタンス概要レポート

| メトリック | 説明 |
|---|---|
| 名前 | NetScalerインスタンスのホスト名。 |
| IPアドレス | NetScalerのIPアドレス。 |
| セッション起動総数 | 指定された時間間隔中に作成された一意のユーザーセッションの総数。 |
| アプリケーション総数 | 指定された時間間隔中に起動された一意のアプリケーションの総数。 |
| タイプ | N/A |



#### しきい値レポート

しきい値レポートは、選択した期間に*エンティティ*がインスタンスとして選択された場合に違反したしきい値の数を表します。詳細については、「しきい値の作成方法」を参照してください。

#### スキップされたフロー

スキップされたフローとは、ICA接続の解析をスキップしたレコードです。これは、サポートされていないCitrix Virtual Apps and Desktopsのバージョン、サポートされていないワークスペースの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バージョンまたはワークスペースタイプを使用しているなど、複数の理由で発生する可能性があります。この表には、IPアドレスとスキップされたフローの数が表示されます。これらのワークスペースは、ホワイトリストに登録されたワークスペースの一部ではない可能性があります。したがって、これらのセッションは監視からスキップされます。

### 世界地図ビュー

HDX Insightのワールドマップビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者は、システムの世界地図ビューを表示し、地域をクリックするだけで特定の国、さらに都市へとドリルダウンできます。管理者は、さらに都市や州ごとの情報を表示するためにドリルダウンできます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightのワールドマップでは以下の詳細を表示でき、各メトリックの密度はヒートマップの形式で表示されます。

- ICA RTT
- WAN 遅延
- DC 遅延
- 帯域幅
- 合計バイト

### インスタンスごとの表示

インスタンスごとの表示では、特定の選択されたNetScalerインスタンスについて、詳細なエンドユーザーエクスペリエンスレポートが提供されます。

**インスタンス表示に移動するには:**

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Analytics \> HDX Insight \> Instances** に移動します。
3. **インスタンスサマリーレポート**から特定のインスタンスを選択します。

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| IPアドレス | これは、選択されたインスタンスのNetScaler IPアドレスを表します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| セッション起動総数 | 指定された時間間隔におけるアクティブなCitrix Virtual Appセッションの総数。 |
| アプリケーション総数 | 指定された時間間隔に起動された一意のアプリケーションの総数。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart-4.png)

### アプリケーション棒グラフ

アクティブなアプリ、セッション起動総数、アプリ起動総数、または起動期間の基準に基づいて、上位5つのアプリケーションを表示します。

棒グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-applications-bar-graph.png)

### ユーザー棒グラフ

ユーザー棒グラフは、以下の基準に基づいて上位5人のユーザーを表示します。

- 帯域幅
- WAN遅延
- DC遅延
- ICA RTT

ユーザーグラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-users-bar-graph.png)

### デスクトップユーザーレポート

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する情報を提供します。これらのメトリクスは、デスクトップ起動回数と帯域幅でソートできます。

| メトリクス | 説明 |
| --- | --- |
| 名前 | シトリックス バーチャル デスクトップ の名称。 |
| デスクトップ起動回数 | デスクトップが起動された回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリクス | 説明 |
| --- | --- |
| 帯域幅 | 選択された時間間隔中にエンドツーエンド通信に使用された1秒あたりの合計バイト数。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScaler GatewayとVDI、CVAD、またはStoreFrontサーバー間の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppsおよびDesktopsでそれぞれホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーが経験する画面の遅延です。 |

デスクトップユーザー(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)

### 世界地図ビュー

HDX Insightのワールドマップビューでは、管理者は地理的な観点から履歴ユーザーとアクティブユーザーの詳細を表示できます。管理者は、システムの世界地図ビューを表示し、地域をクリックして特定の国、さらに都市へとドリルダウンできます。管理者は、さらにドリルダウンして都市や州ごとの情報を表示できます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightのワールドマップでは以下の詳細を表示でき、各メトリックの密度はヒートマップ形式で表示されます。

- ICA RTT
- WAN遅延
- DC遅延
- 帯域幅
- 合計バイト数

世界地図ビュー(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## ライセンスビューレポートとメトリック

ライセンスビューには、NetScaler Gatewayのライセンス情報に関する詳細が表示されます。

### ライセンスビューに移動するには：

1. サポートされているWebブラウザを使用してNetScaler Consoleにログオンします。
2. **Analytics \> HDX Insight \> Licenses** に移動します。

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| 使用中のライセンス | 選択した期間中に使用されているNetScaler Gateway CCUライセンス。各カウントはユーザーセッションの数を表します。これは、そのユーザーが起動したアプリケーションおよびデスクトップセッションとは独立しています。 |
| 合計ライセンス数 | お客様が利用できるNetScaler Gateway CCUライセンスの総数。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart.png)

#### しきい値レポート

しきい値レポートは、選択した期間に*エンティティ*がライセンスとして選択された、違反したしきい値の数を表します。詳細については、しきい値の作成方法を参照してください。

## アプリケーションビューのレポートとメトリック

このビューのレポートとメトリックは、Citrix Virtual Appsに焦点を当てています。

### アプリケーションビューに移動するには：

1. **Gateway > HDX™ Insight > Applications** に移動します。

### 概要ビュー

概要ビューには、選択したタイムライン中にログインしたすべてのアプリケーションのレポートが表示されます。

明示的に言及されていない限り、以下のすべてのメトリック/レポートには、選択した期間に対応する値が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # セッション数 | 指定された時間間隔におけるセッションの総数。 |
| 起動時間 | アプリケーションの起動にかかる平均時間。 |

### アプリケーション概要レポート

| メトリック | 説明 |
| --- | --- |
| 名前 | Citrix Virtual App の名前。 |
| セッション起動総数 | 指定された時間間隔におけるアクティブな Citrix Virtual App セッションの総数。 |
| アプリケーション起動総数 | 指定された時間間隔における起動された Citrix Virtual App アプリケーションの総数。 |
| 起動時間 | Citrix Virtual App の起動にかかった平均時間。 |

### アクティブなアプリケーションレポート

| メトリック | 説明 |
| --- | --- |
| 名前 | Citrix Virtual Appの名前。 |
| 状態 | アプリケーションの状態を表示します: 緑 - アクティブ、赤 - 非アクティブ |
| #アクティブセッション | 指定された時間間隔でこのアプリを使用しているアクティブなユーザーセッションの数。 |
| #アクティブアプリ | このアプリケーションのアクティブセッション数。 |

アクティブアプリケーションレポートの画像。(/en-us/netscaler-application-delivery-management-software/media/hdx-active-applications.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### しきい値レポート

しきい値レポートは、選択された期間にエンティティとしてアプリケーションが選択された場合に違反したしきい値の数を表します。詳細については、しきい値とアラートの作成方法を参照してください。

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # アクティブセッション | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| 起動時間 | アプリケーションの起動にかかる平均時間。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart-1.png)

### 現在のセッションレポート

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | サーバーネットワークによって引き起こされる、NetScalerを通過するICAトラフィックの平均遅延。 |
| インターバルあたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なく、セッションによって消費された帯域幅。 |
| インターバルあたりのバイト数 | その特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッション開始時刻。 |
| アップタイム | セッション期間。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンドまたはシトリックス バーチャル アプリ サーバー IP。 |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |
| クライアントの種類 | ワークスペースの種類 - Citrix Windows Client など |
| クライアントバージョン | ワークスペースのバージョン。 |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッションの再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gatewayユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 都市 | セッションが確立された都市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー数 | HAフェイルオーバーが発生した回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| 終了理由 | セッション終了の理由を表示します。たとえば、ICAセッションタイムアウト、ユーザーによるセッション終了などです。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktopsでホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンタは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンタは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| サーバー側の高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| ユーザー名 | この特定のCitrix Virtual Appにアクセスしているユーザーのユーザー名。 |
| セッションID | Citrix Virtual Appセッションの一意の識別子。 |
| セッションタイプ | 「アプリケーション」になります。 |
| 状態 | セッション状態: アクティブの場合は緑、非アクティブの場合は赤。 |
| 最大違反遅延 | 設定された時間間隔で定義されたしきい値の違反が発生した場合のL7遅延の最高値。 |
| 平均違反遅延 | システムが「L7遅延違反」状態にある場合のL7遅延の平均値。 |
| L7しきい値違反回数 | L7しきい値違反が発生した回数。 |
| L7クライアント側遅延 | ICAクライアントとNetScalerインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。 |
| L7サーバー側遅延 | NetScalerデバイスとCitrix Virtual App間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。 |



### アプリケーションごとのセッションビュー

アプリケーションごとのセッションビューには、特定の選択されたアプリケーションセッションのレポートが表示されます。

**セッションレポートを表示するには:**

1. 「**Gateway > HDX Insight > Applications**」に移動します。
2. アプリケーションサマリーレポートから特定のユーザーを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 現在のセッションレポートからセッションを選択しました。

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| セッションの再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続する合計回数。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktopsでそれぞれホストされているアプリケーションまたはデスクトップと対話している間にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。 |
| サーバー側ゼロウィンドウサイズイベント | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーへの遅延。 |
| インターバルあたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| サーバー側の再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケット数。 |
| クライアント側の再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側の高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart-2.png)

#### ユーザー棒グラフ

ユーザー棒グラフは、この特定のアプリにログインしているユーザーを表します。

ユーザー棒グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-user-bar-graph.png)

### デスクトップビューのレポートとメトリック

このビューのレポートとメトリックは、Citrix Virtual Desktops に焦点を当てています。

**デスクトップビューに移動するには：**

1. **Gateway > HDX™ Insight > Desktop** の順に移動します。

#### 概要ビュー

概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops のレポートが表示されます。

明示的に言及されていない限り、すべてのメトリック/レポートには、選択した期間に対応する値が表示されます。

#### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # アクティブなセッション | この数値は、アクティブな Citrix Virtual Apps and Desktops セッションの数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| # アクティブなアプリ | この数値は、アクティブな Citrix Virtual App セッションの数を示します。 |
| ICA RTT | ICA RTT は、Citrix Virtual Apps および Desktops でそれぞれホストされているアプリケーションまたはデスクトップをユーザーが操作している際に経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 帯域幅 | 選択された時間間隔中にエンドツーエンド通信にかかる1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケット数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示しています。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-line-chart.png)

#### デスクトップサマリーレポート

| メトリック | 説明 |
| --- | --- |
| アクティブセッション | 指定された時間間隔におけるアクティブなCitrix Virtual Desktopセッションの総数。 |
| アクティブデスクトップ | 指定された時間間隔におけるアクティブなCitrix Virtual Desktopの総数。 |
| ICA RTT | ICA RTTは、ユーザーがCitrix Virtual AppsおよびDesktopsでホストされているアプリケーションまたはデスクトップを操作する際に経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまで。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信に要した1秒あたりの合計バイト数。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |

デスクトップレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-summary-report.png)

#### しきい値レポート

しきい値レポートは、選択した期間に*エンティティ*としてデスクトップが選択されている場合に違反したしきい値の数を表します。詳細については、しきい値とアラートの作成方法を参照してください。

### デスクトップごとのビュー

デスクトップごとのビューは、選択したCitrix Virtual Desktopの詳細なエンドユーザーエクスペリエンスレポートを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**特定のデスクトップビューに移動するには：**

1. **Analytics \> HDX Insight \> Desktop**に移動します。
2. **デスクトップサマリーレポート**から特定の**デスクトップ**を選択します。

折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| # アクティブセッション数 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| # アクティブアプリ数 | この数値は、アクティブなCitrix Virtual App セッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたは デスクトップを操作する際にユーザーが経験 する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起 こされる遅延。つまり、NetScalerからエンド ユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こ される遅延。つまり、NetScalerからバック エンドサーバーまでの遅延です。 |
| 帯域幅 | 選択された時間間隔中にエンドツーエンド通 信にかかった1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で 再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信 されたパケットの数。このメトリックの値が 高いからといって、ユーザーエクスペリエンス がシームレスでなくなるわけではありません が、再送信による高い帯域幅利用率を示して います。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信 タイムアウトが発生した回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-line-chart.png)

### デスクトップユーザーレポート

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する洞察を提供します。これらのメトリックは、デスクトップ起動数と帯域幅で並べ替えることができます。

| メトリック | 説明 |
| --- | --- |
| 名前 | シトリックス バーチャル デスクトップの名前。 |
| デスクトップ起動回数 | デスクトップが起動された回数。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信に要した合計バイト/秒。 |
| DC 遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScaler からバックエンドサーバーまでの遅延。 |
| WAN 遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScaler からエンドユーザーまでの遅延。 |
| ICA RTT | ICA RTT は、Citrix Virtual Apps and Desktops でホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ユーザーデスクトップのアクティブ/非アクティブレポート

以下のメトリックは、インターバルあたりの帯域幅、セッション再接続、およびACRカウントでソートできます。

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意の識別子。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | サーバーネットワークによって引き起こされる、NetScalerインスタンスを通過するICAトラフィックの平均遅延。 |
| インターバルあたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関わらず、セッションによって消費された帯域幅。 |
| インターバルあたりのバイト数 | その特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッションの開始時刻。 |
| アップタイム | セッションの継続時間。 |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンド/シトリックス バーチャル アプリケーションズ サーバーIP。 |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |
| クライアントタイプ | ワークスペースタイプ - Citrix Windows Client など |
| クライアントバージョン | ワークスペースバージョン。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッション再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gatewayユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 市 | セッションが確立された都市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー回数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。例：ICAセッションタイムアウト、ユーザーによるセッション終了。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppsまたはDesktopsでホストされているアプリケーションまたはデスクトップを操作する際に、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 合計バイト数 | 選択された期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送タイムアウトが発生した回数。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送タイムアウトが発生した回数。 |
| VDIイメージ名 | ユーザーが接続しているCitrix Virtual Desktopの名前 |
| 図 | |

非アクティブレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive.png)

### デスクトップセッションごとのビュー

デスクトップセッションごとのビューは、特定の選択されたCitrix Virtual Desktopセッションのレポートを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**デスクトップセッションビューに移動するには：**

1. **Gateway > HDX Insight > Desktop**に移動します。
2. **デスクトップサマリーレポート**から特定のデスクトップを選択します。
3. 現在のセッションレポートからセッションを選択します。

タイムラインチャート

ユーザーごとのセッションビューは、特定の選択されたユーザーのセッションに関するレポートを提供します。

**選択したユーザーのセッションのメトリックを表示するには：**

1. **Gateway > HDX Insight > Users** に移動します。
2. **User Summary Report** セクションから特定のユーザーを選択します。
3. **Current Sessions** または **Terminated Sessions** 列からセッションを選択します。

| メトリック | 説明 |
| --- | --- |
| セッションの再接続 | この数値は、アクティブなCitrix Virtual AppおよびDesktopセッションの数を示します。 |
| ACRカウント | この数値は、アクティブなCitrix Virtual Appセッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppおよびDesktopでホストされているアプリケーションまたはデスクトップと対話する際にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまで。 |
| セッション帯域幅 | 時間間隔に関係なく、セッションによって消費される帯域幅。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示しています。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| 間隔あたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |

タイムラインチャート(/en-us/netscaler-application-delivery-management-software/media/hdx-timeline-chart.png)

### 関連するデスクトップセッションレポート

これらの以下のメトリックは、間隔あたりの帯域幅、セッションの再接続、およびACRカウントでソートできます。

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| ホスト遅延 | NetScalerを通過するICAトラフィックにおける、サーバーネットワークによって引き起こされる平均遅延。 |
| インターバルあたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| インターバルあたりのバイト数 | その特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッションの開始時刻。 |
| アップタイム | セッション期間。 |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンド/シトリックス バーチャル アプリ サーバー IP。 |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |
| クライアントタイプ | Receiverタイプ - Citrix Windows Clientなど |
| クライアントバージョン | Receiverバージョン。 |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッションの再接続 | セッションが再接続された回数。 |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gatewayユーザー/透過モード。 |
| 国 | セッションが確立された国。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| 地域 | セッションが確立された地域。 |
| 市 | セッションが確立された市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名。 |
| HAフェイルオーバー数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。例えば、ICAセッションタイムアウト、ユーザーによるセッション終了など。 |
| ICA RTT | ICA RTTは、ユーザーがCitrix Virtual AppまたはDesktopでホストされているアプリケーションやデスクトップを操作する際に経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側の再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンス |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| | がシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示しています。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側の高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側の高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| VDIイメージ名 | ユーザーが接続しているCitrix Virtual Desktopの名前 |

関連するデスクトップセッション(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive.png)

### ユーザービューのレポートとメトリクス

このビューのレポートとメトリクスは、Citrix Virtual Apps™ および Desktop ユーザーごとに表示されます。

**ユーザービューに移動するには：**

1. **Gateway > HDX™ Insight > Users** に移動します。

   ユーザーメトリクス(/en-us/netscaler-application-delivery-management-software/media/analytics-hgx-users-graph.png)

**サマリービュー**

サマリービューには、選択したタイムライン中にログインしたすべてのユーザーのレポートが表示されます。このビューのすべてのメトリクス/レポートは、特に指定がない限り、選択した期間に対応する値を表示します。

**選択した期間を変更するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 期間リストまたはタイムスライダーを使用して、目的の時間間隔を設定します。
2. **Go** をクリックします。

### 折れ線グラフ

| メトリクス | 説明 |
| --- | --- |
| # アクティブセッション | この数値は、アクティブなCitrix Virtual AppおよびDesktopセッションの数を示します。 |
| # アクティブなアプリ | この数値は、アクティブなCitrix Virtual Appセッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションやデスクトップを操作する際に、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 帯域幅 | 選択された時間間隔中に、エンドツーエンドの通信にかかった1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅利用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送タイムアウトが発生した回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリクス | 説明 |
| --- | --- |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |

### ユーザーサマリーレポート

このレポートに固有のメトリックは次のとおりです。

| メトリック | 説明 |
| --- | --- |
| # アクティブセッション数 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| # アクティブアプリ数 | この数値は、アクティブなCitrix Virtual Appセッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppまたはDesktopでそれぞれホストされているアプリケーションまたはデスクトップを操作しているときに、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信にかかった1秒あたりの合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| | 高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送タイムアウトが発生した回数。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| アプリ起動総数 | 選択した期間中にユーザーが起動したアプリの総数。 |
| 総バイト数 | 選択した期間中にユーザーが消費した総バイト数。 |
| アクティブなデスクトップ | 指定された時間間隔におけるアクティブなCitrix Virtual Desktopsの総数。 |

サマリーレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-user-summary-report.png)

### チャネル

チャネルは、ドーナツグラフの形式で、各ICA®仮想チャネルによって消費される全体的な帯域幅または総バイト数を表します。メトリックを帯域幅または総バイト数で並べ替えることもできます。

### ユーザーエージェント

ユーザーエージェントは、各エンドポイントが消費した総帯域幅/合計バイト数をドーナツグラフ形式で表します。帯域幅または合計バイト数でメトリックをソートすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#### しきい値違反数

しきい値違反数メトリックは、選択した期間内に違反したしきい値の数を表します。詳細については、「しきい値とアラートの作成方法」を参照してください。

#### 世界地図

HDX Insight の世界地図ビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者は、システムの世界地図ビューを表示し、地域をクリックして特定の国、さらに都市へとドリルダウンできます。管理者は、さらにドリルダウンして都市および州ごとの情報を表示できます。NetScaler Console バージョン 12.0 以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insight の世界地図には、次の詳細が表示され、各メトリックの密度はヒートマップ形式で表示されます。

- ICA RTT
- WAN 遅延
- DC 遅延
- 帯域幅
- 合計バイト数

### ユーザー別ビュー

ユーザー別ビューでは、選択した特定のユーザーの詳細なエンドユーザーエクスペリエンスレポートが提供されます。

**特定のユーザーのメトリックに移動するには：**

1. **Gateway > HDX Insight > Users** に移動します。
2. ユーザーサマリーレポートから特定のユーザーを選択します。

#### 折れ線グラフ

折れ線グラフには、選択した期間における、選択した特定のユーザーのすべてのメトリックの概要が表示されます。

#### 現在の/終了したセッションレポート

このレポートは、選択したユーザーの現在または終了したすべてのユーザーセッションに関連しています。これらのメトリックは、開始時刻、セッションの再接続、およびACRカウントで並べ替えることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| セッションID | ICAセッションの一意のID。 |
| セッションタイプ | アプリケーション/デスクトップ。 |
| 状態 | アクティブ/非アクティブセッションの場合は緑/赤。 |
| ホスト遅延 | サーバーネットワークによって引き起こされる、NetScalerインスタンスを通過するICAトラフィックの平均遅延。 |
| インターバルあたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| セッション帯域幅 | 時間間隔に関係なくセッションによって消費された帯域幅。 |
| インターバルあたりのバイト数 | その特定の時間間隔中にセッションによって消費されたバイト数。 |
| 開始時刻 | セッション開始時刻。 |
| アップタイム | セッション期間。 |
| クライアントIPアドレス | エンドユーザーIP。 |
| サーバーIPアドレス | バックエンド/シトリックス バーチャル アプリ サーバー アイピー。 |
| NetScaler IPアドレス | NetScaler管理IP (NSIP)。 |
| クライアントの種類 | ワークスペースの種類 - Citrix Windows Client など |
| クライアントバージョン | ワークスペースバージョン。 |
| MSI | ブール値 (はい/いいえ)。セッションがマルチストリームICAであるかどうかを示します。 |
| セッションの再接続 | セッションが再接続された回数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| ACRカウント | クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。 |
| ユーザーアクセスタイプ | ICAセッションのアクセスモードを表示します。例: NetScaler Gatewayユーザー/透過モード。 |
| 国 | セッションが確立された国。 |
| 地域 | セッションが確立された地域。 |
| 市 | セッションが確立された市。 |
| USBステータス | アクティブ/非アクティブ - 緑/赤。 |
| 承認されたUSBインスタンスの数 | 承認されたUSBインスタンスの数。 |
| 拒否されたUSBインスタンスの数 | 拒否されたUSBインスタンスの数。 |
| 停止されたUSBインスタンスの数 | 停止されたUSBインスタンスの数。 |
| クライアントホスト名 | クライアントのホスト名です。 |
| HAフェイルオーバー数 | HAフェイルオーバーが発生した回数。 |
| 終了理由 | セッション終了の理由を表示します。例: ICAセッションタイムアウト、ユーザーによるセッション終了。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作する際に、ユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側で発生する遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側で発生する遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| 合計バイト数 | 選択した期間中にユーザーが消費した合計バイト数。 |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側ゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側ゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |

### HDX INSIGHTにおけるEDTのサポート

NetScaler Consoleは、HDX Insightの分析を表示するために、エンライトンデータトランスポート(EDT) をサポートするようになりました。つまり、NetScaler ConsoleはUDPとTCPの両方のプロトコルをサポートしています。NetScaler GatewayのEDTサポートにより、Citrix Workspaceを実行しているユーザーに対して、仮想デスクトップのセッション内ユーザーエクスペリエンスが高精細になります。

HDX Insightは、アクティブセッションレポートの一部として、EDTセッションと非EDTセッションの数を表示するようになりました。ユーザーテーブルには、システム内のすべてのユーザーの詳細なレポートが表示されます。このテーブルには、WAN遅延、DC遅延、再送信、RTOなどのメトリックが表示されます。これらのメトリックの一部は、現在TCPスタックから計算されているため、EDTセッションを持つユーザーには利用できません。したがって、それらは「NA」と表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDXインサイト(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-edt-support-1.png)

新しいドーナツチャートが導入され、ユーザーが消費した帯域幅と、ユーザーが使用するプロトコルの種類に基づいた合計バイト数を確認できるようになりました。

EDT(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-edt-support-2.png)

**NetScaler Console 12.0以降で利用可能なHDX Insightメトリック:**

| L7クライアント側遅延 | ICAクライアントとNETSCALERインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCITRIX以外のデバイスが存在する場合に役立ちます。 |
|---|---|
| L7サーバー側遅延 | NetScalerデバイスとCitrix Virtual App間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。 |
| 最大違反遅延 | 設定された時間間隔で定義されたしきい値の違反が発生した場合のL7遅延の最高値。 |
| 平均違反遅延 | システムが「L7遅延違反」状態にある場合のL7遅延の平均値。 |
| L7しきい値違反回数 | L7しきい値違反が発生した回数。 |

現在のセッション(/en-us/netscaler-application-delivery-management-software/media/hdx-current-sessions-1.png)

### デスクトップユーザー

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する洞察を提供します。これらのメトリックは、デスクトップ起動回数と帯域幅でソートできます。

| メトリック | 説明 |
|---|---|
| 名前 | シトリックス バーチャルデスクトップ の名前。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| デスクトップ起動回数 | デスクトップが起動された回数。 |
| 帯域幅 | 選択された時間間隔中のエンドツーエンド通信に使用された1秒あたりの合計バイト数。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーへの遅延。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーへの遅延。 |
| ICA RTT | ICA RTTは、ユーザーがそれぞれCitrix Virtual AppsまたはCitrix Virtual Desktopsでホストされているアプリケーションまたはデスクトップを操作している間に経験する画面の遅延です。 |



アプリケーション

アクティブ、合計セッション起動数、合計アプリ起動数、および起動時間でソートされたアプリを表す棒グラフ。



インスタンス

アクティブなアプリと合計アプリでソートされたNetScalerインスタンスを表す棒グラフ



チャネル

チャネルは、ドーナツグラフの形式で、各ICA仮想チャネルによって消費される全体的な帯域幅または合計バイト数を表します。帯域幅または合計バイト数でメトリックをソートすることもできます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ユーザーエージェント

ユーザーエージェントは、ドーナツグラフの形式で、各エンドポイントによって消費される全体的な帯域幅/合計バイト数を表します。帯域幅または合計バイト数でメトリックをソートすることもできます。



### ユーザーセッションごとの表示

ユーザーセッションごとの表示では、特定の選択されたユーザーのセッションに関するレポートが提供されます。

**選択したユーザーのセッションのメトリックを表示するには：**

1. **Gateway > HDX Insight > Users** に移動します。
2. **User Summary Report** セクションから特定のユーザーを選択します。
3. **Current Sessions** または **Terminated Sessions** 列からセッションを選択します。

### タイムラインチャート

| メトリック | 説明 |
|---|---|
| セッションの再接続 | この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。 |
| ACRカウント | この数値は、アクティブなCitrix Virtual Appsセッションの数を示します。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppsまたはDesktopsでホストされているアプリケーションまたはデスクトップを操作する際にユーザーが経験する画面の遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。 |
| セッション帯域幅 | 時間間隔に関係なく、セッションによって消費される帯域幅。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| サーバー側再送信 | NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。 |
| クライアント側再送信 | NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。 |
| クライアント側高速RTO | NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。 |
| サーバー側高速RTO | NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。 |
| 間隔あたりの帯域幅 | その特定の時間間隔中にセッションによって消費された帯域幅。 |
| サーバー側のゼロウィンドウサイズイベント | このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。 |
| クライアント側のゼロウィンドウサイズイベント | このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。 |

タイムラインチャート (/en-us/netscaler-application-delivery-management-software/media/hdx-timeline-chart.png)

### アクティブなアプリケーション

**アクティブなアプリケーション**セクションには、選択したユーザーのアクティブなアプリケーションが表示されます。これらのアプリケーションは、アクティブなセッション数と起動期間でソートすることもできます。

アクティブなアプリケーション (/en-us/netscaler-application-delivery-management-software/media/hdx-active-application.png)

### 関連セッション

関連セッションセクションには、選択したユーザーのセッションの関連セッションが表示されます。関連性は、共通サーバーまたは共通NetScalerとして選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

関連セッション (/en-us/netscaler-application-delivery-management-software/media/hdx-related-sessions.png)

## インスタンスビューのレポートとメトリック

インスタンスビューのレポートとメトリックは、NetScalerインスタンスに焦点を当てています。

### インスタンスビューに移動するには：

1. **Gateway > HDX™ Insight > Instances** に移動します。

### インスタンスサマリービュー

このビューは、NetScaler Consoleに追加されたすべてのNetScalerインスタンスのレポートを表示するため、サマリービューと呼ばれます。

明示的に言及されていない限り、すべてのメトリック/レポートには、選択された期間に対応する値が表示されます。

#### インスタンス棒グラフ

このグラフは、グラフキャンバスの右上にあるリストから選択できる、インスタンスと合計セッション起動数および合計アプリを表示します。

棒グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-instance-bar-graph.png)

#### インスタンス/アクティブインスタンスサマリーレポート

| メトリック | 説明 |
|---|---|
| 名前 | NetScalerインスタンスのホスト名。 |
| IPアドレス | NetScalerのIPアドレス。 |
| セッション起動総数 | 指定された時間間隔中に作成された一意のユーザーセッションの総数。 |
| アプリケーション総数 | 指定された時間間隔中に起動された一意のアプリケーションの総数。 |
| タイプ | 該当なし |

サマリーレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive-summary.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### しきい値レポート

しきい値レポートは、選択した期間にエンティティとしてインスタンスが選択された場合に違反したしきい値の数を表します。詳細については、しきい値とアラートの作成方法を参照してください。

### スキップされたフロー

スキップされたフローとは、ICA接続の解析をスキップしたレコードです。これは、サポートされていないCitrix Virtual Apps and Desktopsのバージョン、サポートされていないワークスペースのバージョンまたはワークスペースタイプを使用しているなど、複数の理由で発生する可能性があります。この表には、IPアドレスとスキップされたフローの数が表示されます。これらのワークスペースは、ホワイトリストに登録されたワークスペースの一部ではない可能性があります。したがって、これらのセッションは監視からスキップされます。

ICA解析に関連する問題の詳細については、「**エラー\! ハイパーリンク参照が無効です**」を参照してください。

スキップされたフロー(/en-us/netscaler-application-delivery-management-software/media/hdx-skipped-flow.png)

### ワールドビュー

HDX Insightのワールドマップビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者はシステムのワールドビューを表示し、地域をクリックすることで特定の国、さらに都市へとドリルダウンできます。管理者はさらにドリルダウンして、都市や州ごとの情報を表示できます。NetScalerバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightのワールドマップでは以下の詳細を表示でき、各メトリックの密度はヒートマップ形式で表示されます。

- ICA® RTT
- WAN遅延
- DC遅延
- 帯域幅
- 合計バイト数

## インスタンスごとのビュー

インスタンスごとのビューでは、特定の選択されたNetScalerインスタンスの詳細なエンドユーザーエクスペリエンスレポートが提供されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**インスタンスビューに移動するには：**

1. **Gateway > HDX Insight > Instances** に移動します。
2. **インスタンスサマリーレポート**から特定のインスタンスを選択します。

### 折れ線グラフ

| メトリック | 説明 |
| --- | --- |
| IPアドレス | これは、選択されたインスタンスのNetScaler IPアドレスを表します。 |
| 合計セッション起動数 | 指定された時間間隔におけるアクティブなCitrix Virtual Appセッションの合計数。 |
| 合計アプリ数 | 指定された時間間隔に起動された一意のアプリケーションの合計数。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart-4.png)

### アプリケーション棒グラフ

アクティブなアプリ、合計セッション起動数、合計アプリ起動数、または起動期間の基準に基づいて、上位5つのアプリケーションを表示します。

アプリケーション棒グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-applications-bar-graph.png)

### ユーザー棒グラフ

ユーザー棒グラフは、以下の基準に基づいて上位5人のユーザーを表示します。

- 帯域幅
- WAN遅延
- DC遅延
- ICA RTT

ユーザー棒グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-users-bar-graph.png)

### デスクトップユーザーレポート

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する洞察を提供します。これらのメトリックは、デスクトップ起動回数と帯域幅でソートできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| メトリック | 説明 |
| --- | --- |
| 名前 | シトリックス バーチャル デスクトップの名前。 |
| デスクトップ起動回数 | デスクトップが起動された回数。 |
| 帯域幅 | 選択した時間間隔中にエンドツーエンド通信にかかった1秒あたりの合計バイト数。 |
| DC遅延 | ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーへの遅延です。 |
| WAN遅延 | ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーへの遅延です。 |
| ICA RTT | ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作しているときにユーザーが経験する画面の遅延です。 |

デスクトップユーザーレポート(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)

### ワールドビュー

HDX Insightのワールドマップビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者は、システム全体のワールドビューを表示し、地域をクリックして特定の国、さらに都市へとドリルダウンできます。管理者は、さらに都市や州ごとの情報を表示するためにドリルダウンできます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightのワールドマップでは以下の詳細を表示でき、各メトリックの密度はヒートマップ形式で表示されます。

- ICA RTT
- WAN遅延
- DC遅延
- 帯域幅

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 合計バイト数

ワールドビュー(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

### ライセンスビューレポートとメトリクス

ライセンスビューには、NetScaler Gatewayのライセンス情報が表示されます。

**ライセンスビューに移動するには：**

1. **Gateway > HDX™ Insight > Licenses** に移動します。

**折れ線グラフ**

| メトリクス | 説明 |
| --- | --- |
| 使用中のライセンス | 選択した期間中に使用されているNetScaler Gateway CCUライセンス。各カウントはユーザーセッションの数を表します。これは、そのユーザーが起動したアプリケーションおよびデスクトップセッションとは独立しています。 |
| 合計ライセンス数 | お客様が利用できるNetScaler Gateway CCUライセンスの総数。 |

折れ線グラフ(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart.png)

**しきい値レポート**

しきい値レポートは、選択した期間中に*エンティティ*が「ライセンス」として選択された場合に違反したしきい値の数を表します。詳細については、しきい値とアラートの作成方法を参照してください。

## HDX™ Insight の問題のトラブルシューティング

HDX Insight ソリューションが期待どおりに機能しない場合、問題は以下のいずれかにある可能性があります。トラブルシューティングについては、それぞれのセクションのチェックリストを参照してください。

- HDX Insight の構成。
- NetScaler と NetScaler Console 間の接続。
- NetScaler での HDX/ICA トラフィックのレコード生成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console でのレコードの入力。

### HDX Insight 構成チェックリスト

- NetScaler で AppFlow 機能が有効になっていることを確認します。詳細については、「AppFlow の有効化」を参照してください。
- NetScaler の実行中の構成で HDX Insight 構成を確認します。

  `show running | grep -i <appflow_policy>` コマンドを実行して HDX Insight 構成を確認します。バインドタイプが ICA REQUEST であることを確認してください。例:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type ICA_REQUEST
  ```

  透過モードの場合、バインドタイプは ICA_REQ_DEFAULT である必要があります。例:

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- シングルホップ/Access Gateway またはダブルホップ展開の場合、HDX Insight AppFlow ポリシーが HDX/ICA トラフィックが流れる VPN 仮想サーバーにバインドされていることを確認してください。
- 透過モードまたは LAN ユーザーモードの場合、ICA® ポート 1494 および 2598 が設定されていることを確認してください。
- NetScaler GatewayまたはVPN仮想サーバーの `appflowlog` パラメータが、Access Gatewayまたはダブルホップ展開で有効になっているか確認します。詳細については、仮想サーバーのAppFlowを有効にするを参照してください。
- ダブルホップNetScalerで「Connection Chaining」が有効になっているか確認します。詳細については、NetScaler Gatewayアプライアンスを構成してデータをエクスポートするを参照してください。
- HAフェイルオーバー後にHDX Insightの詳細がスキップ解析される場合は、ICAパラメータ「enableSRonHAFailover」が有効になっているか確認します。詳細については、NetScaler高可用性ペアでのセッション信頼性を参照してください。

### NetScalerとNetScaler Console間の接続チェックリスト

- NetScalerでAppFlowコレクターのステータスを確認します。詳細については、NetScalerとAppFlowコレクター間の接続ステータスを確認する方法を参照してください。
- HDX Insight AppFlow®ポリシーのヒットを確認します。

  AppFlowポリシーのヒットを確認するには、コマンド `show appflow policy <policy_name>` を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUIで**設定 > AppFlow > ポリシー**に移動して、AppFlowポリシーのヒットを確認することもできます。

- ファイアウォールがAppFlowポート4739または5557をブロックしていないか検証します。

### NetScalerにおけるHDX/ICAトラフィックのレコード生成チェックリスト

ログ検証のためにコマンド`tail -f /var/log/ns.log | grep -i "default ICA Message"`を実行します。生成されたログに基づいて、この情報をトラブルシューティングに利用できます。

- ログ: **ICA接続の解析をスキップしました - このホストではHDX Insightはサポートされていません**

  **原因**: サポートされていないCitrix Virtual Apps and Desktopsのバージョン

  **回避策**: Citrix Virtual Apps and Desktopsサーバーをサポートされているバージョンにアップグレードします。

- ログ: **クライアントタイプ0x53を受信しました、サポートされていません**

  **原因**: Citrix Workspaceのサポートされていないバージョン

  **解決策**: Citrix Workspaceをサポートされているバージョンにアップグレードしてください。詳細については、Citrix Workspaceアプリを参照してください。

- ログ: **Expand Packetからのエラー - このフローのすべてのHDX処理をスキップしています**

  **原因**: ICAトラフィックの解凍に関する問題

  **解決策**: 新しいセッションが確立されるまで、このICAセッションのレポートは利用できません。

- ログ: **無効な遷移: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  **原因**: ICAハンドシェイクの解析に関する問題

  **解決策**: 新しいセッションが確立されるまで、この特定のICAセッションのレポートは利用できません。

- ログ: **EUEM ICA RTTがありません**

  **原因**: エンドユーザーエクスペリエンス監視チャネルデータを解析できません

  **解決策**: Citrix Virtual Apps and Desktopsサーバーでエンドユーザーエクスペリエンス監視サービスが開始されていることを確認してください。Citrix Workspaceアプリのサポートされているバージョンを使用していることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ログ: **無効なチャネルヘッダー**

  **原因**: チャネルヘッダーを識別できません

  **解決策**: 新しいセッションが確立されるまで、この特定のICAセッションのレポートは利用できません。

- ログ: **スキップコード**

  スキップコードに以下のいずれかの値が表示される場合、Insight の詳細はスキップ解析されます。

  スキップコード0は、レコードがNetScalerから正常にエクスポートされたことを示します。

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| 100 | NS_ICA_ERR_NULL_FRAG | ICAフラグメントの処理エラー。メモリの状態が原因である可能性が高い |
| 101 | NS_ICA_ERR_INVALID_HS_CMD | 無効なハンドシェイクコマンドを受信しました |
| 102 | NS_ICA_ERR_REDUC_PARAM_CNT | V3エキスパンダの初期化に無効なパラメータが指定されました |
| 103 | NS_ICA_ERR_REDUC_INIT | V3エキスパンダーを正しく初期化できません |
| 104 | NS_ICA_ERR_REDUC_PARAM_BYTES | チャネルにコーダーを割り当てるのに十分なバイトがありません |
| 105 | NS_ICA_ERR_INVALID_CHANNEL | 無効なICAチャネル番号 |
| 106 | NS_ICA_ERR_INVALID_DECODER | チャネルに指定されたデコーダーが無効です |
| 107 | NS_ICA_ERR_INVALID_TW_PARAM | Thinwireチャネルに指定されたパラメータ数が無効です |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| 108 | NS_ICA_ERR_INVALID_TW_DECODER | Thinwireチャネルのデコーダーが無効です |
| 109 | NS_ICA_ERR_REDUC_NO_DECODER | チャネルにデコーダーが定義されていません |
| 110 | NS_ICA_ERR_REDUC_V3_EXPANDER | チャネルデータの展開に失敗しました |
| 111 | NS_ICA_ERR_REDUC_BYTES_V3_OOR | エキスパンダーエラー: 消費されたバイト数が利用可能なバイト数を超えています |
| 112 | NS_ICA_ERR_REDUC_BYTES_OOR | エラー: 非圧縮データのオーバーラン |
| 113 | NS_ICA_ERR_REDUC_INVALID_CMD | 未定義のエクスパンダーコマンド |
| 114 | NS_ICA_ERR_CGP_FILL_HOLE | 分割されたCGPフレームの処理中にエラーが発生しました |
| 115 | NS_ICA_ERR_MEM_NSB_ALLOC | NSB割り当てエラー – メモリ不足のため |
| 116 | NS_ICA_ERR_MEM_REDUC_CTX_ALLOC | エクスパンダーコンテキストのメモリ割り当てエラー |
| 117 | NS_ICA_ERR_ICA_OLD_SERVER | 古いサーバー、機能ブロックはサポートされていません |
| 118 | NS_ICA_ERR_PIR_MANY_FRAG | パケット初期化要求が断片化されており、処理できません |
| 119 | NS_ICA_ERR_INIT_ICA_CAPS | ICA機能の初期化エラー |
| 120 | NS_ICA_ERR_NO_MSI_SUPPORT | ホストはMSI機能をサポートしていません。XenAppバージョン6.5未満または |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| | | XenDesktopバージョン5.0未満の場合を示します |
| 121 | NS_ICA_ERR_CGP_INVALID_CMD | 無効なCGPコマンドが検出されました |
| 122 | NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES | チャネル上のバイト不足 |
| 123 | NS_ICA_ERR_CHANNEL_DATA | EUEM、CONTROL、またはSEAMLESSチャネル上のデータが不正です |
| 124 | NS_ICA_ERR_INVALID_PURE_CMD | pure ICAチャネルデータを処理中に無効なコマンドを受信しました |
| 125 | NS_ICA_ERR_INVALID_PURE_LEN0 | pure ICAチャネルデータを処理中に無効な長さが検出されました |
| 126 | NS_ICA_ERR_INVALID_PURE_LEN | PURE ICAチャネルデータを処理中に無効な長さが検出されました |
| 127 | NS_ICA_ERR_INVALID_CLNT_DATA | クライアントから受信したデータ長が無効です |
| 128 | NS_ICA_ERR_MSI_GUID_SZ | MSI GUIDサイズのエラー |
| 129 | NS_ICA_ERR_INVALID_CHANNEL_HEADER | 無効なチャネルヘッダーを検出しました |
| 130 | NS_ICA_ERR_CGP_PARSE_RECONNECT_ID | 再接続されたセッションの取得に失敗しました |
| 131 | NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT | SRの無効化中にエラーが発生しました |
| 132 | NS_ICA_ERR_REDUC_NOT_V3 | サポートされていないICA Reducerバージョン |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| 133 | NS_ICA_ERR_HS_COMPRESSION_DISABLED | 圧縮が無効になっています。ホストによって認識されません。 |
| 134 | NS_ICA_ERR_IDENT_PROTO | ICAまたはCGPプロトコルを識別できません。不正なワークスペースで発生します。 |
| 135 | NS_ICA_ERR_INVALID_SIGNATURE | 不正なICA署名またはマジック文字列 |
| 136 | NS_ICA_ERR_PARSE_RAW | ICAハンドシェイクパケットの解析中にエラーが発生しました |
| 137 | NS_ICA_ERR_INCOMPLETE_PKT | ハンドシェイクで不完全なパケットを受信しました |
| 138 | NS_ICA_ERR_ICAFRAME_TOO_LARGE | ICAフレームが大きすぎます。1460バイトを超えています |
| 139 | NS_ICA_ERR_FORWARD | ICAデータの転送中にエラーが発生しました |
| 140 | NS_ICA_ERR_MAX_HOLES | CGPコマンドがサポートされている制限を超えて分割されているため、処理できません |
| 141 | NS_ICA_ERR_ASSEMBLE_FRAME | ICAフレームを正しく再構築できません |
| 142 | NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION | このワークスペース（クライアント）は許可リストにないため、ICA解析をスキップしました |
| 143 | NS_ICA_ERR_LOOKUP_RECONNECT_ID | クライアントの再接続クッキーの解析状態を検出できません |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| 144 | NS_ICA_ERR_SYNCUP_RECONNECT_ID | クライアント再接続後に無効な再接続クッキーの長さが検出されました |
| 145 | NS_ICA_ERR_INVALID_RECONNECT_ID | クライアントの再接続クッキーが必要な制約を満たしていません |
| 146 | NS_ICA_ERR_INVALID_CLIENT_VERSION | クライアントから無効なワークスペースバージョン文字列が受信されました |
| 147 | NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID | クライアントから無効な製品IDが受信されました |
| 148 | NS_ICA_ERR_V3_HDR_CORRUPT_LEN | 展開後のチャネル長が無効です |
| 149 | NS_ICA_ERR_SPECIAL_THINWIRE | 解凍エラー |
| 150 | NS_ICA_ERR_SEAMLESS_INSUFFBYTE | シームレスコマンドに十分なバイト数が見つかりませんでした |
| 151 | NS_ICA_ERR_EUEM_INSUFFBYTE | EUEMコマンドに十分なバイト数が見つかりませんでした |
| 152 | NS_ICA_ERR_SEAMLESS_INVALID_EVENT | シームレスチャネル解析のイベントが無効です |
| 153 | NS_ICA_ERR_CTRL_INVALID_EVENT | CTRLチャネル解析用の無効なイベント |
| 154 | NS_ICA_ERR_EUEM_INVALID_EVENT | EUEMチャネル解析用の無効なイベント |
| 155 | NS_ICA_ERR_USB_INVALID_EVENT | USBチャネル解析用の無効なイベント |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| 156 | NS_ICA_ERR_PURE_INVALID_EVENT | pureチャネル解析用の無効なイベント |
| 157 | NS_ICA_ERR_VCP_INVALID_EVENT | 仮想チャネル解析用の無効なイベント |
| 158 | NS_ICA_ERR_ICAP_INVALID_EVENT | ICAデータ解析の無効なイベント |
| 159 | NS_ICA_ERR_CGPP_INVALID_EVENT | CGPデータ解析の無効なイベント |
| 160 | NS_ICA_ERR_BASICCRYPT_INVALIDSTATE | 基本暗号化における暗号化コマンドの無効な状態 |
| 161 | NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD | 基本暗号化における無効な暗号化コマンド |
| 162 | NS_ICA_ERR_ADVCRYPT_INVALIDSTATE | RC5暗号化における暗号化コマンドの無効な状態 |
| 163 | NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD | RC5暗号化における無効な暗号コマンド |
| 164 | NS_ICA_ERR_ADVCRYPT_ENC | RC5暗号化/復号化のエラー |
| 165 | NS_ICA_ERR_ADVCRYPT_DEC | RC5暗号化/復号化のエラー |
| 166 | NS_ICA_ERR_SERVER_NOT_REDUCER_V3 | VDAはReducerバージョン3をサポートしていません |
| 167 | NS_ICA_ERR_CLIENT_NOT_REDUCER_V3 | ワークスペースはReducerバージョン3をサポートしていません |
| 168 | NS_ICA_ERR_ICAP_INSUFFBYTE | ICAハンドシェイクで予期しないバイト数 |
| 169 | NS_ICA_ERR_HIGHER_RECONSEQ | 再接続後のピアからのCGP再開シーケンス番号が高い |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
|---|---|---|
| 170 | NS_ICA_ERR_DESCSRINFO_ABSENT | 再接続後にICA解析状態を復元できません |
| 171 | NS_ICA_ERR_NSAP_PARSING | Insightチャネルデータの解析中にエラーが発生しました |
| 172 | NS_ICA_ERR_NSAP_APP | Insightチャネルデータからアプリの詳細を解析中にエラーが発生しました |
| 173 | NS_ICA_ERR_NSAP_ACR | InsightチャネルデータからのACR詳細の解析中にエラーが発生しました |
| 174 | NS_ICA_ERR_NSAP_SESSION_END | Insightチャネルデータからのセッション終了詳細の解析中にエラーが発生しました |
| 175 | NS_ICA_ERR_NON_NSAP_SN | Insightチャネルのサポートがないため、サービスノードでのICA解析をスキップしました |
| 176 | NS_ICA_ERR_NON_NSAP_CLIENT | NSAPはクライアントでサポートされていません |
| 177 | NS_ICA_ERR_NON_NSAP_SERVER | NSAPはVDAでサポートされていません |
| 178 | NS_ICA_ERR_NSAP_NEG_FAIL | NSAPデータネゴシエーション中のエラー |
| 179 | NS_ICA_ERR_SN_RECONNECT_TKT_FETCH | サービスノードでサービス再接続チケットの取得中にエラーが発生しました |
| 180 | NS_ICA_ERR_SN_HIGHER_RECONSEQ | サービスノードでより高い再接続シーケンス番号を受信したときにエラーが発生しました |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| スキップコード | エラーメッセージ | エラーの原因 |
| --- | --- | --- |
| 181 | NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP | 非NSAP接続に対してHDX Insightを無効にしているときにエラーが発生しました |

**サンプルログ:**

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

## エラーカウンター

ICA解析では様々なカウンターが取得されます。次の表に、ICA解析の様々なカウンターを示します。 カウンターの詳細を表示するには、コマンド`nsconmsg –g hdx –d statswt0`を実行します。

| HDXカウンター名 | 目的 | カテゴリ（統計/エラー/診断） |
| --- | --- | --- |
| hdx_tot_ica_conn | NSによって検出された純粋なICA接続の総数を示します。クライアントPCB上のICAシグネチャに基づいてICA接続が検出されるたびに増加します。 | 統計 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| HDXカウンター名 | 目的 | カテゴリ（統計/エラー/診断） |
|---|---|---|
| hdx_tot_cgp_conn | NSによって検出されたCGP接続の総数を示します（セッション信頼性ON）。クライアントPCB上のCGPシグネチャに基づいてCGP接続が検出されるたびに増加します。 | 統計 |
| hdx_dbg_tot_udt_conn | NSによって検出されたUDP ICA接続の総数を示します | 統計 |
| hdx_dbg_tot_nsap_conn | NSによって検出されたNSAPサポート接続の総数を示します | 統計 |
| hdx_tot_skip_conn | 無効なICAまたはCGP署名が原因で、パーサーによってスキップされたICA接続の数を示します。 | 統計 |
| hdx_dbg_active_conn | その時点でのアクティブなEDT/CGP/ICA接続の合計数。 | 統計 |
| hdx_dbg_active_nsap_conn | その時点でのアクティブなEDT/CGP/ICA NSAP接続の合計数。 | 統計 |
| hdx_dbg_skip_appflow_disabled | AppFlowの無効化により、セッションからAppFlowがデタッチされたインスタンスの総数 | 統計/診断 |
| hdx_dbg_transparent_user | 透過的なユーザーアクセスの総数 | 統計/診断 |
| hdx_dbg_ag_user | Access Gatewayユーザーアクセスの合計数 | 統計/診断 |
| hdx_dbg_lan_user | LANユーザーモードアクセスの合計数 | 統計/診断 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| HDXカウンター名 | 目的 | カテゴリ（統計/エラー/診断） |
|---|---|---|
| hdx_basic_enc | 基本暗号化を使用しているICA接続の数を示します | 統計/診断 |
| hdx_advanced_enc | 高度なRC5ベースの暗号化を使用しているICA接続の数を示します | 統計/診断 |
| hdx_dbg_reconnected_session | NetScalerエラーなしでクライアントからの再接続要求の合計数 | 統計/診断 |
| hdx_dbg_host_rejected_ns_reconnect | クライアントによって再接続要求が拒否されたホストの総数 | 統計/診断 |
| hdx_euem_available | エンドユーザーエクスペリエンス監視チャネルが利用可能な接続の数を示します。エンドユーザーエクスペリエンス監視チャネルは、ICA RTTなどの統計情報を収集するために必要です。 | 統計/診断 |
| hdx_err_disabled_sr | セッション信頼性は `nsapimgr` ノブを使用して無効になっています。このセッションではセッションは機能しません。 | エラー |
| hdx_err_skip_no_msi | XA/XDサーバーにMSI機能がありません。これは古いサーバーバージョンを示しており、HDX Insightはこの接続をスキップします。 | エラー |
| hdx_err_skip_old_server | 古いサポート対象外のサーバーバージョン | エラー |
| hdx_err_clnt_not_whitelist | クライアントワークスペースが許可リストにないため、 | エラー |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| HDXカウンター名 | 目的 | カテゴリ（統計/エラー/診断） |
|---|---|---|
| | HDX Insightはこの接続をスキップします | |
| hdx_sm_ica_cam_channel_disabled | SmartAccessポリシーによって無効にされたNS_ICA_CAM_CHANNELの総数 | 診断 |
| hdx_sm_ica_usb_channel_disabled | SmartAccessポリシーによって無効にされたNS_ICA_USB_CHANNELの総数 | 診断 |
| hdx_sm_ica_clip_channel_disabled | SmartAccessポリシーによって無効にされたNS_ICA_CLIP_CHANNELの総数 | 診断 |
| hdx_sm_ica_ccm_channel_disabled | SmartAccessポリシーによって無効にされたNS_ICA_CCM_CHANNELの総数 | 診断 |
| hdx_sm_ica_cdm_channel_disabled | SmartAccessポリシーによって無効化されたNS_ICA_CDM_CHANNELの総数 | 診断 |
| hdx_sm_ica_com1_channel_disabled | SmartAccessポリシーによって無効化されたNS_ICA_COM1_CHANNELの総数 | 診断 |
| hdx_sm_ica_com2_channel_disabled | SmartAccessポリシーによって無効化されたNS_ICA_COM2_CHANNELの総数 | 診断 |
| hdx_sm_ica_cpm_channel_disabled | SmartAccessポリシーによって無効化された | 診断 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| HDXカウンター名 | 目的 | カテゴリ（統計/エラー/診断） |
|---|---|---|
| | NS_ICA_CPM_CHANNELの総数 | |
| hdx_sm_ica_lpt1_channel_disabled | SmartAccessポリシーによって無効化されたNS_ICA_LPT1_CHANNELの総数 | 診断 |
| hdx_sm_ica_lpt2_channel_disabled | SmartAccessポリシーによって無効化されたNS_ICA_LPT2_CHANNELの総数 | 診断 |
| dx_dbg_sm_ica_msi_disabled | SmartAccessポリシーによってMSIが無効化されたケースの総数 | 診断 |
| hdx_sm_ica_file_channel_disabled | SmartAccessポリシーによって無効化されたNS_ICA_FILE_CHANNELの総数 | 診断 |
| hdx_dbg_usb_accept_device | 許可されたUSBデバイスの総数 | 診断 |
| hdx_dbg_usb_reject_device | 拒否されたUSBデバイスの総数 | 診断 |
| hdx_dbg_usb_reset_endpoint | リセットされたUSBエンドポイントの総数 | 診断 |
| hdx_dbg_usb_reset_device | リセットされたUSBデバイスの総数 | 診断 |
| hdx_dbg_usb_stop_device | 停止されたUSBデバイスの総数 | 診断 |
| hdx_dbg_usb_stop_device_response | 停止されたUSBデバイスからの応答総数 | 診断 |
| hdx_dbg_usb_device_gone | 消失したUSBデバイスの総数 | 診断 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| HDXカウンター名 | 目的 | カテゴリ（統計/エラー/診断） |
| --- | --- | --- |
| hdx_dbg_usb_device_stopped | 停止したUSBデバイスの総数 | 診断 |

### nstraceの検証

NetScalerから出力されるすべてのAppFlowレコードを確認するには、CFLOWプロトコルをチェックします。

### NetScaler Consoleチェックリストにおけるレコードの入力

- コマンド `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` を実行し、ログを確認してNetScaler ConsoleがAppFlowレコードを受信していることを確認します。
- NetScalerインスタンスがNetScaler Consoleに追加されていることを確認します。
- ネットスケーラー コンソールでネットスケーラー ゲートウェイ/VPN仮想サーバーがライセンスされていることを検証します。
- ダブルホップの場合、マルチホップパラメータ設定が有効になっていることを確認してください。
- ダブルホップ展開で、NetScaler Gatewayがセカンドホップに対してクリアされていることを確認してください。

### Citrixテクニカルサポートに連絡する前に

迅速な解決のために、Citrixテクニカルサポートに連絡する前に以下の情報を用意してください。

- 展開とネットワークトポロジの詳細。
- NetScalerとNetScaler Consoleのバージョン。
- Citrix Virtual Apps and Desktopsサーバーのバージョン。
- クライアントワークスペースのバージョン。
- 問題発生時のアクティブなICAセッション数。
- NetScalerコマンドプロンプトで `show techsupport` コマンドを実行して取得した技術サポートバンドル。
- NetScaler Console用に取得した技術サポートバンドル。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- すべてのNetScalerで取得されたパケットトレース。 パケットトレースを開始するには、`start nstrace -size 0'`と入力します。 パケットトレースを停止するには、`stop nstrace`と入力します。
- `show arp`コマンドを実行して、システムのARPテーブルのエントリを収集します。

### 既知の問題

HDX Insightの既知の問題については、NetScalerのリリースノートを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# インフラストラクチャ

NetScaler Consoleは、NetScalerインスタンスを検出、監視、管理するためのインフラストラクチャ管理および分析機能を提供します。以下のトピックは、NetScalerインフラストラクチャの管理に役立ちます。

- インフラストラクチャ分析
- インスタンス管理
- SSL証明書管理
- イベント
- ネットワーク機能
- ネットワークレポート
- 構成
- セキュリティアドバイザリ
- アップグレードアドバイザリ
- オーケストレーション

## インフラストラクチャ分析

ネットワーク管理者にとって重要な目標の1つは、NetScalerインスタンスを監視することです。NetScalerインスタンスは、それを通じてアクセスされるアプリケーションやデスクトップの使用状況とパフォーマンスに関する興味深い洞察を提供します。管理者はNetScalerインスタンスを監視し、各NetScalerインスタンスによって処理されるアプリケーションフローを分析する必要があります。これにより、アプリケーションの使用状況やパフォーマンスに影響を与える可能性のある、構成、セットアップ、接続、証明書などの問題に対処できます。たとえば、アプリケーショントラフィックパターンの突然の変化は、SSLプロトコルの無効化のようなSSL構成の変更が原因である可能性があります。管理者は、以下のことを確実にするために、これらのデータポイント間の相関関係を迅速に特定できる必要があります。

- アプリケーションの可用性が最適な状態であること
- リソース消費、ハードウェア、容量、または構成変更の問題がないこと
- 未使用のインベントリがないこと
- 期限切れの証明書がないこと

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インフラストラクチャ分析機能は、複数のデータソースを関連付け、インスタンスの健全性を定義する測定可能なスコアとして定量化することで、データ分析プロセスを簡素化します。この機能により、管理者は問題があるかどうか、問題の原因、および実行可能な対処法を理解するための単一の接点を得ることができます。

## インフラストラクチャ分析

NetScaler Consoleのインフラストラクチャ分析機能は、NetScalerインスタンスから収集されたすべてのデータを照合し、インスタンスの健全性を定義する**インスタンススコア**として定量化します。インスタンススコアは、表形式ビューまたはサークルパック視覚化として要約されます。インフラストラクチャ分析機能は、インスタンスで問題を引き起こした、または引き起こす可能性のある要因を視覚化するのに役立ちます。この視覚化は、問題とその再発を防ぐために実行する必要があるアクションを決定するのにも役立ちます。

## インスタンススコア

インスタンススコアは、NetScalerインスタンスの健全性を示します。スコアが100の場合、問題のない完全に健全なインスタンスであることを意味します。インスタンススコアは、インスタンス上のさまざまなレベルの潜在的な問題を捉えます。これはインスタンスの健全性を定量的に測定するものであり、複数の「健全性インジケーター」がスコアに貢献します。

**健全性インジケーター**はインスタンススコアの構成要素であり、スコアは、事前定義された「監視期間」に対して、その時間枠で検出されたすべてのインジケーターに基づいて定期的に計算されます。現在、Infrastructure analytics は、インスタンスから収集されたデータに基づいて、1時間ごとにインスタンススコアを計算します。 インジケーターは、インスタンス上の以下のいずれかのカテゴリに属するアクティビティ（イベントまたは問題）として定義できます。

- システムリソースインジケーター
- 重大イベントインジケーター
- SSL構成インジケーター
- 設定偏差インジケーター

## 健全性インジケーター

- システムリソースインジケーター

  NetScalerインスタンスで発生する可能性があり、NetScaler Consoleによって監視される重要なシステムリソースの問題は次のとおりです。

  - **高いCPU使用率**。NetScalerインスタンスでCPU使用率が上限しきい値を超えました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **高いメモリ使用率**。NetScalerインスタンスでメモリ使用率が上限しきい値を超えました。
- **高いディスク使用率**。NetScalerインスタンスでディスク使用率が上限しきい値を超えました。
- **ディスクエラー**。NetScalerインスタンスがインストールされているハイパーバイザーのハードディスク0またはハードディスク1にエラーがあります。
- **電源障害**。NetScalerインスタンスへの電源供給が失敗したか、切断されました。
- **SSLカード障害**。インスタンスにインストールされているSSLカードが故障しました。
- **フラッシュエラー**。NetScalerインスタンスでコンパクトフラッシュエラーが検出されました。
- **NIC破棄**。NetScalerインスタンスでNICカードによって破棄されたパケットが上限しきい値を超えました。

これらのシステムリソースエラーの詳細については、「」(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management.html#how-to-use-the-instance-dashboard)を参照してください。

- 重大なイベントインジケーター

  NetScaler Consoleのイベント管理機能のイベントで、重大度「クリティカル」に設定されているものが、以下の重要なイベントとして識別されます。

  - **HA同期失敗**。高可用性構成のNetScalerインスタンス間の構成同期が、セカンダリサーバーで失敗しました。
  - **HAハートビートなし**。高可用性構成のNetScalerインスタンスのペアにおけるプライマリサーバーが、セカンダリサーバーからハートビートを受信していません。
  - **HAセカンダリ状態不良**。高可用性構成のNetScalerインスタンスのペアにおけるセカンダリサーバーが、ダウン、不明、またはセカンダリ維持状態です。
  - **HAバージョン不一致**。高可用性構成のNetScalerインスタンスのペアにインストールされているNetScalerソフトウェアイメージのバージョンが一致しません。
  - **クラスター同期失敗**。クラスターモードのNetScalerインスタンス間の構成同期が失敗しました。
  - **クラスターバージョン不一致**。クラスターモードのNetScalerインスタンスにインストールされているNetScalerソフトウェアイメージのバージョンが一致しません。
  - **クラスター伝播失敗**。クラスター内のすべてのインスタンスへの構成の伝播が失敗しました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注**
>
> イベントの重大度レベルを変更することで、重要なSNMPイベントのリストを作成できます。重大度レベルの変更方法の詳細については、「」(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/events/how-to-modify-the-reported-severity-of-events.html)を参照してください。

NetScaler Consoleのイベントの詳細については、「」(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/events.html)を参照してください。

- SSL構成インジケーター
  - **推奨されない鍵強度**。SSL証明書の鍵強度がNetScaler®の標準に準拠していません
  - **推奨されない発行者**。SSL証明書の発行者がCitrixによって推奨されていません。
  - **SSL証明書の期限切れ**。NetScalerインスタンスにインストールされているSSL証明書の期限が切れました。
  - **SSL証明書の期限が間近**。NetScalerインスタンスにインストールされているSSL証明書が、今後1週間以内に期限切れになります。
  - **推奨されないアルゴリズム**。NetScalerインスタンスにインストールされているSSL証明書の署名アルゴリズムが、NetScalerの標準に準拠していません。

SSL証明書の詳細については、SSLダッシュボードを参照してください。

- 構成の逸脱インジケーター
  - **構成ドリフトテンプレート**。特定のインスタンスで監査したい特定の構成で作成した監査テンプレートから、構成にドリフト（未保存の変更）があります。
  - **構成ドリフトのデフォルト**。デフォルトの構成ファイルから、構成にドリフト（未保存の変更）があります。

構成の逸脱に関する詳細、および構成の逸脱を確認するための監査レポートの実行方法については、監査レポートの表示を参照してください。

## NetScalerの容量の問題を表示する

NetScalerインスタンスが利用可能な容量のほとんどを消費すると、クライアントトラフィックの処理中にパケットドロップが発生する可能性があります。この問題は、NetScalerインスタンスのパフォーマンス低下を引き起こします。このようなNetScalerの容量の問題を理解することで、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerのパフォーマンスを安定させるために、追加のライセンスを事前に割り当てることができます。

NetScalerの容量の問題を表示するには、,

1. **インフラストラクチャ > インフラストラクチャ分析** に移動します。
2. 容量の問題を表示したいインスタンスを展開します。

NetScaler Consoleは、NetScalerインスタンスから5分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンターの増分が存在する場合は表示します。問題は、以下の容量パラメーターに基づいて分類されます。

- **スループット制限に到達** – スループット制限に到達した後にインスタンスでドロップされたパケットの数。
- **PE CPU制限に到達** - PE CPU制限に到達した後にすべてのNICでドロップされたパケットの数。
- **PPS制限に到達** – PPS制限に到達した後にインスタンスでドロップされたパケットの数。
- **SSLスループットレート制限** – SSLスループット制限に達した回数。
- **SSL TPSレート制限** – SSL TPS制限に達した回数。

NetScaler Consoleは、定義された容量しきい値に基づいてインスタンススコアを計算します。

- 低しきい値 – 1パケットのドロップまたはレート制限カウンターの増分
- 高しきい値 – 10000パケットのドロップまたはレート制限カウンターの増分

したがって、NetScalerインスタンスが容量しきい値を超えると、インスタンススコアに影響が及びます。

パケットがドロップしたり、レート制限カウンターが増加したりすると、`NetScalerCapacityBreach`カテゴリでイベントが生成されます。これらのイベントを表示するには、**アカウント > システムイベント**に移動します。

### ヘルスインジケーターの値

インジケーターは、その値に基づいて、高優先度インジケーターと低優先度インジケーターに次のように分類されます。

同じグループ内のヘルスインジケーターには、異なる重みが割り当てられています。あるインジケーターは、別のインジケーターよりもインスタンススコアの低下に大きく寄与する可能性があります。たとえば、高いメモリ使用量は、高いディスク使用量、高いCPU使用量、NIC破棄よりも

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンススコアを大きく低下させます。インスタンスで検出されるインジケーターの数が多いほど、インスタンススコアは低くなります。

インジケーターの値は、以下のルールに基づいて計算されます。インジケーターは、次の3つのいずれかの方法で検出されたと見なされます。

1. **アクティビティに基づく**。たとえば、インスタンスで電源障害が発生するたびにシステムリソースインジケーターがトリガーされ、このインジケーターはインスタンススコアの値を低下させます。インジケーターがクリアされるとペナルティがクリアされ、インスタンススコアが増加します。
2. **しきい値の違反に基づく**。たとえば、NICカードがパケットを破棄し、しきい値レベルが違反されたときにシステムリソースインジケーターがトリガーされます。
3. **低および高しきい値の違反に基づく**。ここでは、インジケーターは2つの方法でトリガーできます。
    - インジケーターの値が低しきい値と高しきい値の間にある場合、インスタンススコアに部分的なペナルティが課されます。
    - 値が高しきい値を超えた場合、インスタンススコアに完全なペナルティが課されます。
    - 値が低しきい値を下回った場合、インスタンススコアにペナルティは課されません。

たとえば、CPU使用率は、使用量の値が低しきい値を超えたとき、および値が高しきい値を超えたときにトリガーされるシステムリソースインジケーターです。

## インフラストラクチャ分析ダッシュボード

**インフラストラクチャ > インフラストラクチャ分析**に移動します。

インフラストラクチャ分析は、**サークルパック**形式または**表形式**で表示できます。これら2つの形式を切り替えることができます。



- 表形式ビューでは、検索バーにホスト名またはIPアドレスを入力してインスタンスを検索できます。
- デフォルトでは、インフラストラクチャ分析ページには、ページの右側にサマリーパネルが表示されます。
- **設定**アイコンをクリックして、**設定**パネルを表示します。
- どちらの表示形式でも、サマリーパネルにはネットワーク内のすべてのインスタンスの詳細が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# サークルパックビュー

サークルパッキング図は、インスタンスグループを密に組織化された円として示します。これらは多くの場合、より小さなインスタンスグループが同じカテゴリの他のグループと類似した色で表示されるか、より大きなグループ内にネストされている階層を示します。サークルパックは階層データセットを表し、階層内の異なるレベルとそれらがどのように相互作用するかを示します。

## インスタンスの円

**色**。各インスタンスは、サークルパックで色付きの円として表示されます。円の色は、そのインスタンスの健全性を示します。

- **緑** - インスタンススコアが100から80の間です。インスタンスは正常です。
- **黄** - インスタンススコアが80から50の間です。いくつかの問題が確認されており、レビューが必要です。
- **赤** - インスタンススコアが50未満です。そのインスタンスで複数の問題が確認されているため、インスタンスは危機的な状態にあります。

インスタンスの円(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-3.png)

**サイズ**。これらの色付きの円のサイズは、そのインスタンスに構成されている仮想サーバーの数を示します。円が大きいほど、仮想サーバーの数が多いことを示します。

各インスタンスの円（色付きの円）にマウスポインターを合わせると、概要が表示されます。ホバーツールチップには、インスタンスのホスト名、アクティブな仮想サーバーの数、およびそのインスタンスに構成されているアプリケーションの数が表示されます。

インスタンスの円(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-4.png)

## グループ化されたインスタンスの円

サークルパックは、当初、以下の基準に基づいてグループ化、ネスト、または別の円の中にパックされたインスタンスの円で構成されています。

- デプロイされているサイト
- デプロイされているインスタンスのタイプ - VPX、MPX、SDX、およびCPX
- NetScalerインスタンスの仮想モデルまたは物理モデル
- インスタンスにインストールされているNetScalerイメージのバージョン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の画像は、インスタンスが最初にデプロイされているサイトまたはデータセンターによってグループ化され、次にそのタイプ（VPXおよびMPX）に基づいてさらにグループ化されているサークルパックを示しています。

グループ化された円(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-5.png)

これらすべてのネストされた円は、2つの最も外側の円によって囲まれています。外側の2つの円は、NetScaler Consoleによって監視されるイベントの4つのカテゴリ（システムリソース、クリティカルイベント、SSL構成、構成偏差）と、それに寄与する健全性インジケータを表しています。

### クラスター化されたインスタンスの円

NetScaler Consoleは多くのインスタンスを監視します。これらのインスタンスの監視とメンテナンスを容易にするために、Infrastructure Analyticsでは2つのレベルでインスタンスをクラスター化できます。つまり、インスタンスのグループ化を別のグループ化内にネストできます。

たとえば、BLRデータセンターには、VPXとMPXの2種類のNetScalerインスタンスがデプロイされています。まず、NetScalerインスタンスをタイプ別にグループ化し、次にすべてのインスタンスをグループ化されているサイト別にグループ化できます。これにより、管理しているサイトにデプロイされているインスタンスのタイプ数を簡単に特定できます。

クラスター(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-6.png)

サークルパックの選択(/en-us/netscaler-application-delivery-management-software/media/circle-pack-select.png)

2レベルクラスタリングのその他の例を次に示します。

**サイトとモデル:**

サイト(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-7.png)

**タイプとバージョン:**

モデル(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-8.png)

**サイトとバージョン:**

バージョン(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-9.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Circle Pack の使用方法

各色の円をクリックして、そのインスタンスを強調表示します。

Circle Pack の使用方法(/en-us/netscaler-application-delivery-management-software/media/circle-pack-how-to.png)

そのインスタンスで発生したイベントに応じて、外側の円には、それらの健全性インジケーターのみが強調表示されます。たとえば、以下の2つのCircle Packの画像は、両方のインスタンスがクリティカル状態であるにもかかわらず、異なるリスクインジケーターのセットを表示しています。

健全性インジケーターをクリックして、そのリスクインジケーターを報告したインスタンスの数に関する詳細情報を取得することもできます。たとえば、`Not recommended Algo`をクリックして、そのリスクインジケーターの概要レポートを表示します。

## 表形式ビュー

表形式ビューには、インスタンスとそのインスタンスの詳細が表形式で表示されます。表示される詳細は次のとおりです。

- インスタンスのホスト名
- インスタンスのIPアドレス
- インスタンスの状態
- インスタンススコア
- そのインスタンスで構成されている仮想サーバーの数
- そのインスタンスで構成されているアプリケーションの数
- リスク指標の合計数
- インスタンススコアの低下に大きく寄与しているイベント

クリティカル状態のインスタンスがテーブルの最上部に表示され、次にレビューが必要なインスタンス、そして健全なインスタンスが続きます。

表形式ビューでインスタンスのIPアドレスをクリックすると、そのインスタンスの詳細がダッシュボード表示で確認できます。インスタンスダッシュボードには、インスタンスのCPU、メモリ、ディスク使用量を確認できるインスタンスの概要が表示されます。また、SSL証明書管理、構成監査、ネットワーク機能、およびインスタンスの詳細なネットワーク使用状況を示すネットワーク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レポートに関する詳細も確認できます。さらに下にスクロールすると、このインスタンスで有効になっている機能とモードのリストが表示されます。

各行の先頭にある矢印をクリックして行を展開すると、詳細が表示されます。

展開されたテーブル行には、インスタンスで発生したすべてのカテゴリのエラーが表示されます。上記の例では、システムリソース、SSL構成、および構成ファイルの逸脱にエラーがあったことがわかります。ただし、インスタンスから報告された重大なイベントはありません。

## 概要パネルの使用方法

**概要パネル**は、レビューが必要なインスタンスやクリティカル状態のインスタンスに効率的かつ迅速に焦点を当てるのに役立ちます。このパネルは、概要、インスタンス情報、トラフィックプロファイルの3つのタブに分かれています。このパネルで行った変更は、サークルパック形式と表形式ビューの両方の表示を変更します。以下のセクションでは、これらのタブについて詳しく説明します。以下のセクションの例は、さまざまな選択基準を効率的に使用して、インスタンスによって報告された問題を分析するのに役立ちます。

**概要**:

**概要**タブでは、ハードウェアエラー、使用状況、期限切れの証明書、およびインスタンスで発生する可能性のある同様の指標に基づいてインスタンスを監視できます。ここで監視できる指標は次のとおりです。

- CPU使用率
- メモリ使用量
- ディスク使用量
- システム障害
- 重大なイベント
- SSL証明書の有効期限切れ

次の例は、エラーを報告しているインスタンスを分離するために、**概要**パネルを操作する方法を示しています。

**例1：レビュー状態のインスタンスを表示する：**

**レビュー**チェックボックスを選択すると、重大なエラーを報告していないが、まだ注意が必要なインスタンスのみが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**概要**パネルのヒストグラムは、高いCPU使用率、高いメモリ使用率、および高いディスク使用率のイベントに基づいて集計されたインスタンスの数を表します。ヒストグラムは10%、20%、30%、40%、50%、60%、70%、80%、90%、100%で段階分けされています。棒グラフのいずれかにマウスポインターを合わせます。グラフの下部にある凡例には、使用範囲とその範囲内のインスタンス数が表示されます。棒グラフをクリックして、その範囲内のすべてのインスタンスを表示することもできます。

**例2：割り当てられたメモリの10%から20%を消費しているインスタンスを表示する：**

メモリ使用量セクションで、棒グラフをクリックします。凡例には、選択された範囲が10～20%であり、その範囲で動作しているインスタンスが29個あることが示されます。

これらのヒストグラムで複数の範囲を選択することもできます。

**例3：複数の範囲で高いディスク容量を消費しているインスタンスを表示する：**

0%から10%のディスク容量を消費したインスタンスを表示するには、マウスポインターを2つの範囲にドラッグします。

概要(/en-us/netscaler-application-delivery-management-software/media/overview-infra.png)

**注**

「X」をクリックして選択を解除します。複数の選択を解除するには、**リセット**をクリックすることもできます。

**概要**パネルの横棒グラフは、システムエラー、重大なイベント、およびSSL証明書の有効期限ステータスを報告するインスタンスの数を示します。それらのインスタンスを表示するには、チェックボックスを選択します。

**例 4: 期限切れのSSL証明書のインスタンスを表示する:**

1 - **フィルタ**リストをクリックします。

2 - **SSL証明書の有効期限**セクションで、インスタンスを表示するには、**期限切れ**チェックボックスを選択します。

## インスタンス情報

**インスタンス情報**パネルでは、展開の種類、インスタンスの種類、モデル、およびソフトウェアバージョンに基づいてインスタンスを表示できます。複数のチェックボックスを選択して、選択範囲を絞り込むことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**例 5: 特定のビルド番号を持つNetScaler VPXインスタンスを表示する:**

表示したいバージョンを選択します。



### トラフィックプロファイル

**トラフィックプロファイル**パネルのヒストグラムは、インスタンスのライセンススループット、インスタンスによって処理されるリクエスト数、接続数、トランザクション数に基づいて集計されたインスタンスの数を表します。その範囲のインスタンスを表示するには、棒グラフを選択します。

**例 6: TCP接続をサポートするインスタンスを表示する:**

次の画像は、TCP接続をサポートするインスタンスの数を示しています。



## 設定パネルの使用方法

**設定**パネルでは、インフラストラクチャ分析のデフォルトビューを設定できます。また、CPU使用率、ディスク使用率、メモリ使用率が高い場合の低しきい値と高しきい値を設定することもできます。設定パネルは、との2つのタブに分かれています。

### 表示

- **デフォルトビュー**。分析ページのデフォルトビューとして、**Circle Pack**または表形式を選択します。選択した形式は、NetScaler Consoleでページにアクセスするたびに表示されるものです。
- **Circle Pack - インスタンスサイズ**。インスタンス円のサイズを、仮想サーバーの数またはアクティブな仮想サーバーの数のいずれかに設定できます。
- **Circle Pack - クラスター化の基準**。インスタンス円の2レベルのクラスタリングを決定します。インスタンスのクラスタリングの詳細については、「クラスター化されたインスタンス円」を参照してください。



### スコアしきい値

組織のトラフィック要件に応じて、CPU、メモリ、ディスク使用率が高い場合の低しきい値と高しきい値を変更できます。各選択ヒストグラムのハンドルをドラッグして値を設定します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

**設定の適用**をクリックしてこれらの変更を適用するか、**リセット**をクリックしてすべての変更を削除します。

## ダッシュボードでデータを視覚化する方法

インフラストラクチャ分析を使用すると、ネットワーク管理者は数秒以内に最も注意が必要なインスタンスを特定できるようになりました。データ視覚化をより詳細に理解するために、ExampleCompanyのネットワーク管理者であるChrisのケースを考えてみましょう。

クリスは組織内で多数のNetScalerインスタンスを管理しています。いくつかのインスタンスは大量のトラフィックを処理するため、クリスはそれらを綿密に監視する必要があります。クリスは、いくつかの高トラフィックインスタンスが、以前のように通過するトラフィックを完全に処理していないことに気づきました。この減少を分析するために、以前はクリスがさまざまなソースから送られてくる複数のデータレポートを読み込む必要がありました。クリスは、データを手動で関連付け、どのインスタンスが最適な状態ではなく注意が必要かを特定するために、より多くの時間を費やす必要がありました。

クリスは、Infrastructure Analytics機能を使用して、すべてのインスタンスの健全性を視覚的に確認します。

以下の2つの例は、Infrastructure Analyticsがクリスのメンテナンス作業をどのように支援するかを示しています。

**例1 - SSLトラフィックの監視:**

クリスはCircle Packで、あるインスタンスのインスタンススコアが低く、「Critical」状態にあることに気づきました。クリスはそのインスタンスをクリックして、問題が何かを確認します。インスタンスの概要には、そのインスタンスでSSLカード障害が発生しており、SSLトラフィックを処理できないこと（SSLトラフィックが減少していること）が表示されます。クリスはこの情報を抽出し、すぐに問題を調査するようチームにレポートを送信します。

**例2 - 設定変更の監視:**

クリスはまた、別のインスタンスが「Review」状態であり、最近設定の逸脱があったことにも気づきました。クリスが設定逸脱リスクインジケーターをクリックすると、RC4 Cipher、SSL v3、TLS 1.0、およびTLS 1.1に関連する設定変更が行われていることに気づきました。これはセキュリティ上の懸念が原因である可能性があります。クリスはまた、このインスタンスのSSLトランザ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クショントラフィックプロファイルが低下していることにも気づきました。クリスはこのレポートをエクスポートし、さらに調査を依頼するために管理者に送信します。

## Infrastructure Analytics でインスタンスの詳細を表示

1. 「**インフラストラクチャ > インフラストラクチャ分析**」に移動します。
2. サークルパックビューをクリックし、IPアドレスを選択します。

   テーブルビューからIPアドレスをクリックすることもできます。

- **ホスト名** – NetScalerインスタンスに割り当てられたホスト名を示します。
- **IPアドレス** – NetScalerインスタンスのIPアドレスを示します。
- **スコア** – NetScalerインスタンスのスコアと、Critical、Good、Fairなどのステータスを示します。
- **可用性** – NetScalerインスタンスのステータス（**稼働中**、**停止中**、**サービス停止中**など）を示します。
- **最大寄与** – NetScalerインスタンスが最大のエラー数を記録している問題カテゴリを示します。
- **CPU使用率** – インスタンスによって使用されている現在のCPU使用率（%）を示します。
- **メモリ使用率** – インスタンスによって使用されている現在のメモリ使用率（%）を示します。
- **ディスク使用率** – インスタンスによって使用されている現在のディスク使用率（%）を示します。
- **システム障害** – インスタンスシステムのエラーの総数を示します。
- **重大イベント** – NetScalerインスタンスが最大数のイベントを持つイベントカテゴリを示します
- **SSL有効期限** – NetScalerインスタンスにインストールされているSSL証明書のステータスを示します
- **タイプ** – VPX、SDX、MPX、CPXなどのNetScalerインスタンスタイプを示します
- **展開** – NetScalerインスタンスがスタンドアロンインスタンスとして展開されているか、HAペアとして展開されているかを示します
- **モデル** – NetScalerインスタンスのモデル番号を示します
- **バージョン** – NetScalerインスタンスのバージョンとビルド番号を示します
- **スループット** – NetScalerインスタンスからの現在のネットワークスループットを示します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HTTPSリクエスト/秒** – NetScalerインスタンスが受信した現在のHTTPSリクエスト/秒を示します
- **TCP接続** – 現在確立されているTCP接続を示します
- **SSLトランザクション** – NetScalerインスタンスによって処理された現在のSSLトランザクションを示します
- **サイト** – NetScalerインスタンスが展開されているサイトの名前を示します。

**注**

5分ごとに、CPU使用率、メモリ使用率、ディスク使用率、スループットなどの現在の値が更新されます。

**インスタンスの詳細**をクリックして、詳細を表示します。

以下の詳細が表示されます。

- **情報** - インスタンスタイプ、展開タイプ、バージョン、モデルなどのインスタンスの詳細。
- **機能** – デフォルトでは、ライセンスされていない機能が表示されます。**ライセンスされた機能**をクリックして、ライセンスされている機能を表示します。
- **モード** – デフォルトでは、インスタンスで無効になっているすべてのモードが表示されます。**有効なモードを表示**をクリックして、インスタンスで有効になっているモードを表示します。

インスタンスダッシュボードには、以下の詳細を確認できるインスタンスの概要が表示されます。

- **インスタンススコア**

  **1** – 選択した期間の現在のNetScalerインスタンススコアを示します。最終スコアは**100から合計ペナルティを引いた値**として計算されます。グラフには、選択した期間のスコア範囲が表示されます。

  **2** – **稼働中、停止中、サービス停止中**など、NetScalerインスタンスのステータスを示します。

  **3** – NetScalerインスタンスが稼働している期間を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**4** – インスタンスで有効および無効になっているネットワークインターフェイスの合計数を示します。クリックすると、ネットワークインターフェイス名やステータス（有効または無効）などの詳細が表示されます。

**5** – リストから期間を選択して、インスタンスの詳細を表示します。

**6** – NetScalerインスタンスの合計問題数と問題カテゴリを表示します。

- **主要メトリック**

  各タブをクリックして詳細を表示します。各メトリックでは、選択した時間の平均値と差分値を表示できます。

  次の画像はHTTPS Req/Secの例で、選択された期間は1時間です。値**692**は1ヶ月間のHTTPS Req/Secの平均値であり、値**20**は差分値です。グラフでは、最初の値が**139**で、最後の値が**119**です。差分値は**139 – 119 = 20**です。

  メトリック(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-metrics.png)

  選択した期間のインスタンスメトリックをグラフ形式で表示できます。

  - **CPU使用率** – 選択した期間におけるインスタンスからの平均CPU使用率（パケットCPUと管理CPUの両方に表示されます）。
  - **メモリ使用率** – 選択した期間におけるインスタンスからの平均メモリ使用率。
  - **ディスク使用率** – 選択した期間におけるインスタンスからの平均ディスク容量使用率。
  - **スループット** – 選択した期間においてインスタンスによって処理された平均ネットワークスループット。
  - **HTTPSリクエスト/秒** – 選択した期間においてインスタンスによって受信された平均HTTPSリクエスト数。
  - **TCP接続** – 選択した期間においてクライアントとサーバーによって確立された平均TCP接続数。
  - **SSLトランザクション** – 選択した期間においてインスタンスによって処理された平均SSLトランザクション数。

- **問題**

  NetScalerインスタンスで発生する以下の問題を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 問題カテゴリ | 説明 | 問題 |
| --- | --- | --- |
| システムリソース | CPU、メモリ、ディスク使用量など、NetScalerシステムリソースに関連するすべての問題を表示します。 | - 高いCPU使用率 |
| | | - 高いメモリ使用率 |
| | | - 高いディスク使用率 |
| | | - SSLカード障害 |
| | | - 電源障害 |
| | | - ディスクエラー |
| | | - フラッシュエラー |
| | | - NIC破棄 |
| SSL設定 | NetScalerインスタンス上のSSL設定に関連するすべての問題を表示します。 | - SSL証明書の期限切れ |
| | | - 推奨されない発行者 |
| | | - 推奨されないアルゴリズム |
| | | - 推奨されない鍵強度 |
| 構成の逸脱 | NetScalerインスタンスに適用された構成ジョブに関連するすべての問題を表示します。 | - 構成ドリフト |
| | | - 実行中とテンプレートの比較 |
| 重大なイベント | HAペアおよびクラスターで構成されたNetScalerインスタンスに関連するすべての重大なイベントを表示します。 | - クラスタープロパゲーションの失敗 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 問題カテゴリ | 説明 | 問題 |
| --- | --- | --- |
| | | - クラスター同期の失敗 |
| | | - クラスターバージョンの不一致 |
| | | - HAセカンダリ状態の異常 |
| | | - HAハートビートなし |
| | | - HA同期失敗 |
| | | - HAバージョン不一致 |
| ネットワーク | インスタンスで発生する運用上の問題を表示します。 | 詳細については、「新しいインジケーターによる強化されたインフラストラクチャ分析」を参照してください。 |

各タブをクリックして、問題を分析し、トラブルシューティングします。たとえば、選択した期間にインスタンスで次のエラーが発生したとします。

- **Current**タブには、現在インスタンススコアに影響を与えている問題が表示されます。
- **All**タブには、選択した期間に検出されたすべてのインフラストラクチャの問題が表示されます。

## NetScalerインスタンスのキャパシティ問題を表示する

NetScalerインスタンスが利用可能なキャパシティのほとんどを消費すると、クライアントトラフィックの処理中にパケットドロップが発生する可能性があります。この問題は、NetScalerインスタンスのパフォーマンス低下を引き起こします。このようなNetScalerのキャパシティ問題を理解することで、NetScalerのパフォーマンスを安定させるために、追加のライセンスを積極的に割り当てることができます。

**サークルパックビュー**では、NetScalerインスタンスのキャパシティ問題が存在する場合に表示できます。

NetScalerのキャパシティ問題を表示するには、,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **インフラストラクチャ > インフラストラクチャ分析**に移動します。
2. サークルパックビューを選択します。

> **注**
>
> **インフラストラクチャ分析**では、サークルパックビューと表形式ビューに、過去1時間に発生したイベントと問題が表示されます。

次の図は、選択したインスタンスにキャパシティ問題が存在することを示しています。

キャパシティ問題のサークルパックビューを表示(/en-us/netscaler-application-delivery-management-software/media/adc-capacity-issues.png)

問題は、次のキャパシティパラメータに基づいて分類されます。

- **スループット制限に到達** – スループット制限に到達した後にインスタンスでドロップされたパケットの数。
- **PE CPU制限に到達** – PE CPU制限に到達した後にすべてのNICでドロップされたパケットの数。
- **PPS制限に到達** – PPS制限に到達した後にインスタンスでドロップされたパケットの数。
- **SSLスループットレート制限** – SSLスループット制限に到達した回数。
- **SSL TPSレート制限** – SSL TPS制限に達した回数。

### キャパシティの問題を解決するための推奨アクションを表示

NetScaler Consoleは、キャパシティの問題を解決できるアクションを推奨します。推奨アクションを表示するには、次の手順を実行します。

1. **Infrastructure > Infrastructure Analytics**で、表形式ビューを選択します。
2. キャパシティの問題があるインスタンスを選択し、**Details**をクリックします。

   
3. インスタンスページで、**Issues**セクションまでスクロールします。
4. 各問題を選択し、キャパシティの問題を解決するための推奨アクションを表示します。

   

NetScaler Consoleは、NetScalerインスタンスから5分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンターの増分が存在する場合に表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleは、定義されたキャパシティしきい値に基づいてインスタンススコアを計算します。

- **低しきい値** – 1パケットドロップまたはレート制限カウンターの増分
- **高しきい値** – 10000パケットドロップまたはレート制限カウンターの増分

したがって、NetScalerインスタンスがキャパシティしきい値を超えると、インスタンススコアに影響が出ます。

パケットドロップまたはレート制限カウンターが増加すると、`ADCCapacityBreach`カテゴリの下にイベントが生成されます。これらのイベントを表示するには、**Accounts > System Events**に移動します。

## 新しいインジケーターによる強化されたインフラストラクチャ分析

NetScaler Consoleのインフラストラクチャ分析を使用すると、次のことができます。

- NetScalerインスタンスで発生する新しい一連の運用上の問題を表示します。
- エラーメッセージを表示し、問題をトラブルシューティングするための推奨事項を確認します。

管理者として、問題の根本原因分析を迅速に特定できます。

**注**

ルールインジケーターは、以下ではサポートされていません。

- クラスターモードで構成されたNetScalerインスタンス。
- 管理パーティションで構成されたNetScalerインスタンス。

NetScaler Consoleで、**インフラストラクチャ > インフラストラクチャ分析**に移動して、次のインジケーターを表示します。

| インフラストラクチャ分析のインジケーター名 | 説明 |
| --- | --- |
| **ポート割り当ての失敗** | NetScalerがSNIPを使用して新しいサーバー接続と通信し、そのSNIPで利用可能なポートがすべて使い果たされたときに検出します。推奨されるアクションは、同じサブネットに別のSNIPを追加することです。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インフラストラクチャ分析のインジケーター名 | 説明 |
| --- | --- |
| **デフォルトルート構成なし** | ルートが利用できないためにトラフィックがドロップされたときに検出します。 |
| **IP競合** | ネットワーク内の2つ以上のインスタンスで同じIPアドレスが設定または適用されている場合に検出します。 |
| **VRID競合** | 指定されたVRIDで断続的なアクセス問題が発生したときに検出します。 |
| **VLAN不一致** | IPサブネットにバインドされたVLAN設定中にエラーが発生した場合に検出します。 |
| **TCPスモールウィンドウ攻撃** | 進行中のスモールウィンドウ攻撃の可能性がある場合に検出します。このアラートは情報提供のみを目的としています。NetScalerはすでにこの攻撃を軽減しているためです。 |
| **レート制御しきい値** | 設定されたレート制御しきい値に基づいてパケットがドロップされたときに検出します。 |
| **永続性制限** | NetScalerメモリに最大ヒットが課されたときに検出します。 |
| **GSLBサイト名不一致** | サイト名の不一致によりGSLB構成の同期障害が発生したときに検出します。 |
| **不正なIPヘッダー** | IPv4パケットの健全性チェックが失敗した場合に検出します。 |
| **不正なL4チェックサム** | TCPパケットのチェックサム検証が失敗した場合に検出します。 |
| **IP移動によるCPU使用率の増加** | 多数のMACアドレスを更新する必要がある場合に検出します。 |
| **過剰なパケットステアリング** | 非対称RSSキータイプを使用しているために、ソフトウェアパケットステアリングのレベルが高い場合に検出します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インフラストラクチャ分析のインジケーター名 | 説明 |
| --- | --- |
| **レイヤー2ループ** | ネットワーク内のレイヤー2ループの存在を検出します。 |
| **タグ付きVLANの不一致** | タグ付きVLANパケットがタグなしインターフェイスで受信された場合に検出します。 |

### 表形式ビュー

**Infrastructure Analytics**の表形式ビューオプションを使用して、異常を表示することもできます。**Infrastructure > Infrastructure Analytics**に移動し、

をクリックして、すべての管理対象インスタンスを表示します。

をクリックして詳細を展開します。

### 異常の詳細を表示

例えば、ネットワーク内の**IPアドレスの競合**の詳細を表示したい場合は、IPアドレスの競合として表示されている異常をクリックして詳細を表示します。

- **詳細** - どのような異常が検出されたかを示します
- **検出メッセージ** - IPアドレスが競合しているMACアドレスを示します
- **推奨事項** - このIPアドレスの競合を解決するためのアクション項目を示します

# インスタンス管理

インスタンスとは、NetScaler Console を使用して管理、監視、トラブルシューティングできる Citrix NetScaler アプライアンスです。インスタンスを監視するには、NetScaler Console に追加する必要があります。インスタンスは、NetScaler Console のセットアップ時または後で追加できます。NetScaler Console にインスタンスを追加すると、継続的にポーリングされ、後で問題の解決やレポートデータとして使用できる情報が収集されます。

インスタンスは、静的グループまたはプライベート IP ブロックとしてグループ化できます。インスタンスの静的グループは、構成ジョブなどの特定のタスクを実行する場合に役立ちます。プライベート IP ブロックは、地理的な場所に基づいてインスタンスをグループ化します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## インスタンスを追加する

インスタンスは、NetScaler Console サーバーを初めてセットアップするとき、または後で追加できます。インスタンスを追加するには、各 NetScaler インスタンスのホスト名または IP アドレス、あるいは IP アドレスの範囲を指定する必要があります。

NetScaler Console へのインスタンスの追加方法については、「NetScaler Console へのインスタンスの追加」を参照してください。

NetScaler Console サーバーにインスタンスを追加すると、サーバーは暗黙的に自身をインスタンスのトラップ宛先として追加し、インスタンスのインベントリを収集します。詳細については、「NetScaler Console がインスタンスを検出する方法」を参照してください。

インスタンスを追加した後、**Infrastructure > Instances** に移動し、**All Instances** をクリックして削除できます。Instances ページで、削除するインスタンスを選択し、**Remove** をクリックします。

## インスタンスダッシュボードの使用方法

NetScaler Console のインスタンスごとのダッシュボードには、選択したインスタンスのデータが表形式とグラフ形式で表示されます。ポーリングプロセス中にインスタンスから収集されたデータがダッシュボードに表示されます。

デフォルトでは、管理対象インスタンスはデータ収集のために毎分ポーリングされます。状態、1秒あたりの HTTP リクエスト数、CPU 使用率、メモリ使用率、スループットなどの統計情報は、NITRO コールを使用して継続的に収集されます。管理者として、この収集されたすべてのデータを1つのページで表示し、インスタンスの問題を特定し、それらを修正するための即時アクションを実行できます。

特定のインスタンスのダッシュボードを表示するには、**Infrastructure > Instances** に移動します。概要からインスタンスタイプを選択し、表示したいインスタンスを選択して **Dashboard** をクリックします。

次の図は、インスタンスごとのダッシュボードに表示されるさまざまなデータの概要を示しています。



- **概要**。概要タブには、選択したインスタンスの CPU とメモリの使用率が表示されます。インスタンスによって生成されたイベントとスループットデータも表示できます。IP アドレス、ハードウェアおよび LOM バージョン、プロファイルの詳細、シリアル番号、担当者などのイ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンスタンス固有の情報もここに表示されます。さらに下にスクロールすると、選択したインスタンスで利用可能なライセンス機能と、それに構成されているモードが表示されます。

詳細については、「インスタンスの詳細」を参照してください。

- **SSLダッシュボード**。インスタンスごとのダッシュボードにあるSSLタブを使用して、選択したインスタンスのSSL証明書、SSL仮想サーバー、およびSSLプロトコルの詳細を表示または監視できます。グラフ内の「数値」をクリックすると、さらに詳細が表示されます。
- **構成監査**。構成監査タブを使用して、選択したインスタンスで発生したすべての構成変更を表示できます。ダッシュボードの**NetScaler® config saved status**および**NetScaler config drift**チャートには、保存済み構成と未保存構成における構成変更に関する概要が表示されます。
- **ネットワーク機能**。ネットワーク機能ダッシュボードを使用すると、選択したNetScalerインスタンスで構成されているエンティティの状態を監視できます。仮想サーバーのグラフを表示して、クライアント接続、スループット、サーバー接続などのデータを表示できます。
- **ネットワーク使用状況**。ネットワーク使用状況タブで、選択したインスタンスのネットワークパフォーマンスデータを表示できます。1時間、1日、1週間、または1か月間のレポートを表示できます。タイムラインスライダー機能を使用して、生成されるネットワークレポートの期間をカスタマイズできます。デフォルトでは8つのレポートのみが表示されますが、画面右下隅にある「プラス」アイコンをクリックすると、追加のパフォーマンスレポートを追加できます。

## グローバルに分散されたサイトを監視する

ネットワーク管理者として、地理的に異なる場所に展開されているネットワークインスタンスを監視および管理する必要がある場合があります。しかし、地理的に分散されたデータセンターでネットワークインスタンスを管理する場合、ネットワークの要件を把握するのは容易ではありません。

NetScaler Console のジオマップは、サイトのグラフィカルな表示を提供し、地理別にネットワーク監視エクスペリエンスを分類します。ジオマップを使用すると、場所別にネットワークインスタンスの分布を視覚化し、ネットワークの問題を監視できます。

以下のセクションでは、NetScaler Console でデータセンターを監視する方法について説明します。

NetScaler Console サイトは、特定の地理的場所にある Citrix NetScaler インスタンスの論理的なグループ化です。たとえば、あるサイトが Amazon Web Services (AWS) に割り当てられ、別のサイトが Azure に割り当てられる場合があります。さらに別のサイトは、テナントのオンプレミスでホストされます。NetScaler Console は、すべてのサイトに接続されているすべての NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスを管理および監視します。NetScaler Console を使用して、管理対象インスタンスから発生する syslog、AppFlow、SNMP、およびその他のデータを監視および収集できます。

NetScaler Console のジオマップは、サイトのグラフィカルな表示を提供します。ジオマップは、地理別にネットワーク監視エクスペリエンスを分類します。ジオマップを使用すると、場所別にネットワークインスタンスの分布を視覚化し、すべてのネットワークの問題を監視できます。世界地図上に作成されたサイトの視覚的な表示については、**インフラストラクチャ > インスタンス** ページに移動できます。

### ユースケース

大手携帯電話会社である ExampleCompany は、リソースとアプリケーションのホスティングをプライベートサービスプロバイダーに依存していました。同社はすでに2つのサイトを持っていました。1つは米国のミネアポリスに、もう1つはオーストラリアのアリススプリングスにあります。この画像では、2つのマーカーが既存の2つのサイトを表していることがわかります。



マーカーには、各サイトのアプリケーション数を示す数字も表示されます。これらのマーカーをクリックすると、各サイトに関する詳細情報が表示されます。



詳細を表示するには、タブをクリックします。

- **インスタンス** タブ: このタブで以下を表示します。
  - 各ネットワークインスタンスのIPアドレス
  - インスタンスのタイプ
  - それらで発生した重大なイベントの数
  - NetScalerインスタンスで発生した重要なイベントとすべてのイベント。
- **イベント**タブ: インスタンスで発生した重大なイベントと重要なイベントのリストを表示します。
- **証明書**タブ: このタブで以下を表示します。
  - すべてのインスタンスの証明書のリスト
  - 有効期限ステータス
  - 重要な情報と、使用中の証明書が多い上位10インスタンス。
- **エージェント**タブ: インスタンスがバインドされているエージェントのリストを表示します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ジオマップの構成

ExampleCompanyは、インドのバンガロールに3番目のサイトを作成することを決定しました。同社は、重要度の低い社内ITアプリケーションの一部をバンガロールオフィスにオフロードすることで、クラウドをテストしたいと考えていました。同社はAWSクラウドコンピューティングサービスを使用することにしました。

管理者として、まずサイトを作成し、次にNetScaler ConsoleにNetScalerインスタンスを追加する必要があります。また、インスタンスをサイトに追加し、エージェントを追加し、エージェントをサイトにバインドする必要があります。NetScaler Consoleは、NetScalerインスタンスとエージェントが属するサイトを認識します。

NetScalerインスタンスの追加の詳細については、「インスタンスの追加」を参照してください。

**サイトを作成するには:**

NetScaler Consoleにインスタンスを追加する前にサイトを作成します。場所情報を提供することで、サイトを正確に特定できます。

「**インフラストラクチャ > インスタンス > サイト**」に移動し、「**追加**」をクリックします。

1. 「**サイトの作成**」ページで、次の情報を指定します。
   a. 「**サイトの種類**」:「**データセンター**」を選択します。

「

**注**

」

サイトはプライマリデータセンターまたはブランチとして機能できます。適切に選択してください。

   b. 「**種類**」:リストからクラウドプロバイダーとしてAWSを選択します。

「

**注**

」

「**既存のVPCをサイトとして使用**」チェックボックスを適切にオンにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 「**サイト名**」: サイトの名前を入力します。

d. 「**市区町村**」: 市区町村を入力します。

e. 「**郵便番号**」: 郵便番号を入力します。

f. 「**地域**」: 地域を入力します。

g. 「**国**」: 国を入力します。

h. 「**緯度**」: 場所の緯度を入力します。

i. 「**経度**」: 場所の経度を入力します。

2. 「**作成**」をクリックします。



**インスタンスを追加してサイトを選択するには：**

サイトを作成したら、NetScaler Consoleでインスタンスを追加する必要があります。以前に作成したサイトを選択することも、サイトを作成してインスタンスを関連付けることもできます。

サイトを作成したら、NetScaler Consoleでインスタンスを追加する必要があります。以前に作成したサイトを選択することも、サイトを作成してインスタンスを関連付けることもできます。

1. NetScaler Consoleで、**インフラストラクチャ > インスタンス**に移動します。
2. 作成するインスタンスの種類を選択し、**追加**をクリックします。
3. 「**NetScaler VPXの追加**」ページで、IPアドレスを入力し、リストからプロファイルを選択します。
4. リストからサイトを選択します。**サイト**フィールドの横にある「+」記号をクリックしてサイトを作成するか、編集アイコンをクリックしてデフォルトサイトの詳細を変更できます。
5. 右矢印をクリックし、表示されるリストからエージェントを選択します。



6. エージェントを選択したら、そのエージェントをサイトに関連付ける必要があります。この手順により、エージェントをサイトにバインドできます。エージェントを選択し、**サイトの関連付け**をクリックします。



リストからサイトを選択し、**保存**をクリックします。

**OK**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「**Infrastructure > Instances > Agents**」に移動して、エージェントをサイトにアタッチすることもできます。

**NetScalerエージェントをサイトに関連付けるには：**

1. NetScaler Consoleで、「**Infrastructure > Instances > Agents**」に移動します。
2. エージェントを選択し、「**Attach Site**」をクリックします。

   エージェントをアタッチ(/en-us/netscaler-application-delivery-management-software/media/nmaservice-global-datacenters-8.png)

サイトを関連付けて、**保存**をクリックします。

NetScaler Consoleは、バンガロールサイトに追加されたNetScalerインスタンスと、他の2つのサイトのインスタンスも監視し始めます。

## タグを作成してインスタンスに割り当てる方法

NetScaler Consoleでは、Citrix NetScalerインスタンスにタグを関連付けることができるようになりました。タグとは、インスタンスに割り当てることができるキーワードまたは単一の単語です。タグはインスタンスに関する追加情報を提供します。タグは、インスタンスを説明するのに役立つメタデータと考えることができます。タグを使用すると、特定のキーワードに基づいてインスタンスを分類および検索できます。また、単一のインスタンスに複数のタグを割り当てることもできます。

次のユースケースは、インスタンスのタグ付けが監視を改善するのにどのように役立つかを理解するのに役立ちます。

- **ユースケース1**: 英国内のすべてのインスタンスを識別するためのタグを作成できます。ここでは、キーを「Country」、値を「UK」とするタグを作成できます。このタグは、英国内のすべてのインスタンスを検索および監視するのに役立ちます。
- **ユースケース2**: ステージング環境にあるインスタンスを検索したいとします。ここでは、キーを「Purpose」、値を「Staging_NS」とするタグを作成できます。このタグは、ステージング環境で使用されているすべてのインスタンスを、クライアントリクエストが実行されているインスタンスから分離するのに役立ちます。
- **ユースケース3**: 英国の「スウィンドン」地域にあり、David T.が所有するNetScalerインスタンスのリストを調べたい状況を考えてみましょう。これらのすべての要件に対してタグを作成し、これらの条件を満たすすべてのインスタンスに割り当てることができます。

**NetScaler VPXインスタンスにタグを割り当てるには:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler** に移動します。
2. **NetScaler VPX** タブを選択します。
3. 必要なNetScaler VPXを選択します。
4. **Tags** をクリックします。
5. タグを作成し、**OK** をクリックします。

表示される **Tags** ウィンドウでは、作成したすべてのキーワードに値を割り当てることで、独自の「キーと値」のペアを作成できます。

たとえば、次の画像は、作成されたいくつかのキーワードとその値を示しています。独自のキーワードを追加し、各キーワードに値を入力できます。





「+」をクリックして複数のタグを追加することもできます。複数の意味のあるタグを追加することで、インスタンスを効率的に検索できます。



キーワードに複数の値をコンマで区切って追加できます。

例えば、同僚のGreg T.に管理者ロールを割り当てるとします。彼の名前をコンマで区切って追加できます。複数の名前を追加することで、いずれかの名前または両方の名前で検索するのに役立ちます。NetScaler Consoleは、コンマで区切られた値を2つの異なる値として認識します。



タグに基づいてインスタンスを検索する方法の詳細については、タグとプロパティの値を使用してインスタンスを検索する方法を参照してください。

**注**

後で新しいタグを追加したり、既存のタグを削除したりできます。作成できるタグの数に制限はありません。

## タグとプロパティの値を使用してインスタンスを検索する方法

NetScaler Consoleが多数のNetScalerインスタンスを管理している状況があるかもしれません。管理者として、特定のパラメータに基づいてインスタンスインベントリを検索する柔軟性を求めるかもしれません。NetScaler Consoleは現在、検索フィールドで定義したパラメータに基づいてNetScalerインスタンスのサブセットを検索するための改善された検索機能を提供しています。インスタンスは、タグとプロパティという2つの基準に基づいて検索できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **タグ**。タグは、NetScalerインスタンスに関する追加の説明を追加するために、NetScalerインスタンスに割り当てることができる用語またはキーワードです。NetScalerインスタンスにタグを関連付けることができるようになりました。これらのタグは、NetScalerインスタンスをより適切に識別し、検索するために使用できます。
- **プロパティ**。NetScaler Consoleに追加された各NetScalerインスタンスには、そのインスタンスに関連付けられたいくつかのデフォルトパラメータまたはプロパティがあります。たとえば、各インスタンスには独自のホスト名、IPアドレス、バージョン、ホストID、ハードウェアモデルIDなどがあります。これらのプロパティのいずれかの値を指定してインスタンスを検索できます。

たとえば、バージョン12.0でUP状態にあるNetScalerインスタンスのリストを見つけたい状況を考えてみましょう。ここで、インスタンスのバージョンと状態はデフォルトのプロパティによって定義されます。

インスタンスのバージョン12.0とUP状態に加えて、あなたが所有するインスタンスも検索できます。「Owner」タグを作成し、そのタグに「David T」という値を割り当てることができます。タグの作成と割り当て方法の詳細については、「タグを作成してインスタンスに割り当てる方法」を参照してください。

タグとプロパティを組み合わせて、独自の検索条件を作成できます。

### NetScaler VPXインスタンスを検索するには

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler** > **VPX**タブに移動します。
2. 検索フィールドをクリックします。タグまたはプロパティを使用するか、両方を組み合わせて検索式を作成できます。

   次の例は、検索式を効率的に使用してインスタンスを検索する方法を示しています。

   a. **タグ**オプションを選択し、**所有者**を選択します。「David T.」を選択します。

   NetScaler Consoleは、検索式で正規表現とワイルドカード文字をサポートしています。

   b. 正規表現を使用して検索条件をさらに拡張できます。たとえば、DavidまたはStephenのいずれかが所有するインスタンスを検索したい場合、値を「\|」式で区切って入力できます。

   c. ワイルドカード文字を使用して、1つ以上の文字を置き換えたり表現したりすることもできます。たとえば、`Dav*` と入力すると、David T と Dave P が所有するすべてのインスタンスを検索できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



**注**

正規表現とワイルドカード文字、およびそれらの使用方法の詳細については、検索バーの「情報」アイコンをクリックしてください。

## NetScaler® Console を介した集中型 GeoIP DB アップデート

NetScaler Console を使用すると、管理者は MaxMind から GeoIP DB (地理位置情報データベース) ファイルを NetScaler Console 経由で直接アップロードできます。GeoIP DB ファイルを管理対象の NetScaler インスタンスにすぐにプッシュするか、後で更新をスケジュールすることができます。これらのファイルは、GSLB およびセキュリティポリシーで一般的に使用される、正確な IP から場所へのマッピングに不可欠です。

この機能強化により、更新履歴追跡も可能になり、更新が成功したか失敗したかを確認できます。また、以前にアップロードまたはプッシュされた GeoIP DB バージョンを NetScaler Console から表示、削除、またはダウンロードできます。この機能強化では、NetScaler Console での GeoIP DB ファイルの手動更新、バージョン管理、および自動更新ワークフローも導入され、GSLB サービスに影響を与えることなくシームレスな GeoIP DB 更新が可能になります。

以前は、NetScaler には NetScaler 上で GeoIP DB の更新を管理するための集中型メカニズムがありませんでした。管理者は各デバイスで手動で更新を実行する必要があり、これは時間と手間がかかり、エラーが発生しやすく、本番環境では中断を招く可能性がありました。

この機能強化には、次の利点があります。

- **自動化**: 更新プロセスは自動化されており、計画されたダウンタイムなしで実行されるため、運用上のオーバーヘッドが削減されます。
- **効果的なスケーラビリティ**: 複数の NetScaler インスタンスにわたる更新の管理は効率的で、簡単にスケーリングできます。
- **バージョン管理**: 問題が発生した場合、履歴バージョンを追跡し、古い GeoIP DB ファイルをアップロードして同期できます。

### 制限事項

- **MaxMind に限定された形式変換のサポート**: 自動形式変換は MaxMind ファイルのみでサポートされています。他のベンダーの場合、ファイルはすでにサポートされている形式である必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **削除の制限**: アクティブに使用中のファイルを削除することはできません。削除する前に、アクティブな依存関係がないことを確認してください。

### NetScaler Console を介した集中型 GeoIP DB 更新の構成

前提条件

- GeoIP DB ファイルを使用するために必要な有効な MaxMind ライセンスがあることを確認してください。
- 他のベンダーのファイル形式を使用している場合は、ファイルがサポートされている形式であることを確認してください。

MaxMindまたはその他のベンダーからGeoIP DBファイルをアップロードするには、次の手順を実行します。

1. **Infrastructure > GeoIP DB Sync** に移動し、**Get Started** をクリックします。

   集中型GeoIP DBの開始(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-get-started.png)

2. 次のいずれかのオプションを選択します。

   - **新しいファイルをアップロード**: ローカルシステムからファイルをアップロードできます。
   - **既存のファイルを使用**: NetScaler Consoleにすでに存在するファイルを選択できます。

   **注:**

   - GeoIP DBファイルを初めてアップロードする場合、**既存のファイルを使用**オプションは表示されません。ファイルがすでにアップロードされている場合にのみ、その後のアップロード時に**既存のファイルを使用**オプションが表示されます。
   - MaxMindファイルをアップロードすると、NetScaler Consoleサービスはアップロード中にNetScalerが推奨する形式にファイルを自動的に変換します。他のプロバイダーからファイルをアップロードする場合、CSV形式である必要があり、NetScalerが推奨する次のフィールド順序（IP範囲、国コード、地域、都市）に従う必要があります。

3. ファイルがアップロードされたら、次のいずれかのアクションを実行できます。

   - **Sync Now** をクリックし、次に **Start Sync** をクリックします。すべてのNetScalerインスタンスがすぐに更新されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Create Schedule** をクリックします。NetScalerインスタンスを更新する将来の日付と時刻を選択できます。

集中型GeoIP DB同期オプション(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-sync-options.png)

4. **GeoIP DB Sync** ページで、同期の進行状況とインスタンスごとの同期ステータスを表示します。

集中型GeoIP DB同期の進行状況(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-view-sync-progress.png)

5. 要件に基づいて、次のアクションを実行できます。

- 「**新しいファイルの選択**」：**新しいファイルの選択**をクリックして、ローカルからGeoIP DBファイルをアップロードするか、NetScaler Consoleからアップロード済みのファイルを選択します。
- 「**ファイル情報の表示**」：**ファイル情報の表示**をクリックして、以前にアップロードされたファイルを表示します。問題が発生した場合、履歴バージョンを追跡し、古いGeoIP DBファイルをアップロードして同期できます。
- 「**アクティブなスケジュール**」：**アクティブなスケジュール**をクリックして、まだ実行されていない今後のスケジュールを表示します。
- 「**履歴スケジュール**」：**履歴スケジュール**をクリックして、完了した以前のGeoIP DB同期アクティビティを表示します。

集中型GeoIP DB同期の進行状況(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-other-options.png)

## NetScalerインスタンスの管理パーティションを管理する

Citrix NetScalerインスタンスで管理パーティションを設定し、組織内の異なるグループに同じNetScalerインスタンス上の異なるパーティションを割り当てることができます。ネットワーク管理者は、複数のNetScalerインスタンス上の複数のパーティションを管理するように割り当てることができます。

NetScaler Consoleは、管理者が所有するすべてのパーティションを単一のコンソールからシームレスに管理する方法を提供します。これらのパーティションは、他のパーティション設定を中断することなく管理できます。

複数のユーザーが異なる管理パーティションを管理できるようにするには、グループを作成し、それらのグループにユーザーとパーティションを割り当てる必要があります。各ユーザーは、自分

© 1997–2026 Citrix Systems, Inc. All rights reserved.

が属するグループ内のパーティションのみを表示および管理できます。各管理パーティションは、NetScaler Consoleではインスタンスとして扱われます。NetScalerインスタンスを検出すると、そのNetScalerインスタンスで設定されている管理パーティションがシステムに自動的に追加されます。

各インスタンスに2つのパーティションが設定された2つのNetScaler VPXインスタンスがあるとします。たとえば、NetScalerインスタンス10.102.216.49にはPartition_1、Partition_2、Partition_3があり、NetScalerインスタンス10.102.29.120にはp1とp2があります。これは次の図に示されています。

パーティションを表示するには、**Infrastructure > Instances > NetScaler > VPX** に移動し、**Partitions** をクリックします。

user-p1には、10.102.29.120-p1と10.102.216.49-Partition_1のパーティションを割り当てることができます。また、user-p2には、10.102.29.80-p2、10.102.216.49-Partition_2、および10.102.216.49-Partition_3のパーティションを管理するように割り当てることができます。

次に、user-p1とuser-p2の2人のユーザーを作成し、作成したグループにユーザーを割り当てる必要があります。

まず、適切な権限（例：管理者権限）を持つ2つのグループを作成し、各グループに必要な管理パーティションインスタンスを含める必要があります。たとえば、システムグループpartition1-adminを作成し、NetScaler管理パーティション10.102.29.120-p1と10.102.216.49-Partition_1をこのグループに追加します。また、システムグループpartition2-adminを作成し、NetScaler管理パーティション10.102.29.120-p2、10.102.216.49-Partition_2、および10.102.216.49-Partition_3をこのグループに追加します。

管理パーティションを作成した後、監査目的でリビジョン履歴差分機能と管理パーティションの監査テンプレート機能も使用できます。

管理パーティションの**リビジョン履歴差分**を使用すると、パーティション化されたNetScalerインスタンスの最新5つの構成ファイル間の差分を表示できます。構成ファイルを相互に比較したり（例：構成リビジョン-1と構成リビジョン-2）、現在の実行中/保存済み構成と構成リビジョンを比較したりできます。構成の差分に加えて、修正構成も表示されます。すべての修正コマンドをローカルフォルダーにエクスポートして、構成を修正できます。

**リビジョン履歴差分を表示するには：**

1. **Infrastructure > Configuration Audit** に移動します。インスタンス構成ステータスを表すドーナツチャート内をクリックします。開いた**Audit Reports**ページで、パーティション化されたNetScalerインスタンスをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(/en-us/netscaler-application-delivery-management-software/media/admin-partition.png)

2. **Action** メニューから、**Revision History Diff** をクリックします。

   「リビジョン履歴の差分を表示」(/en-us/netscaler-application-delivery-management-software/media/admin-partition-1.png)

3. **リビジョン履歴の差分**ページで、比較するファイルを選択します。たとえば、保存された構成と構成リビジョン-1を比較し、**構成の差分を表示**をクリックします。

   「構成の差分を表示」(/en-us/netscaler-application-delivery-management-software/media/admin-partition-3.png)

4. 選択したパーティション化されたNetScalerインスタンスの最新5つの構成ファイル間の差分を以下に示すように表示できます。修正構成コマンドを表示し、これらの修正コマンドをローカルフォルダーにエクスポートすることもできます。これらの修正コマンドは、構成を目的の状態（比較に使用されている構成ファイル）にするためにベースファイルで実行する必要があるコマンドです。

   「構成差分レポート」(/en-us/netscaler-application-delivery-management-software/media/admin-partition-4.png)

**パーティションの監査テンプレート**を使用すると、カスタム構成テンプレートを作成し、それをパーティションインスタンスに関連付けることができます。インスタンスの実行中の構成と監査テンプレートとの間の差異は、**監査レポート**ページの**テンプレートと実行中の差分**列に表示されます。構成の差分とともに、修正構成も表示されます。すべての修正コマンドをローカルフォルダーにエクスポートして、構成を修正することもできます。

**テンプレートと実行中の差分を表示するには：**

1. **監査レポート**ページから、パーティション化されたNetScalerインスタンスをクリックします。

   「テンプレートと実行中の差分を表示」(/en-us/netscaler-application-delivery-management-software/media/admin-partition-dup.png)

2. 監査テンプレートと実行中の差分との間に差異がある場合、その差異はハイパーリンクとして表示されます。差異がある場合は、ハイパーリンクをクリックして表示します。構成の差分とともに、修正構成も表示されます。すべての修正コマンドをローカルフォルダーにエクスポートして、構成を修正することもできます。

**グループを作成するには：**

1. **設定 > ユーザー管理 > グループ**に移動し、**追加**をクリックします。
2. **システムユーザーの作成**ページで、以下を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **グループ設定**タブ：グループ名とロール権限を入力します。特定のインスタンスへのアクセスを許可するには、**すべてのインスタンス**チェックボックスをオフにし、**インスタンスの選択**ページでインスタンスを選択します。
- **アプリケーションとテンプレート**タブ：このグループをすべてのアプリケーションと構成テンプレートで使用することを選択できます。
- **ユーザーの選択**タブ: このグループに追加するユーザーを選択します。「**利用可能**」テーブルの「**新規**」リンクをクリックして、新しいユーザーを作成できます。オプションで、セッションタイムアウトを設定できます。ここでは、ユーザーがアクティブな状態を維持できる期間を設定できます。

3. 「**完了**」をクリックします。



**ユーザーを作成するには:**

1. **設定 > ユーザー管理 > ユーザー** に移動し、「**追加**」をクリックします。
2. 「**システムユーザーの作成**」ページで、ユーザー名とパスワードを指定します。オプションで、外部認証を有効にし、セッションタイムアウトを設定できます。
3. 「**利用可能**」リストから「**構成済み**」リストにグループ名を追加して、ユーザーをグループに割り当てます。
4. 「**作成**」をクリックします。

ログアウトし、user-p1の資格情報でログインします。管理および監視のために割り当てられた管理者パーティションのみを表示および管理できます。

## NetScaler高可用性ペアを作成する

NetScaler高可用性（HA）ペアは、ダウンタイムやネットワーク障害発生時でも中断のない運用を提供できます。NetScaler Consoleを使用して、NetScalerインスタンスのHAペアを作成できます。詳細については、「NetScaler高可用性」を参照してください。

NetScaler ConsoleでNetScalerインスタンスのHAペアを作成するには、次の手順を実行します。

1. **Infrastructure > Instances > NetScaler**の順に移動します。
2. HAペアを作成するNetScalerインスタンスをリストから選択します。

   選択したインスタンスは、HAペアのプライマリインスタンスになります。
3. **Action > Create HA Pair**をクリックします。
4. **Instance Selection**で、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Secondary IP Address**で、セカンダリインスタンスを選択するためにクリックします。
b. HAペアでセカンダリとして構成するNetScalerインスタンスを選択します。
c. オプション：HAペアインスタンスが2つのサブネットにある場合は、**INC（Independent Network Configuration）モードをオンにする**を選択します。
d. **Next**をクリックします。

(/en-us/netscaler-application-delivery-management-software/media/create-ha-pair-select-instance.png)

5. **Execute**で、HAペアを今すぐ作成するか、後で作成するかを決定できます。
   a. **Execution Mode**で、次のいずれかの実行モードを選択します。
      - **今すぐ** - HAペアを今すぐ作成するには、このオプションを選択します。
      - **後で** - 特定の日時にHAペアを作成するには、このオプションを選択します。
   b. **実行モード**リストで**後で**を選択した場合は、このタスクを実行する**実行日**と**開始時刻**を選択します。

      **注**

      実行時刻は、NetScaler Consoleで設定されているタイムゾーンで表示されます。

   NetScaler HAペアのタスクまたはジョブを実行する(/en-us/netscaler-application-delivery-management-software/media/create-ha-pair-execute.png)

このタスクの実行レポートは、次の方法で受け取ることができます。

- **メール** - リストからメール配信を選択します。

  配信リストを追加するには、**追加**をクリックします。配信リストを追加するために必要なパラメータを指定し、**作成**をクリックします。

  メール配信リスト(/en-us/netscaler-application-delivery-management-software/media/config-jobs-maintenance-6.png)

- **Slack** - リストからSlackプロファイルを選択します。

  Slackプロファイルを追加するには、**追加**をクリックします。**プロファイル名**、**チャネル名**、**トークン**を指定し、**作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Slackプロファイル(/en-us/netscaler-application-delivery-management-software/media/upgrade-slack.png)

## NetScalerインスタンスのバックアップと復元

NetScalerインスタンスの現在の状態をバックアップし、後でバックアップファイルを使用して同じ状態に復元できます。インスタンスをアップグレードする前や、予防措置として常にバックアップしてください。安定したシステムのバックアップがあれば、不安定になった場合に安定した時点に復元できます。

NetScalerインスタンスでバックアップと復元を実行する方法は複数あります。GUIとCLIを使用して、NetScalerの設定を手動でバックアップおよび復元できます。NetScaler Consoleを使用して、自動バックアップと手動復元を実行することもできます。

NetScaler Consoleは、NITROコール、Secure Shell (SSH)、およびSecure Copy (SCP) プロトコルを使用して、管理対象のNetScalerインスタンスの現在の状態をバックアップします。

NetScaler Consoleは、以下のNetScalerインスタンスタイプの完全なバックアップを作成し、復元します。

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

**注:**

- NetScaler Consoleプロファイルに、NetScalerインスタンスをバックアップおよび復元するための管理者アクセス権があることを確認してください。
- NetScaler Consoleから、NetScalerクラスターのバックアップおよび復元操作を実行することはできません。
- あるインスタンスから取得したバックアップファイルを使用して、別のインスタンスを復元することはできません。

バックアップファイルは、以下のディレクトリに圧縮されたTARファイルとして保存されます。

```
/var/mps/tenants/root/device_backup/
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ディスク容量不足による問題を回避するため、このディレクトリにはNetScalerインスタンスごとに最大50個のバックアップファイルを保存できます。

NetScalerインスタンスをバックアップおよび復元するには、まずNetScaler Consoleでバックアップ設定を構成する必要があります。設定を構成した後、単一のNetScalerインスタンスまたは複数のインスタンスを選択し、これらのインスタンス内の構成ファイルのバックアップを作成できます。必要に応じて、これらのバックアップファイルを使用してNetScalerインスタンスを復元することもできます。

### インスタンスのバックアップ設定を構成する

**インスタンスバックアップ設定**ページでは、NetScaler Consoleで選択したNetScalerインスタンスまたは複数のインスタンスをバックアップするための設定を構成できます。

1. NetScaler Consoleで、**設定** > **管理**に移動します。
2. **バックアップ**で、**システムとインスタンスのバックアップを構成**を選択します。
3. **インスタンス**を選択し、以下を指定します。

   - **インスタンスバックアップを有効にする**: デフォルトでは、NetScaler ConsoleはNetScalerインスタンスのバックアップを取得するように有効になっています。インスタンスのバックアップファイルを作成しない場合は、このオプションをオフにします。
   - **ファイルをパスワードで保護**: (オプション) バックアップファイルを暗号化するには、パスワード保護オプションを選択します。バックアップファイルを暗号化することで、バックアップファイル内のすべての機密情報が安全に保たれます。

     **注:**

     暗号化されたバックアップファイルはローカルマシンにダウンロードできますが、NetScaler Console GUIまたは任意のテキストエディタでファイルを開くことはできません。暗号化されたバックアップファイルを復元する際には、パスワードの入力を求められます。ただし、暗号化されていないバックアップファイルはシステムで開くことができます。

   - **保持するバックアップファイルの数**: NetScaler Consoleで保持するバックアップファイルの数を指定します。NetScalerインスタンスごとに最大50個のバックアップファイルを保持できます。デフォルトは3つのバックアップファイルです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

各バックアップファイルは、ある程度のストレージ要件を占めます。要件に応じて、最適な数のNetScalerバックアップファイルをNetScaler Consoleに保存することをお勧めします。

インスタンスのバックアップを指定する(/en-us/netscaler-application-delivery-management-software/media/configure-instance-backup-settings.png)

- **バックアップスケジューリング設定**: (オプション) バックアップファイルを作成するためのオプションは2つありますが、一度に1つのオプションしか使用できません。

  a. デフォルトのバックアップスケジュールオプションは「間隔ベース」です。指定された間隔が経過すると、NetScaler Consoleにバックアップファイルが作成されます。デフォルトのバックアップ間隔は12時間です。

  b. スケジュールされたバックアップの種類を「時間ベース」に変更することもできます。このオプションでは、指定された時間にインスタンスをバックアップするために、`hours:minutes`形式で時間を指定します。NetScaler Consoleでは、インスタンスに対して1日あたり最大4回のバックアップが可能です。

  インスタンスバックアップのスケジュール(/en-us/netscaler-application-delivery-management-software/media/configuring-instance-backup-settings-2.jpg)

- **NetScaler設定**: (オプション) デフォルトでは、NetScaler Consoleは「NetScalerConfigSave」トラップを受信してもバックアップファイルを作成しません。しかし、NetScalerインスタンスがNetScaler Consoleに「NetScalerConfigSave」トラップを送信するたびにバックアップファイルを作成するオプションを有効にできます。NetScalerインスタンスは、インスタンスの構成が保存されるたびに「NetScalerConfigSave」を送信します。
- **Geoデータベースファイル**: (オプション) デフォルトでは、NetScaler ConsoleはGeoデータベースファイルをバックアップしません。これらのファイルのバックアップを作成するオプションも有効にできます。

  NetScaler設定の指定(/en-us/netscaler-application-delivery-management-software/media/configure-netscaler-settings.jpg)

- **外部転送:** (オプション) NetScaler Consoleでは、NetScalerインスタンスのバックアップファイルを外部の場所に転送できます。

  a. 場所のIPアドレスを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. バックアップファイルを転送したい外部サーバーのユーザー名とパスワードを指定します。

c. 転送プロトコルとポート番号を指定します。

d. ファイルを保存する必要があるディレクトリパスを指定できます。

e. オプションで、外部サーバーに転送した後、NetScaler Consoleからバックアップファイルを削除することもできます。

外部転送の詳細を指定(/en-us/netscaler-application-delivery-management-software/media/configuring-instance-backup-settings-4.jpg)

**注:**

NetScaler Consoleは、選択されたNetScalerインスタンスのいずれかでバックアップに失敗した場合、SNMPトラップまたはSyslog通知を自身に送信します。

**NetScaler Consoleを使用して、選択したNetScalerインスタンスのバックアップを作成する**

選択したNetScalerインスタンスまたは複数のインスタンスをバックアップする場合は、このタスクを実行します。

1. NetScaler Consoleで、**Infrastructure > Instances**に移動します。**Instances**の下で、画面に表示するインスタンスのタイプ（例：NetScaler VPX）を選択します。
2. バックアップするインスタンスを選択します。
   - MPX、VPX、およびBLXインスタンスの場合は、**Select Action**リストから**Backup/Restore**を選択します。
   - SDXインスタンスの場合は、**Backup/Restore**をクリックします。
3. **Backup Files**ページで、**Back Up**をクリックします。
4. セキュリティを強化するために、バックアップファイルを暗号化するかどうかを指定できます。パスワードを入力するか、Instance Backup Settingsページで以前に指定したグローバルパスワードを使用できます。
5. **Continue**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Consoleを使用してNetScalerインスタンスを復元する

**注:**

HAペアにNetScalerインスタンスがある場合は、次の点に注意する必要があります。

- バックアップファイルが作成されたのと同じインスタンスを復元します。たとえば、HAペアのプライマリインスタンスからバックアップが取得されたシナリオを考えてみましょう。復元プロセス中に、それがプライマリインスタンスでなくなったとしても、同じインスタンスを復元していることを確認してください。
- プライマリNetScalerインスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできなくなり、セカンダリインスタンスは**STAYSECONDARY**に変更されます。プライマリインスタンスでの復元プロセスが完了すると、セカンダリNetScalerインスタンスは**STAYSECONDARY**から**ENABLED**モードに変わり、再びHAペアの一部になります。復元プロセスが完了するまで、プライマリインスタンスでダウンタイムが発生する可能性があります。

以前に作成したバックアップファイルを使用してNetScalerインスタンスを復元するには、このタスクを実行します。

1. **インフラストラクチャ > インスタンス**に移動し、復元するインスタンスを選択して、**アクションの選択 > バックアップ/復元**をクリックします。

   バックアップファイルを表示(/en-us/netscaler-application-delivery-management-software/media/configure-instance-backup-restore.jpg)
2. **バックアップファイル**ページで、復元する設定を含むバックアップファイルを選択し、**復元**をクリックします。

   バックアップファイルを復元(/en-us/netscaler-application-delivery-management-software/media/restore-backup-instance.jpg)

### NetScaler Consoleを使用してNetScaler SDXアプライアンスを復元する

NetScaler Consoleでは、NetScaler SDXアプライアンスのバックアップには、以下が含まれます。

- アプライアンスでホストされているNetScalerインスタンス
- SVM SSL証明書とキー
- インスタンスのプルーニング設定 (XML形式)
- インスタンスのバックアップ設定 (XML形式)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSL証明書のポーリング設定 (XML形式)
- SVM dbファイル
- SDXに存在するデバイスのNetScaler構成ファイル
- NetScalerビルドイメージ
- NetScaler XVAイメージ。これらのイメージは、次の場所に保存されます。 `/var/mps/sdx_images/`
- SDXシングルバンドルイメージ（SVM+XS）
- サードパーティインスタンスイメージ（プロビジョニングされている場合）

NetScaler SDXアプライアンスをバックアップファイルで利用可能な構成に復元します。アプライアンスの復元中、現在の構成全体が削除されます。

別のNetScaler SDXアプライアンスのバックアップを使用してNetScaler SDXアプライアンスを復元する場合は、復元プロセスを開始する前に、ライセンスを追加し、新しいアプライアンスの管理サービスネットワーク設定をバックアップファイルの設定と一致するように構成してください。つまり、新しいアプライアンスはライセンスを取得し、バックアップファイルの最小ライセンス要件を満たしている必要があります。たとえば、バックアップに合計5 GBの5つのVPXインスタンスが含まれていた場合、新しいアプライアンスもこれらの要件をサポートできる必要があります。または、バックアップアプライアンスがプラチナライセンスを持っていた場合、新しいアプライアンスは同じかそれ以上のライセンスを持っている必要があります。IPアドレス、ネットマスク、ゲートウェイ、XenServer IPアドレス、DNSサーバーなどのネットワーク設定は、新しいアプライアンスで適切に構成されている必要があります。

SDXアプライアンスを復元する前に、バックアップされたSDXアプライアンスのプラットフォームバリアントがアプライアンスと同じであることを確認してください。異なるプラットフォームバリアントから復元することはできません。

**注：**

SDX RMAアプライアンスを復元する前に、バックアップされたバージョンがRMAバージョンと同じかそれ以上であることを確認してください。

バックアップファイルからSDXアプライアンスを復元するには：

1. NetScaler Console GUIで、**Infrastructure > Instances > NetScaler > SDX** に移動します。インスタンスを選択します。
2. **Backup/Restore** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 復元したい同じインスタンスのバックアップファイルを選択します。
4. **Repackage Backup** をクリックします。

   SDXアプライアンスがバックアップされると、XVAファイルとイメージはネットワーク帯域幅とディスクスペースを節約するために個別に保存されます。そのため、SDXアプライアンスを復元する前に、バックアップファイルを再パッケージ化する必要があります。

   バックアップファイルを再パッケージ化すると、SDXアプライアンスを復元するためにすべてのバックアップファイルがまとめられます。再パッケージ化されたバックアップファイルは、SDXアプライアンスの復元を確実に成功させます。
5. 再パッケージ化されたバックアップファイルを選択し、**Restore** をクリックします。

## セカンダリNetScalerインスタンスへのフェールオーバーを強制する

たとえば、プライマリCitrix NetScalerインスタンスを交換またはアップグレードする必要がある場合、フェールオーバーを強制したいことがあります。プライマリインスタンスまたはセカンダリインスタンスのいずれかからフェールオーバーを強制できます。プライマリインスタンスでフェールオーバーを強制すると、プライマリがセカンダリになり、セカンダリがプライマリになります。強制フェールオーバーは、プライマリインスタンスがセカンダリインスタンスがUPであることを判断できる場合にのみ可能です。

強制フェールオーバーは伝播または同期されません。強制フェールオーバー後の同期ステータスを表示するには、インスタンスのステータスを確認できます。

強制フェールオーバーは、次のいずれかの状況で失敗します。

- スタンドアロンシステムでフェールオーバーを強制する。
- セカンダリインスタンスが無効または非アクティブである。セカンダリインスタンスが非アクティブ状態の場合、フェールオーバーを強制するには、その状態がUPになるまで待つ必要があります。
- セカンダリインスタンスがセカンダリのままになるように構成されている。

強制フェールオーバーコマンドを実行したときに潜在的な問題が検出された場合、NetScalerインスタンスは警告メッセージを表示します。このメッセージには、警告をトリガーした情報が含まれており、続行する前に確認を求められます。

プライマリインスタンスまたはセカンダリインスタンスでフェールオーバーを強制できます。

**NetScaler Consoleを使用してセカンダリNetScalerインスタンスへのフェールオーバーを強制するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler > VPX**タブに移動し、インスタンスを選択します。
2. 選択したインスタンスタイプの下にリストされているインスタンスから、HAセットアップのインスタンスを選択します。
3. **Action**メニューから、**Force Failover**を選択します。
4. **Yes**をクリックして、強制フェールオーバーアクションを確認します。

   強制フェールオーバーの作成(/en-us/netscaler-application-delivery-management-software/media/force-failover-1.png)

## セカンダリNetScalerインスタンスをセカンダリのままにするように強制する

HAセットアップでは、プライマリノードの状態に関係なく、セカンダリノードをセカンダリのままにするように強制できます。

たとえば、プライマリノードをアップグレードする必要があり、そのプロセスに数秒かかるとします。アップグレード中にプライマリノードが数秒間ダウンする可能性がありますが、セカンダリノードに引き継がせたくありません。プライマリノードで障害が検出された場合でも、セカンダリノードのままであってほしいとします。

セカンダリノードをセカンダリのままにするように強制すると、プライマリノードがダウンしてもセカンダリのままになります。また、HAペアのノードのステータスをセカンダリのままにするように強制すると、HAステートマシンの遷移には参加しません。ノードのステータスはSTAYSECONDARYと表示されます。

**注**

システムをセカンダリのままにするように強制しても、その強制プロセスは伝播または同期されません。コマンドを実行したノードのみに影響します。

**NetScaler Consoleを使用してセカンダリNetScalerインスタンスをセカンダリのままにするように構成するには：**

1. NetScaler Consoleで、**Infrastructure > Instances** > **NetScaler** > **VPX**タブに移動し、インスタンスを選択します。
2. 選択したインスタンスタイプの下にリストされているインスタンスから、HAセットアップのインスタンスを選択します。
3. **Action**メニューから、**Stay Secondary**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **Yes**をクリックして、「Stay Secondary」アクションの実行を確認します。

   セカンダリのままにするを作成(/en-us/netscaler-application-delivery-management-software/media/stay-secondary-1.png)

## インスタンスグループを作成する

インスタンスグループを作成するには、まずすべてのNetScalerインスタンスをNetScaler Consoleに追加する必要があります。インスタンスを正常に追加した後、インスタンスファミリーに基づいてインスタンスグループを作成します。インスタンスのグループを作成すると、グループ化されたインスタンスに対して一度にアップグレード、バックアップ、または復元を行うことができます。

**インスタンスビュー**では、管理対象のすべてのインスタンスとそれに関連付けられたグループを表示できるため、マップされていないインスタンスを簡単に識別できます。マップされていないインスタンスをグループに割り当てることができます。

### NetScaler Consoleを使用してインスタンスグループを作成するには

1. NetScaler Consoleで、**Infrastructure > Instances > Instance Groups**に移動し、**Add**をクリックします。
2. インスタンスグループの名前を指定し、**Instance Family**リストから**NetScaler**を選択します。
3. **Category**で、**Default**オプションを選択します。
4. **Select Instances**をクリックします。**Select Instances**ページで、グループ化するインスタンスを選択し、**Select**をクリックします。

   テーブルには、選択されたインスタンスとその詳細が表示されます。グループからインスタンスを削除したい場合は、テーブルからインスタンスを選択し、**Delete**をクリックします。
5. **Create**をクリックします。

インスタンスグループを作成する(/en-us/netscaler-application-delivery-management-software/media/024_instancegroups.png)

### マップされていないインスタンスを識別してグループに追加するには

1. **インフラストラクチャ > インスタンス > インスタンスグループ > インスタンスビュー** に移動します。
2. 1つ以上のマップされていないインスタンスを選択します。
3. **Add Instance Group**をクリックします。
4. リストから必要な**インスタンスグループ**を選択します。インターフェースには以下も表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 利用可能なインスタンスグループ。
- 各グループにすでにマッピングされているインスタンス。これにより、重複または誤った割り当てを防ぐことができます。

5. **保存**をクリックします。選択したインスタンスは、選択したグループに割り当てられます。

## NetScaler Console を使用して SDX に NetScaler VPX インスタンスをプロビジョニングする

NetScaler Console を使用して、SDX アプライアンスに1つ以上の NetScaler VPX インスタンスをプロビジョニングできます。デプロイできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と等しい場合、NetScaler Console はそれ以上の NetScaler インスタンスのプロビジョニングを制限します。

開始する前に、VPX インスタンスをプロビジョニングする NetScaler Console に SDX インスタンスを追加してください。

VPX インスタンスをプロビジョニングするには、次の手順を実行します。

1. **Infrastructure > Instances > NetScaler** に移動します。
2. **SDX** タブで、VPX インスタンスをプロビジョニングする SDX インスタンスを選択します。
3. **Select Action** で、**Provision VPX** を選択します。

### ステップ 1 - VPX インスタンスを追加する

NetScaler Console は、SDX アプライアンスで VPX インスタンスを構成するために、次の情報を使用します。

- **名前** - NetScaler インスタンスに名前を指定します。
- SDX と VPX 間の通信ネットワークを確立します。そのためには、リストから必要なオプションを選択します。
  - **内部ネットワーク経由で管理** - このオプションは、NetScaler Console と VPX インスタンス間の通信のために内部ネットワークを確立します。
  - **IP アドレス** - NetScaler VPX インスタンスを管理するために、**IPv4** または **IPv6** アドレス、あるいはその両方を選択できます。VPX インスタンスは、管理 IP (NetScaler IP とも呼ばれます) を1つしか持つことができません。NetScaler IP アドレスを削除することはできません。

    選択したオプションに対して、IP アドレスのネットマスク、デフォルトゲートウェイ、およびネクストホップを NetScaler Console サーバーに割り当てます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **XVA ファイル** - VPX インスタンスをプロビジョニングする XVA ファイルを選択します。次のいずれかのオプションを使用して XVA ファイルを選択します。
  - **ローカル** - ローカルマシンからXVAファイルを選択します。
  - **アプライアンス** - コンソールファイルブラウザからXVAファイルを選択します。
- **管理者プロファイル** - このプロファイルは、VPXインスタンスをプロビジョニングするためのアクセスを提供します。このプロファイルを使用すると、NetScaler Consoleはインスタンスから構成データを取得します。プロファイルを追加する必要がある場合は、**追加**をクリックします。
- **エージェント** - インスタンスを関連付けるエージェントを選択します。
- **サイト** - インスタンスを追加するサイトを選択します。

VPXインスタンスを追加する(/en-us/netscaler-application-delivery-management-software/media/add-vpx-instance-on-sdx.png)

### ステップ2 - ライセンスの割り当て

**ライセンス割り当て**セクションで、VPXライセンスを指定します。Standard、Advanced、Premiumライセンスを使用できます。

- **割り当てモード** - 帯域幅プールには、**固定**モードまたは**バースト可能**モードを選択できます。

  **バースト可能**モードを選択した場合、固定帯域幅に達したときに余分な帯域幅を使用できます。
- **スループット** - インスタンスに合計スループット（Mbps単位）を割り当てます。

**注**

SDXアプライアンス上のCitrix Secure Web Gateway™ (SWG) インスタンスには、別途ライセンス（Secure Web Gateway用SDX 2インスタンスアドオンパック）を購入してください。このインスタンスパックは、SDXプラットフォームライセンスまたはSDXインスタンスパックとは異なります。

ライセンスを割り当てる(/en-us/netscaler-application-delivery-management-software/media/license-allocation.png)

SDX 12.0 57.19バージョン以降、暗号容量を管理するインターフェイスが変更されました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ステップ 3 - リソースの割り当て

「**リソース割り当て**」セクションで、トラフィックを維持するためにVPXインスタンスにリソースを割り当てます。

- 「**合計メモリ (MB)**」 - インスタンスに合計メモリを割り当てます。最小値は `2048` MBです。
- 「**1秒あたりのパケット数**」 - 1秒あたりに送信するパケット数を指定します。
- 「**CPU**」 - インスタンスに割り当てるCPUコアの数を指定します。共有CPUコアまたは専用CPUコアを使用できます。

  インスタンスに共有コアを選択すると、リソース不足時に他のインスタンスがその共有コアを使用できます。

  パフォーマンスの低下を避けるために、CPUコアが再割り当てされたインスタンスを再起動してください。

  SDX 25000xxプラットフォームを使用している場合、インスタンスに最大16コアを割り当てることができます。また、SDX 2500xxxプラットフォームを使用している場合、インスタンスに最大11コアを割り当てることができます。

  「

  **注**

  」

  インスタンスの場合、設定できる最大スループットは180 Gbpsです。

次の表に、サポートされているVPX、シングルバンドルイメージバージョン、およびインスタンスに割り当てることができるコアの数を示します。

| プラットフォーム名 | 合計コア数 | VPXプロビジョニングに利用可能な合計コア数 | 単一インスタンスに割り当て可能な最大コア数 |
|---|---|---|---|
| SDX 8015、SDX 8400、および SDX 8600 | 4 | 3 | 3 |
| SDX 8900 | 8 | 7 | 7 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| プラットフォーム名 | 合計コア数 | VPXプロビジョニングに利用可能な合計コア数 | 単一インスタンスに割り当て可能な最大コア数 |
|---|---|---|---|
| SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、および SDX 20500 | 12 | 10 | 5 |
| SDX 11515、SDX 11520、SDX 11530、SDX 11540、および SDX 11542 | 12 | 10 | 5 |
| SDX 17500、SDX 19500、およびSDX 21500 | 12 | 10 | 5 |
| SDX 17550、SDX 19550、SDX 20550、およびSDX 21550 | 12 | 10 | 5 |
| SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080、およびSDX 14100 | 12 | 10 | 5 |
| SDX 22040、SDX 22060、SDX 22080、SDX 22100、およびSDX 22120 | 16 | 14 | 7 |
| SDX 24100 および SDX 24150 | 16 | 14 | 7 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| プラットフォーム名 | 合計コア数 | VPXプロビジョニングに利用可能な合計コア数 | 単一インスタンスに割り当て可能な最大コア数 |
|---|---|---|---|
| SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14080 40G および SDX 14100 40G | 12 | 10 | 10 |
| SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS および SDX 14100. FIPS | 12 | 10 | 5 |
| SDX 14040 40S、SDX 14060 40S、SDX 14080 40S、およびSDX 14100 40S | 12 | 10 | 5 |
| SDX 25100A、25160A、25200A | 20 | 18 | 9 |
| SDX 25100-40G、25160-40G、25200-40G | 20 | 18 | 16 (バージョンが11.1-51.x以降の場合); 9 (バージョンが11.1-50.x以前の場合、または11.0および10.5のすべてのバージョン) |
| SDX 26100、26160、26200、26250 | 28 | 26 | 13 |
| 15000-50G | 16 | 14 | 7 |
| SDX 16000 | 32 | 30 | 16 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| プラットフォーム名 | 合計コア数 | VPXプロビジョニングに利用可能な合計コア数 | 単一インスタンスに割り当て可能な最大コア数 |
|---|---|---|---|
| SDX 9100 | 10 | 9 | 9 |

**注**

SDX 26xxxプラットフォームでは、VPXインスタンスに割り当てられるCPUコアの最大数は26です。インスタンスに暗号ユニットが割り当てられている場合、コアの最大数は、暗号ユニットとデータインターフェイスの数によって異なります。

例えば、インスタンスに24000の暗号ユニットを割り当てた場合、24個のCPUコアと最大2つのデータインターフェースをそのインスタンスに割り当てることができます。SDXアプライアンスは、データインターフェースと暗号ユニットをPCIデバイスと見なします。26000の暗号ユニットの場合、データインターフェースを追加するスペースがないため、VPXインスタンスのプロビジョニングは失敗します。

### ステップ4 - インスタンス管理の追加

VPXインスタンスの管理者ユーザーを作成できます。これを行うには、**インスタンス管理**セクションで**インスタンス管理の追加**を選択します。

以下の詳細を指定します。

- **ユーザー名**: NetScalerインスタンス管理者のユーザー名。このユーザーはスーパーユーザーアクセス権を持っていますが、VLANやインターフェースを設定するためのネットワークコマンドへのアクセス権はありません。
- **パスワード**: ユーザー名のパスワードを指定します。
- **シェル/Sftp/Scpアクセス**: NetScalerインスタンス管理者に許可されるアクセス。このオプションはデフォルトで選択されています。

インスタンス管理の追加(/en-us/netscaler-application-delivery-management-software/media/instance-administration.png)

### ステップ5 - ネットワーク設定の指定

インスタンスに必要なネットワーク設定を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ネットワーク設定でL2モードを許可する** - NetScalerインスタンスでL2モードを許可できます。ネットワーク設定でL2モードを許可を選択します。インスタンスにログオンしてL2モードを有効にする前に。

  **注**

  インスタンスのL2モードを無効にする場合は、そのインスタンスにログオンしてL2モードを無効にする必要があります。そうしないと、インスタンスを再起動した後に他のすべてのNetScalerモードが無効になる可能性があります。

- **0/1** - **VLANタグ**で、管理インターフェースのVLAN IDを指定します。
- **0/2** - **VLANタグ**で、管理インターフェースのVLAN IDを指定します。

デフォルトでは、インターフェース **0/1** および **0/2** が選択されています。

☐ **データインターフェース**で、**追加**をクリックしてデータインターフェースを追加し、以下を指定します。

- **インターフェース** - リストからインターフェースを選択します。

  **注**

  インスタンスに追加するインターフェースのインターフェースIDは、SDXアプライアンス上の物理インターフェースの番号付けに必ずしも対応しません。

  たとえば、インスタンス1に関連付ける最初のインターフェースがSDXインターフェース1/4である場合、そのインスタンスでインターフェース設定を表示すると、インターフェース1/1として表示されます。このインターフェースは、インスタンス1に関連付けた最初のインターフェースであることを示します。

- **許可されたVLAN** - NetScalerインスタンスに関連付けることができるVLAN IDのリストを指定します。
- **MACアドレスモード** - インスタンスにMACアドレスを割り当てます。次のいずれかのオプションから選択します。
  - **デフォルト** - Citrix WorkspaceがMACアドレスを割り当てます。
  - **カスタム** - このモードを選択して、生成されたMACアドレスを上書きするMACアドレスを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **生成済み** - 以前に設定されたベースMACアドレスを使用してMACアドレスを生成します。

- **VMAC設定 (仮想MACを構成するためのIPv4およびIPv6 VRID)**
  - **VRID IPv4** - VMACを識別するIPv4 VRID。指定可能な値: 1〜255。詳細については、「インターフェースでのVMACの構成」を参照してください。
  - VRID IPv6 - VMACを識別するIPv6 VRID。指定可能な値: 1〜255。詳細については、「インターフェースでのVMACの構成」を参照してください。

データインターフェースの追加(/en-us/netscaler-application-delivery-management-software/media/add-data-interface.png)

「**追加**」をクリックします。

### ステップ6 - 管理VLAN設定の指定

管理サービスとVPXインスタンスの管理アドレス (NSIP) は同じサブネットワーク内にあり、通信は管理インターフェースを介して行われます。

管理サービスとインスタンスが異なるサブネットワークにある場合は、VPXインスタンスをプロビジョニングする際にVLAN IDを指定します。これにより、インスタンスがアクティブになったときにネットワーク経由で到達可能になります。

デプロイメントで、VPXインスタンスのプロビジョニング中にNSIPが選択されたインターフェース経由でのみアクセス可能である必要がある場合は、「**NSVLAN**」を選択します。これにより、NSIPは他のインターフェース経由ではアクセスできなくなります。

- HAハートビートは、NSVLANの一部であるインターフェースでのみ送信されます。
- NSVLANは、VPX XVAビルド`9.3-53.4`以降でのみ構成できます。

**重要**

- VPXインスタンスをプロビジョニングした後、この設定を変更することはできません。
- **NSVLAN**が選択されていない場合、VPXインスタンスの`clear config full`コマンドはVLAN構成を削除します。

VLANの管理(/en-us/netscaler-application-delivery-management-software/media/manage-vlan-settings.png)

「**完了**」をクリックしてVPXインスタンスをプロビジョニングします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### プロビジョニングされたVPXインスタンスの表示

新しくプロビジョニングされたインスタンスを表示するには、次の手順を実行します。

1. 「**インフラストラクチャ > インスタンス > NetScaler**」に移動します。
2. 「**VPX**」タブで、「**ホストIPアドレス**」プロパティでインスタンスを検索し、SDXインスタンスのIPアドレスを指定します。

「プロビジョニングされたVPXインスタンスを表示」(/en-us/netscaler-application-delivery-management-software/media/provisioned-vpx-on-sdx.png)

## VMware ESX上にNetScaler VPXインスタンスをプロビジョニングする

NetScaler Consoleを使用して、VMware ESXでのNetScaler VPXインスタンスの展開と管理を自動化できます。NetScaler Consoleを使用してVMware ESX上にNetScaler VPXインスタンスをプロビジョニングすると、そのインスタンスはNetScaler Console GUIで管理できるようになります。

NetScaler Consoleは、すでに展開されているインスタンスのNetScalerテンプレートを使用して、VMware ESXに新しいインスタンスをプロビジョニングします。必要なVMware ESXサーバーの詳細がサイトに存在するVMware vCenterのデータセンターを保存します。また、クラウドアクセスプロファイルを使用してVMware vCenterにアクセスし、VMware ESX上にVPXを展開します。

### 前提条件

VMware ESXにNetScaler VPXインスタンスをプロビジョニングする前に、以下を完了していることを確認してください。

1. サポートされているVMware ESXiバージョン（6.0、6.5、および6.7）をインストールする。
2. 最小システム要件を満たす管理ワークステーションにVMware Clientをインストールする。
3. NetScaler VPXセットアップファイルのダウンロード(/ja-jp/citrix-adc/current-release/deploying-vpx/install-vpx-on-esx#downloading-the-netscaler-adc-vpx-setup-files)。
4. NetScaler VPXファイルをESXのテンプレートに変換する(/ja-jp/netscaler-application-delivery-management-software//current-release/networks/instance-management/provision-vpx-instances-on-vmware.html#convert-netscaler-vpx-files-into-templates)。
5. NetScaler ConsoleがVMware vCenterにアクセスするための権限を作成する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/provision-vpx-instances-on-vmware.html#create-permissions-for-netscaler-console-to-access-vmware-vcenter)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. NetScaler Consoleでサイトを作成する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/provision-vpx-instances-on-vmware.html#create-a-site-in-netscaler-console)。

### NetScaler VPXファイルをテンプレートに変換する

NetScaler Consoleは、NetScaler VPXファイルによって変換されたESX内のNetScalerテンプレートを使用します。VPXファイルをテンプレートに変換するには、次の手順を実行します。

1. NetScalerセットアップファイルを使用して、NetScaler VPXインスタンスをVMwareに展開します。

   初回は、NetScalerセットアップファイルを使用してVPXインスタンスを展開します。詳細については、「VMwareへのNetScaler VPXインスタンスのインストール」を参照してください。
2. デプロイされたVMを右クリックし、**テンプレート**を選択します。
3. **テンプレートに変換**をクリックします。

VPXセットアップファイルをテンプレートに変換(/en-us/netscaler-application-delivery-management-software/media/convert-to-template.png)

### NetScaler ConsoleがVMware vCenterにアクセスするための権限を作成する

VMware vCenterでNetScaler Consoleのプロビジョニングと管理を有効にするには、次の手順に従います。

1. 権限を持つカスタムロールを作成する

   a. VMware vCenterにログインし、**ロール**セクションに移動します。

   b. NetScaler Console用に調整されたカスタムロールを作成します。

   c. 次の権限を割り当てます。

```
Datastore.AllocateSpace

Resource.AssignVMToPool

VirtualMachine.Config.AdvancedConfig

VirtualMachine.Inventory.CreateFromExisting

VirtualMachine.Inventory.Delete

VirtualMachine.Interact.PowerOff
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
VirtualMachine.Interact.PowerOn

VirtualMachine.Provisioning.DeployTemplate
```

2. ユーザーを作成する
    a. ロールが定義されたら、**ユーザーとグループ**セクションに移動します。
    b. NetScaler ConsoleがVMware vCenterにアクセスするためのユーザーを作成します。
    c. 新しく作成したユーザーのパスワードを設定します。
3. ロールをユーザーに関連付ける
    a. **グローバル権限**セクションに移動し、カスタムロールをユーザーに関連付けます。
    b. この関連付けにより、NetScaler Console は VMware vCenter で必要なアクションを実行するための特権を得られます。

**注:**

記載されている特権は、NetScaler Console が VMware vCenter にアクセスするための最小要件です。制限された特権を持つユーザーを作成することはオプションです。指定された特権のスーパーセットを含む特権を持つユーザーがいる場合、そのユーザーは代わりにそれらの資格情報を提供できます。

VMware vCenter で特権を持つユーザーロールを構成する方法の詳細については、「ユーザーアクセスを構成する」を参照してください。

### NetScaler Console でサイトを作成する

NetScaler Console でサイトを作成し、VMware ESX の詳細を追加します。

1. NetScaler Console で、 **> >** の順に移動します。
2. をクリックします。
3. ペインで、,
    a. タイプとして を選択します。
    b. リストから を選択します。
    c. をクリックします。
4. ペインで、,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. ペインで、VMware ESX 用に作成したプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。

b. クラウドアクセスプロファイルを作成するには、 をクリックして以下を指定します。

- **名前** – NetScaler Console でクラウドアクセスプロファイルを識別するための名前を指定します。
- **IPアドレス** – VPXインスタンスをプロビジョニングするVMware vCenterサーバーのIPアドレスを指定します。
- **ユーザー名** – VMware vCenterサーバーにアクセスするためのユーザー名を指定します。
- **パスワード** – VMware vCenterサーバーにアクセスするためのパスワードを指定し、パスワードを確認します。

c. **ネットワーク (データセンター)** で、NetScaler テンプレートがあるデータセンターを選択します。

d. **サイト名** を指定します。

e. データセンターの地理的位置を識別するために、**地域**、**緯度**、**経度** を指定します。

f. **完了** をクリックします。

### VMware ESX でインスタンスをプロビジョニングする

VMware ESX に関連付けたサイトを使用して、NetScaler VPX インスタンスをプロビジョニングします。

**注:**

現在、NetScaler Console はスタンドアロンの NetScaler インスタンスのプロビジョニングのみをサポートしています。

1. NetScaler Console で、**インフラストラクチャ > インスタンス > NetScaler** に移動します。
2. 「**VPX**」タブで、「**Provision**」をクリックします。

   このオプションは、「**Provision NetScaler VPX on Cloud**」ページを表示します。
3. 「**VMware vCenter**」を選択し、「**Next**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VMware vCenterを選択(/en-us/netscaler-application-delivery-management-software/media/select-vmware.png)

4. 「**Basic Parameters**」で、以下を指定します。

   - **名前** – インスタンスの名前を指定します。
   - **サイト** – 以前に作成したサイトを選択します。
   - **クラウドアクセスプロファイル** – サイト作成時に作成したクラウドアクセスプロファイルを選択します。
   - **NetScalerプロファイル** – 認証を提供するためのNetScalerプロファイルを選択します。
   - **ライセンス** – プールされたキャパシティライセンスを使用して、インスタンスにライセンスを適用します。

   基本パラメータ(/en-us/netscaler-application-delivery-management-software/media/basic-parameters-vmware.png)

5. 「**Next**」をクリックします。
6. 「**Provision Parameters**」で、以下の詳細を指定します。

   - **クラスター** – インスタンスをプロビジョニングするクラスターを選択します。
   - **ホスト** – リストから必要なホストを選択します。
   - **テンプレート** – インスタンスに適用するテンプレートをリストから選択します。
   - **データストア** – リストからデータストアを選択します。
   - **IPアドレス** – インスタンスにIPアドレスを指定します。
   - **ネットマスク** – インスタンスにネットマスクを指定します。
   - **ゲートウェイ** – インスタンスにゲートウェイを指定します。

   ▢

7. VPXインスタンスをプロビジョニングするには、**完了**をクリックします。

## 複数のNetScaler VPXインスタンスを再検出する

NetScaler Consoleセットアップで複数のNetScaler VPXインスタンスを再検出できます。また、それらのインスタンスの最新の状態と構成を表示したい場合にも、複数のNetScaler VPXインスタンスを再検出できます。NetScaler Consoleサーバーは、すべてのNetScaler VPXインスタンスを再検出し、Citrix NetScalerインスタンスが到達可能であるかどうかを確認します。

**複数のNetScaler VPXインスタンスを再検出するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Webブラウザで、NetScaler ConsoleサーバーのIPアドレスを入力します (例：`<http://192.168.100.1>`)。
2. **ユーザー名**と**パスワード**のフィールドに、管理者資格情報を入力します。デフォルトの管理者資格情報は`nsroot`と`nsroot`です。
3. **Infrastructure > Instances > NetScaler** > **VPX**タブに移動し、再検出するインスタンスを選択します。
4. **アクションの選択**メニューで、**再検出**をクリックします。
5. 再検出ユーティリティを実行するための確認メッセージが表示されたら、**はい**をクリックします。

   画面には、各NetScaler VPXインスタンスの再検出の進行状況が表示されます。

## インスタンスの管理を解除する

NetScaler Consoleとネットワーク内のインスタンス間の情報交換を停止したい場合は、インスタンスの管理を解除できます。

NetScalerインスタンスの管理を解除すると、そのNetScalerインスタンスはNetScaler Consoleから管理対象外または登録解除された状態になります。NetScaler Consoleは、NetScaler Consoleベースの機能を実行するために、NetScalerインスタンスにアクセスしたり、通信したりできなくなります。

LASベースのライセンスに関して、NetScalerインスタンスの管理を解除すると、そのNetScalerインスタンスはLASベースのライセンスを失います。

**インスタンスの管理を解除するには:**

**Infrastructure > Instances > NetScaler** \> **VPX**タブに移動します。インスタンスのリストで、インスタンスを右クリックして**Unmanage**を選択するか、インスタンスを選択し、**Select Action**リストから**Unmanage**を選択します。

選択したインスタンスのステータスは、次の図に示すように**Out of Service**に変わります。

インスタンスの管理を解除する(/en-us/netscaler-application-delivery-management-software/media/unmanage-instances-2-1.png)

## インスタンスへのルートをトレースする

NetScaler Consoleからインスタンスへのパケットのルートをトレースすることで、インスタンスに到達するために必要なホップ数などの情報を見つけることができます。Traceroutは、送信元か

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ら宛先へのパケットのパスをトレースします。ルート内の各エンティティのホスト名とIPアドレスとともに、ネットワークホップのリストを表示します。

Tracerouteは、パケットが1つのホップから別のホップへ移動するのにかかった時間も記録します。パケットの転送に中断があった場合、tracerouteは問題がどこにあるかを示します。

**インスタンスのルートをトレースするには：**

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler** > **VPX**タブに移動します。
2. インスタンスのリストで、インスタンスを右クリックして**TraceRoute**を選択するか、インスタンスを選択して**Select Action**メニューから**TraceRoute**をクリックします。

**TraceRoute**メッセージボックスには、インスタンスへのルートと、各ホップで消費された時間（ミリ秒単位）が表示されます。



## NetScalerが所有するIPアドレスを表示する

NetScaler Console GUIから直接、NetScalerインスタンスに設定されているIPアドレスを表示できます。設定変更やその他の操作は、NetScalerインスタンスでのみ実行できます。

NetScalerが所有するIPアドレスを表示するには、**インフラストラクチャ > インスタンス > NetScaler所有IP**に移動します。

この機能は、NetScalerインスタンスに設定されているIPv4アドレスとIPv6アドレスの両方を表示します。IPアドレスの種類は次のとおりです。

- NetScaler IPアドレス
- サブネットIPアドレス
- 仮想IPアドレス
- ADNSサービスIPアドレス
- GSLB IPアドレス
- クラスターIPアドレス
- マップ済みIPアドレス



### NetScalerが所有するIPアドレスをエクスポートする

NetScalerが所有するIPアドレスをエクスポートするには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **インフラストラクチャ > インスタンス > NetScaler所有IP**に移動します。
2. 「**NetScaler Owned IPs**」ページで、右上隅にあるエクスポートアイコンをクリックします。
3. 「**Export Reports**」ページで、「**Export Now**」をクリックします。
4. 「**Export Now**」ページで、エクスポートオプションを選択します。

   **スナップショット**のエクスポートの場合:

   a. エクスポートファイル形式を選択します: PDF、JPG、またはPNG。

      スナップショットのエクスポート(/en-us/netscaler-application-delivery-management-software/media/export-now-snapshot.png)

   **表形式**のエクスポートの場合:

   a. エクスポートファイル形式を選択します: PDFまたはCSV。
   b. リストからエクスポートするデータレコードの数を選択します。

      表形式のエクスポート(/en-us/netscaler-application-delivery-management-software/media/export-now-tabular.png)

5. 「**Export**」をクリックします。

### NetScalerが所有するIPアドレスのエクスポートをスケジュールする

NetScalerが所有するIPアドレスのエクスポートをスケジュールするには:

1. **Infrastructure > Instances > NetScaler Owned IPs**に移動します。
2. 「**NetScaler Owned IPs**」ページで、右上隅にあるエクスポートアイコンをクリックします。
3. 「**レポートのエクスポート**」ページで、「**エクスポートのスケジュール**」をクリックします。
4. 「**エクスポートのスケジュール**」ページで、次の詳細を入力します。

   a. 件名と説明を入力します。
   b. エクスポートタイプを選択します。

      「**スナップショット**」エクスポートタイプの場合:

      - エクスポートファイル形式を選択します: PDF、JPG、またはPNG。

      「**表形式**」エクスポートタイプの場合:

      - エクスポートファイル形式を選択します: PDFまたはCSV。
      - リストからエクスポートするデータレコードの数を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 繰り返しを選択します: 毎日、毎週、または毎月。

d. エクスポート時間を選択します。

e. エクスポートされたIPアドレスの送信方法を選択します: メール、Slack、またはその両方。

メールの場合:

- 「**メール**」を選択し、NetScalerが所有するIPアドレスのリストを送信するメール配信リストを選択します。
  - メール配信リストを追加するには、「**追加**」をクリックし、メールサーバーの詳細を指定します。
  - メール配信リストを編集するには、**編集**をクリックします。
  - メール配信リストが機能していることを確認するには、**テスト**をクリックします。これにより、選択したメール配信リストにテストメールが送信されます。

Slackの場合:

- **Slack**を選択し、NetScalerが所有するIPアドレスのリストを送信するSlackプロファイルリストを選択します。
  - Slackプロファイルを追加するには、**追加**をクリックし、Slackチャネルの**プロファイル名**、**チャネル名**、および**トークン**を指定します。
  - 既存のSlackチャネルを編集するには、**編集**をクリックします。

5. エクスポートをスケジュールするには、**スケジュール**をクリックします。

スケジュールされると、エクスポートスケジュールは**エクスポートレポート**ページに表示され、スケジュールを選択して編集または削除操作を実行できます。選択したスケジュールを編集した後、**保存**をクリックして編集した変更を保存します。**削除**はスケジュールを削除します。

## あるNetScalerインスタンスから別のインスタンスへの構成のレプリケート

NetScaler Consoleの構成レプリケート機能を使用して、NetScalerインスタンスから構成をコピーし、単一のインスタンスまたは複数のインスタンスにレプリケートできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### あるインスタンスから他のNetScalerインスタンスに構成をレプリケートするには

1. **インフラストラクチャ > インスタンス > NetScaler**に移動します。構成を他のインスタンスにレプリケートするソースインスタンスを選択し、**アクションの選択**リストから**構成のレプリケート**をクリックします。
2. **構成のレプリケート**で、ソースインスタンスから構成を適用するターゲットインスタンスを選択します。単一のソースインスタンスから単一のインスタンスまたは複数のターゲットインスタンスに構成をレプリケートできます。

   
3. **作成**をクリックします。

レプリケートされた構成は、NetScaler®インスタンスのリストに追加されます。レプリケートされたインスタンスのステータスを表示するには、更新アイコンをクリックします。

**注：**

レプリケーション中、ソースインスタンスのすべてのネットワークIPがターゲットインスタンスにレプリケートされます。ターゲットインスタンスがソースインスタンスとは異なるネットワークにある場合、ターゲットインスタンスのIPに到達できない可能性があります。IPに到達できない場合、ターゲットインスタンス内のエンティティのステータスは「ダウン」と表示されます。

管理対象のNetScalerインスタンスで構成されているエンティティのステータスを表示するには、**インフラストラクチャ > ネットワーク機能**に移動します。

## SSL証明書管理

機密情報または機微な情報の取り扱いを必要とする組織または個人のWebサイトには、SSL証明書が必要です。Webサーバー上のSSL証明書は、接続クライアントに対するWebサーバーの信頼性を保証するのに役立ちます。これにより、WebサイトのIDが認証されるだけでなく、セッション全体の暗号化に後で使用されるセッションキーの生成にも役立ちます。

Secure Socket Layer (SSL) 証明書は、あらゆるSSLトランザクションの一部であり、企業 (ドメイン) または個人を識別するデジタルデータ形式 (X509) です。この証明書には、サーバーとの安全なトランザクションを開始したいクライアントに表示される公開鍵コンポーネントがあります。Citrix NetScalerアプライアンスに安全に格納されている対応する秘密鍵は、非対称鍵 (または公開鍵) の暗号化と復号化を完了するために使用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleは、SSL証明書のインストール、更新、削除、リンク、ダウンロードを自動化するための統合コンソールを提供します。これにより、Webサイトの評判と顧客の信頼を維持するのに役立ちます。NetScaler Consoleは、証明書管理のあらゆる側面を効率化します。統合コンソールを通じて、組織のITポリシーに従って、推奨される発行者、鍵強度、プロトコル、アルゴリズムを保証する自動ポリシーを構成できます。これにより、未使用または期限切れ間近の証明書を厳重に監視できます。

SSL証明書と鍵は、以下のいずれかの方法で取得できます。

- Verisignなどの認証局 (CA) から
- NetScalerアプライアンスで新しいSSL証明書と鍵を生成する

## エンタープライズSSLポリシー設定

すべての企業は独自のSSLポリシーを持ち、すべてのSSL証明書が遵守しなければならない要件を定義しています。セキュリティは常にすべてのエンタープライズユーザーにとって最優先事項の1つであり、そのためSSL設定は重要な役割を果たします。

たとえば、ABC社は、すべての証明書が2,048ビット以上の最小鍵強度を持つことを義務付けています。証明書は、信頼できるCAまたは発行者によって承認されている必要があります。管理者は、証明書が会社のポリシーを遵守していることを確認するために、すべてのSSLパラメータを確認する必要があります。各証明書を手動で検証するのは面倒な作業です。このシナリオを克服するために、NetScaler Consoleはエンタープライズ SSLポリシー設定を構成するのに役立ち、「推奨されません」タグ付きの非準拠証明書を表示します。

SSLダッシュボードで、非準拠 (推奨されません) 証明書の概要を表示できます。



**注**

「推奨されません」証明書はさまざまなパラメータに基づいて分類されており、関連するコンポーネントで表示できます。

## NetScaler Console証明書の仕組み

SSLダッシュボードは、異なるNetScalerインスタンスにインストールされているすべてのSSL証明書の視覚的な表示を提供します。SSLダッシュボードには、NetScalerインスタンスにインストールされている各証明書に関する以下の情報が含まれています。これは以下に基づいて分類されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **自己署名 vs CA署名。** 自己署名 vs CA署名セクションは、証明書を自己署名証明書とCA署名証明書に分類するのに役立ちます。
- **署名アルゴリズム。** このセクションでは、暗号化に使用されている署名アルゴリズムに基づいてSSL証明書を分類します。
- **使用状況。** このセクションでは、使用されている証明書と未使用の証明書に基づいてSSL証明書を分類します。未使用の証明書は、仮想サーバーにバインドし忘れている可能性があるため、特別な注意が必要です。
- **発行者。** このセクションでは、証明書の発行者に基づいてSSL証明書を分類します。
- **鍵強度。** このセクションでは、秘密鍵の鍵強度に基づいてSSL証明書を分類します。
- **上位10インスタンス。** このセクションでは、インストールされているSSL証明書の数に基づいて、上位10のNetScalerインスタンスの詳細を提供します。



## SSL証明書管理のユースケース

以下のユースケースでは、SSL証明書を使用して複数のNetScalerインスタンス間で証明書を管理および監視する方法について説明します。

### SSL証明書のインストール

必要なSSL証明書を展開する必要があるNetScalerインスタンスのフリートがあると想像してください。NetScaler Consoleは、複数のNetScalerインスタンスに一度にSSL証明書を展開するための統合コンソールを提供します。

たとえば、1つまたは複数のNetScalerインスタンスにいくつかのSSL証明書をインストールしたい場合があります。このアプローチにより、各NetScalerインスタンスにSSL証明書をインストールする手動介入を最小限に抑えることができます。1つまたは複数のNetScalerインスタンスにSSL証明書を一括インストールできます。

SSL証明書の概要を取得するには、**NetScaler Console**にログオンし、**Infrastructure > SSL Dashboard**に移動します。

### 証明書の有効期限に関する通知設定

このユースケースでは、複数のNetScalerインスタンスにわたって多数の証明書を所有している場合があり、各証明書の有効期限を追跡することが負担になります。各証明書を手動で追跡し、有効期限が切れる前に更新することは面倒な作業です。このようなシナリオを避けるために、NetScaler Consoleを構成して、構成済みの電子メール、ポケットベル、Slack、または

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ServiceNowプロファイルに通知またはアラートを送信できます。これにより、証明書の有効期限を常に把握し、有効期限が切れるかなり前に証明書を更新できます。

たとえば、有効期限が近づいている証明書の追跡を忘れる可能性があります。そして、証明書の有効期限が切れるとサービス停止が発生し、多数のユーザーアプリケーションに影響を与える可能性があります。NetScaler Consoleの証明書有効期限通知設定を使用すると、このような予期せぬシナリオを回避できます。

**SSLダッシュボード**で、有効期限が近づいている証明書の概要を表示し、追跡できます。

任意の期間に有効期限が切れる証明書のレポートを表示するには、タイルをクリックして、その期間に有効期限が切れるすべての証明書の詳細を取得できます。

有効期限切れのSSL証明書(/en-us/netscaler-application-delivery-management-software/media/expiry-ssl-certificate.png)

### 証明書の更新

NetScaler Consoleから証明書を更新できるようになりました。既存の証明書を更新するか、以下に基づいて証明書を作成できます。

#### 既存の証明書を更新する

このユースケースでは、認証局 (CA) から更新された証明書を受け取ったら、既存の証明書を更新する必要があります。NetScalerインスタンスにログインすることなく、NetScaler Consoleから既存の証明書を更新できるようになりました。

たとえば、既存の証明書に変更や修正がある場合があります。CAは更新された証明書を発行します。NetScalerアプライアンスにアクセスする代わりに、NetScaler ConsoleからSSL証明書を更新できるようになりました。

証明書を更新するには、NetScaler Consoleにログオンし、**Infrastructure > SSL Dashboard**に移動します。

更新したい証明書を選択し、**Update**をクリックします。

NetScaler Consoleから、選択した証明書の関連フィールドを更新するオプションがあります。

SSL証明書更新ページ(/en-us/netscaler-application-delivery-management-software/media/update-ssl-certificate-page.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 証明書署名要求の作成

組織のポリシーに準拠していないSSL証明書があるユースケースを想像してください。認証局から新しい証明書を取得したいとします。NetScaler Consoleから証明書署名要求 (CSR) を生成できるようになりました。CSRと公開鍵をCAに送信して、SSL証明書を取得できます。

CSRを決定して作成するには、目的の証明書を選択し、 をクリックします。

公開鍵または秘密鍵のペアが必要です。鍵をアップロードするには、 をクリックしてリストから選択します。鍵を作成するには、 オプションを選択し、関連するパラメーターを指定します。

キーペアCSRの作成(/en-us/netscaler-application-delivery-management-software/media/create-key-pair-csr.png)

CSRを作成するために、選択したキーの共通名、組織名、都市、国、都道府県、組織単位、メールIDなどの詳細情報を提供します。

CSRキーの詳細(/en-us/netscaler-application-delivery-management-software/media/csr-key-info-details.png)

### SSL証明書のリンクとリンク解除

複数のSSL証明書を相互にバインドして、証明書バンドルを作成できます。ある証明書を別の証明書にリンクするには、最初の証明書の発行者が2番目の証明書のドメインと一致している必要があります。

証明書のリンクとリンク解除(/en-us/netscaler-application-delivery-management-software/media/link-unlink-ssl-certificate.png)

### 監査ログ

監査ログは、NetScaler Consoleによって生成されるテキストログファイルのコレクションです。NetScaler Consoleを使用して特定のNetScalerアプライアンスに追加、変更、および変更されたSSL証明書の履歴を表示します。監査ログには、NetScalerアプライアンスのIPアドレス、ステータス、開始時刻、および特定の操作の終了時刻も表示されます。

この例では、特定の証明書に対して一定期間に発生した変更を検証したい場合があります。また、デバイスログとコマンドログで証明書への変更履歴を表示するオプションがあります。

SSL証明書の情報を確認するには、 で をクリックします。アプリケーションの概要には、開始時刻と終了時刻を含むSSL証明書のステータスが含まれます。

SSL監査証跡(/en-us/netscaler-application-delivery-management-software/media/ssl-audit-trail.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

特定のSSL証明書のNetScalerアプライアンスの情報を確認するには、目的の関連する証明書チェックボックスを選択します。 をクリックします。



コマンドタイプとメッセージの情報を表示するには、「**コマンドログ**」をクリックします。



## ACMEプロトコルを使用した証明書の自動更新

NetScaler Consoleは、SSL/TLS証明書の更新を自動化するために設計されたオープンプロトコルであるACME（Automated Certificate Management Environment）をサポートしています。

以前は、ネットワーク管理者は証明書を更新するために、手間のかかる多段階の手動プロセスを経る必要がありました。ACMEのサポートは、証明書の自動更新のための堅牢なフレームワークを提供することで、これらの課題を軽減し、以下の操作を実行します。

- 信頼できる認証局（CA）から新しい証明書を要求する。
- 自動化された方法（例：DNS-01チャレンジ）を使用してドメインの所有権を検証する。
- 有効期限が切れる前に証明書を自動的に更新する。

### NetScaler® ConsoleでのACMEサポート

NetScaler Consoleは`acme.sh`クライアントを使用し、以下の認証局をサポートしています。

- レッツエンクリプト
- DigiCert Inc
- セクティゴ・リミテッド
- エントラスト・インク
- GlobalSign
- GoDaddy.com, Inc
- ZeroSSL
- Google トラスト サービス
- Google パブリック CA
- BuyPass Go SSL
- アクタリス
- SSL.com
- ハシコープ ヴォールト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- スモールステップ
- ペブル
- HARICA
- EJBCA

NetScaler Console での証明書の自動更新の仕組みを以下の手順で説明します。

1. NetScaler Console が `acme.sh` クライアントを使用してドメインの証明書要求を開始すると、クライアントは選択された認証局（例：Let's Encrypt または DigiCert）に接続します。
2. CA はドメイン所有権を証明するためのチャレンジを発行します。この場合、それは DNS-01 チャレンジです。
3. NetScaler Console は、事前に設定された資格情報を使用して、CA から提供された値でドメインの DNS TXT レコードを自動的に更新します。
4. CA は TXT レコードを検証し、ドメイン所有権を確認します。
5. 検証が成功すると、CAはSSL/TLS証明書をNetScaler Consoleに発行します。
6. NetScaler Consoleは、証明書をそれぞれのストア（証明書ストア/ゼロタッチストア）に保存します。
7. お客様が指定した更新期間に基づき、NetScaler Consoleは証明書の有効期限が切れる前に、この更新プロセスを自動的に繰り返します。

ACMEサポートのハイレベルアーキテクチャ(/en-us/netscaler-application-delivery-management-software/media/acme-high-level-architecture.png)

NetScaler ConsoleのACMEサポートにより、以下の操作を実行できます。

- 証明書の有効期限が切れる前に自動的に更新する
- 更新中にCAを切り替える
- CSRを生成またはアップロードし、新しい証明書を要求する

主な利点は以下のとおりです。

- 証明書の発行または更新において手動介入なしの完全自動化されたライフサイクル。
- 組織のニーズに合わせたカスタマイズ可能な更新スケジュール（例：有効期限の7日前に更新するように設定）。
- 期限切れの証明書によるダウンタイムを排除します。
- 有効期限の追跡と更新を自動化することで、運用上のオーバーヘッドを削減します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 常に有効で、CAのベストプラクティスに準拠した証明書により、セキュリティ体制が向上します。

### ACME統合のための設定手順

ACMEの統合は一度限りのプロセスであり、以下の手順が含まれます。

- ステップ1：認証局（CA）を構成します。
- ステップ2：更新する証明書を選択します。
- ステップ3：DNSプロバイダーを追加し、対応するドメインをマッピングします。

#### 前提条件

- 認証局（CA）の有効なアカウントと、そのライセンスを持っていることを確認してください。
- DNSプロバイダーのアクセス資格情報を持っていることを確認してください。

#### ステップ1：認証局（CA）を構成する

更新に使用される認証局（CA）を登録するには、以下の手順を実行します。

1. **Infrastructure > SSL Dashboard** に移動します。ACMEを初めて構成する場合、「SSL証明書の自動更新」というバナーが表示されます。**Get Started** をクリックします。

   

   または

   **Infrastructure > SSL Dashboard > Third-party Integration > CA Vendors** に移動し、**Add** をクリックします。
2. 名前を入力し、CAベンダーを選択します。現在、**Let's Encrypt** と **DigiCert Inc** のみがサポートされています。
3. メールアドレス、ACMEディレクトリURLなどのその他の詳細を入力します。
4. NetScaler Console が証明書を自動的に更新する必要がある日数を入力します。
5. **保存して続行**をクリックします。NetScaler Console は CA への接続を試行します。接続に失敗した場合は、提供された詳細を確認し、構成の詳細を修正してから再試行してください。

   

#### ステップ2：更新する証明書を選択します

CA の詳細が追加されると、NetScaler Console はすべての証明書（証明書ストアとゼロタッチストアの両方から）を自動的にスキャンし、構成された CA によって発行された証明書を個別に一覧表示します。一覧表示された証明書を確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 自動的に更新したい証明書を選択します。たとえば、Let's Encrypt を CA として構成し、Let's Encrypt から 2 つ、別のベンダーから 2 つの証明書がある場合、ダッシュボードには次のように表示されます: `Let's Encrypt: 2 and Other CA: 2`。



2. 別の CA によって発行された証明書を追加するには**追加**をクリックするか、自動的に更新したくない証明書を削除するには**削除**をクリックします。別のベンダーの証明書を選択すると、ベンダー変更を確認するプロンプトが表示されます。確認すると、これらの証明書は更新期間に達したときに、新しく構成された CA を通じて更新されます。

> **注:**
>
> 証明書ストアとゼロタッチ証明書ストアに重複する証明書がないことを確認してください。重複する証明書がある場合、更新プロセスは各ストアで2回実行されます。



3. **保存して続行**をクリックします。

> **注:**
>
> 証明書は更新後もそれぞれのストアに残ります。たとえば、証明書が証明書ストアに保存されている場合、その更新されたバージョンも証明書ストアに配置されます。証明書がゼロタッチストアに保存されている場合、その更新されたバージョンもゼロタッチストアに配置されます。

証明書の展開動作はストアの種類によって異なります。

- 証明書が証明書ストアに保存されている場合、それらは手動でNetScalerに展開する必要があります。
- 証明書がゼロタッチストアに保存されている場合、管理者の介入なしにNetScalerに自動的に展開されます。 更新された証明書のシームレスで完全に自動化された展開には、ゼロタッチ証明書管理を使用することをお勧めします。詳細については、「ゼロタッチ証明書管理」を参照してください。

### ステップ3：DNSプロバイダーを追加し、ドメインをマッピングする

1. **DNSプロバイダーとドメインマッピング**ページで**追加**をクリックします。
2. **DNSプロバイダーの選択**ドロップダウンリストからDNSプロバイダーを選択します。`acme.sh`でサポートされているDNSプロバイダーは、ドロップダウンリストに表示されま

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。リストにDNSプロバイダーが表示されない場合、それはサポートされていないことを意味します。

3. アクセスキーID、シークレットアクセスキーなどのプロバイダーの詳細を入力し、**保存**をクリックして設定を保存します。
4. **ドメインマッピング**の下にある**ドメインの追加**をクリックします。
5. 設定済みのDNSプロバイダーによって提供されるドメインを選択します。

**重要:**

各ドメインが正しいDNSプロバイダーにリンクされていることを確認してください。NetScaler Consoleはこれらのマッピングを使用して、DNS-01チャレンジを自動的に実行します。発行または更新中に、NetScaler ConsoleはマッピングされたDNSプロバイダーに必要なTXTレコードを作成します。検証が成功すると、CAは証明書を発行または更新します。証明書は、関連するすべてのドメインがDNSプロバイダーに正しくマッピングされている場合にのみ更新されます。

たとえば、組織がDNSプロバイダーとしてAmazon Route53を使用している場合。まず、DNSプロバイダーの詳細の下にAmazon Route53の資格情報（アクセスキーIDとシークレットキー）を追加します。次に、Amazon Route53によって管理されるドメイン（例：example.com、app.example.com）をマッピングします。これらのドメインの証明書が発行または更新されると、NetScaler ConsoleはAmazon Route53に必要なTXTレコードを自動的に作成します。検証が成功すると、CAは証明書を発行または更新します。
以下のパブリックDNSプロバイダーがサポートされています。

- 1984.ホスティング
- ACME DNS
- AcmeProxy サーバーAPI
- アクティブ24
- Akamai.com エッジDNS
- アリユン
- All-inkl Kas サーバー
- Alviy.com
- アマゾン ルート53
- Anexia.com CloudDNS
- ArtFiles.de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ArvanCloud.ir
- autoDNS-InternetX
- アジュール DNS
- Azion.om
- Beget.com
- BookMyName.com
- Bunny.net
- CloudFlare
- ClouDNS.net
- ConoHa
- Constellix.com
- コアネットワーク
- cPanel サーバーAPI
- Curanet.dk
- cyon.ch
- DDNSS.de
- deSEC.io
- DigitalOcean
- DirectAdmin
- DNSサービス
- DNSExit.com
- dns.la
- DNSMadeEasy
- DNSシンブル
- dnsHome.de
- DNSPod.cn
- DNSPod.com
- ドメイン・オフェンシブ do.de
- DomeneShop.no
- DreamHost

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DuckDNS.org
- durabledns.com
- Dyn.com
- DynDnsFree.de
- Dynu.com
- DynV6.com
- easyDNS.net
- エッジセンター DNS API
- EUserv.com
- エクソスケール
- Fornex.com
- FreeDNS
- FreeMyIP.com
- ガンディ ライブDNS
- Gcore.com
- GeoScaling.com
- GoDaddy.com
- グーグル クラウド DNS
- グーグル ドメイン
- Hetzner.com
- Hexonet.com
- hosting.de
- HuaweiCloud.com
- ハリケーンエレクトリック
- ハリケーンエレクトリック HE.net DDNS
- インフォブロックス
- Infomaniak.com
- INWX
- イオノス クラウド DNS
- IONOS.de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- InternetBS.net
- アイエスピーコンフィグ 3.1
- jdcloud.com
- Joker.com
- kapper.net
- King.host
- ノットDNS
- Leaseweb.com
- レキシコンDNSクライアント
- リマシティ.de
- リノード
- Linode.com-Old
- ルーピア
- LuaDNS
- MailinaBox
- MaraDNS
- mijn.host
- Misaka.io
- MyDNS.JP
- ミシックビースト.com
- Name.com
- ネームチープ
- NameMaster.de
- ネームシロ
- Nanelo.com
- NederHost.nl
- Neodigit.net
- ネットカップ
- Netlify.com
- nic.ru

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ニャラ
- NLnetLabs NSD
- NS1.com
- ネクセス
- one.com
- Online.net
- omg.lol
- OpenProvider
- オープンスタック Designate API
- オーピーエヌセンス
- オラクル クラウド インフラストラクチャ - OCI
- OVH.com
- プレスク XML
- PointHQ
- Porkbun.com
- PowerDNS
- RackCorp.com
- RackSpace.com
- rage4.com
- RcodeZero
- reg.ru
- ScaleWay.com
- シュルントテック
- セレクテル
- SelfHost.de
- ServerCow.de
- Simply.com
- テクニティウム DNS サーバー
- tele3.cz
- Tencent.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Timeweb.Cloud
- TransIP.nl
- UltraDNS
- ユナイテッドドメインズ リセリング
- unoeuro.com
- variomedia.de
- Vercel.com
- veesp.com
- versio.nl AuroraDNS
- VSCALE
- vshosting.cz CloudDNS
- ヴァルチャー
- Websupport.sk
- West.cn
- World4You.com
- ヤンデックス 360 for Business DNS API。
- ヤンデックス クラウド DNS
- ジローレ
- Zone.eu
- ZoneEdit.com
- ゾノミ

これら3つのステップがすべて完了すると、NetScaler ConsoleはACME CAサーバーを設定します。選択された証明書は、マッピングされたドメインに対して更新されます。 NetScaler Consoleは定期的に証明書の有効性をチェックし、有効期限が切れる前に（設定された期間に基づいて）更新します。手動での介入が不要なため、証明書は常に有効で最新の状態に保たれます。

### 発行と更新

すべての更新アクティビティと、証明書発行から発生した新しいリクエストを確認するには、**Infrastructure > SSL Dashboard > Issuance & Renewals**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 自動更新

**Automatic renewals**タブには、自動更新に登録されている証明書が一覧表示されます。設定された更新期間に達すると、NetScaler Consoleはそれらを自動的に更新します。

スケジュールされた更新期間の前に、オンデマンドで更新をトリガーすることもできます。オンデマンド更新の場合は、必要な証明書を選択し、**Renew now**をクリックします。

一部の証明書を自動的に更新したくない場合は、手動更新に移行できます。証明書を自動更新から手動更新に移行するには、必要な証明書を選択し、**Migrate to manual renewal**をクリックします。

### 手動更新

**Manual renewals**タブには、手動で更新する必要があるすべての証明書が一覧表示されます。これらの証明書は、オフラインで証明書を更新して適切なストアに新しい証明書をアップロードするか、**Renew now**オプションを使用して手動で更新する必要があります。

証明書を更新するには、証明書を選択して**Renew now**をクリックします。証明書が登録済みのCAによって発行され、そのドメインのDNSプロバイダーが設定されている場合、自動更新に移行することなく、ACMEを使用してオンデマンドで更新できます。

証明書を自動更新に移行することもできます。証明書を手動更新から自動更新に移行するには、必要な証明書を選択し、**Migrate to automatic renewal**をクリックします。

**注記：**

一度に更新または移行できる証明書は1つだけです。

ACMEサポートのハイレベルアーキテクチャ(/en-us/netscaler-application-delivery-management-software/media/acme-manual-renewals.png)

### 発行と更新のログ

「**発行と更新のログ**」タブには、ACMEを使用した証明書要求のリスト（発行と更新を含む）が表示されます。失敗したイベントについては、情報アイコンをクリックして詳細なエラー情報を表示できます。

ACMEサポートのハイレベルアーキテクチャ(/en-us/netscaler-application-delivery-management-software/media/acme-issuance-renewal-logs.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 証明書の発行

NetScaler ConsoleのACME統合は、ACMEプロトコルを使用して新しい証明書を直接要求することをサポートしています。NetScaler Console内でCSRを作成するか、既存のCSRをアップロードして新しい証明書を要求できます。

**Infrastructure > SSL dashboard > Issuances & Renewal**に移動し、**Issue Certificate**をクリックして、シナリオに基づいて以下のいずれかを選択します。

- 「**CSRがありません**」: CSRをまだ持っていない場合、NetScaler ConsoleでCSRを生成し、新しい証明書を発行できます。
- 「**CSRがあります**」: オフラインで生成されたCSRがすでにある場合、それをアップロードして証明書を発行できます。

#### CSRなしで証明書を発行する

CSRを生成して新しい証明書を発行するには、次の手順を実行します。

1. **Infrastructure > SSL dashboard > Issuances & Renewal**に移動し、**Issue Certificate**をクリックして、「**CSRがありません**」を選択します。

   ACMEサポート証明書の発行(/en-us/netscaler-application-delivery-management-software/media/acme-issue-certificate.png)
2. 「**Certificate key**」ページで、「**キーがあります**」を選択して既存のキーをアップロードするか、「**キーがありません**」を選択して新しいキーを生成します。

   ACME証明書キー(/en-us/netscaler-application-delivery-management-software/media/acme-certificate-key-without-csr.png)
3. 必要なCSR情報を入力します。

   
4. ACMEリクエストのCA、DNSプロバイダー、および証明書展開モードを選択します。手動展開の場合は**Cert Store**を、NetScalerでの自動展開の場合は**Zero Touch Store**を選択します。
5. 将来的に証明書を自動更新したい場合は、**証明書を自動更新**を選択します。

   
6. **保存**をクリックします。

#### CSRを使用して証明書を発行する

オフラインで生成されたCSRが既にあり、それをアップロードして証明書を発行したい場合は、以下の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Infrastructure > SSL dashboard > Issuances & Renewal**に移動し、**Issue Certificate**をクリックして**I have CSR**を選択します。



2. ローカルシステムからCSRファイルと関連するキーファイルを選択します。



3. ACMEリクエストのCA、DNSプロバイダー、および証明書展開モードを選択します。手動展開の場合は**Cert Store**を、NetScalerでの自動展開の場合は**Zero Touch Store**を選択します。
4. 将来的に証明書を自動更新したい場合は、**証明書を自動更新**を選択します。



5. **保存**をクリックします。

### サードパーティ統合

複数のCAベンダーとDNSプロバイダーを追加および管理できます。

**サードパーティ統合**ページから次のアクションを実行できます。

- CAベンダーを追加または編集します
- 自動更新設定を変更します
- 既存の構成済みCAから証明書を追加または編集します
- DNSプロバイダーを追加または編集します
- ドメインマッピングを変更します

#### CAベンダーを追加または編集します

異なるベンダーが発行した証明書を管理するために、複数のCAベンダーを登録できます。既存のCAベンダーの詳細を編集することもできます。

1. **SSLダッシュボード > サードパーティ統合 > ACME > CAベンダー**に移動します。**追加**をクリックします。
2. CAベンダーを追加するには、CAベンダーの名前を指定し、CAを選択します。
3. 既存のCAベンダーの詳細を編集するには、CAベンダーを選択し、**編集**をクリックします。
4. 必要な詳細を追加または更新します。
5. 「**保存**」をクリックします。

#### 自動更新設定を変更する

自動更新設定を変更するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **SSLダッシュボード > サードパーティ統合 > ACME > CAベンダー**に移動します。
2. CAベンダーを選択し、**編集**をクリックします。
3. 「**証明機関ベンダーの構成**」で、「**自動更新設定**」セクションの要件に応じて日数を変更します。
4. 「**保存して続行**」をクリックします。
5. ワークフローを完了します。

### 既存の構成済みCAから証明書を追加または編集する

既存の構成済みCAから証明書を追加または編集するには、次の手順を実行します。

1. **SSLダッシュボード > サードパーティ統合 > ACME > CAベンダー**に移動します。
2. CAベンダーを選択し、**編集**をクリックします。
3. 「**ステップ2 証明書の選択**」に移動し、必要な証明書を追加または削除します。
4. 「**保存して続行**」をクリックします。
5. ワークフローを完了します。

**注記:**

証明書が元のCAからマッピング解除されていない場合、新しいCAの選択リストには表示されません。

### DNSプロバイダーの追加または編集

新しいDNSプロバイダーを追加するか、既存のDNSプロバイダーの既存のドメインマッピングを編集するには、次の手順を実行します。

1. **SSLダッシュボード > サードパーティ統合 > ACME > DNSプロバイダー**に移動します。
2. DNSプロバイダーを追加するには、**追加**をクリックします。DNSプロバイダーを選択し、**保存**をクリックします。
3. 既存のDNSプロバイダーを編集するには、DNSプロバイダーを選択し、**編集**をクリックします。
4. 必要な詳細を追加または更新します。
5. **保存**をクリックします。

### ドメインマッピングの変更

既存のDNSプロバイダーのドメインマッピングを編集するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **SSLダッシュボード > サードパーティ統合 > ACME > DNSプロバイダー**に移動します。
2. DNSプロバイダーを選択し、**編集**をクリックします。
3. **ドメインマッピング**に移動し、必要に応じてドメインを追加または削除します。
4. **保存**をクリックします。

**重要:**

ドメインがマッピング解除されると、証明書の更新は停止します。更新が継続されるように、常にドメインを有効なDNSプロバイダーに再マッピングしてください。

### 制限事項

- 証明書の更新は、`acme.sh`でサポートされているDNSプロバイダーに対してのみ行われます。

### 自動証明書更新に関する問題のトラブルシューティング

発生する可能性のある一般的なエラーメッセージとその根本原因をこのセクションに示します。

- 証明書のドメイン名がACME要件に従って有効でない場合、**Certificate has invalid domain - ADCD**エラーが報告されます。
- 要求されたドメイン名にドットがない場合（「example.com」ではなく「example」など）、**Invalid identifiers requested :: Cannot issue for "testdomain": Domain name needs at least one dot**が報告されます。
- ACMEクライアントがCAからノンスを取得できない場合（多くの場合、ネットワークまたはサーバーの問題が原因）、**Could not get nonce from the CA server. Please check the CA server configuration.**が報告されます。
- ACMEクライアントがCAサーバーとの通信を初期化できない場合（設定ミスが原因である可能性あり）、**Cannot initialize API for the CA server. Please check the CA server configuration.**が報告されます。
- ドメイン名の形式が無効であるか、ACMEプロトコルで許可されていない場合、**Invalid domain name provided. Please check the domain name and try again.**が報告されます。
- ドメインリストに変更がなく、証明書がすでに存在する場合に証明書要求が行われると、**Domains not changed. Certificate with same configuration already exists.**が報告されます。
- ACMEクライアントがドメイン検証に必要なDNS TXTレコードを追加できない場合、**Error adding TXT record for domain validation. Please check the DNS configuration and try again.**が報告されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 署名が一致しない場合（多くの場合、クライアントとサーバー間の時刻同期の問題が原因）、**Signature does not match. Please check the server time as it may not be in sync.**が報告されます。
- DNSベースのドメイン検証にDNSプロバイダーが指定されていない場合、**Certificate is missing a DNS provider name.**が報告されます。
- 「**アクティブなDNSプロバイダーが設定されていないため、更新はスキップされました。**」は、証明書の更新が試行されたが、アクティブなDNSプロバイダーが設定されていない場合に報告されます。
- 「**連絡先の検証エラー :: メールアドレスを解析できません**」は、提供された連絡先メールアドレスが無効であるか、解析できない場合に報告されます。
- 「**注文確定リクエストを処理できません。(無効なACMEディレクトリURLの場合)**」は、ACMEクライアントが注文を確定できない場合に報告されます。これは、多くの場合、無効または到達不能なACMEディレクトリURLが原因です。
- 「**DNSプロバイダー - TestDNSが存在しないか、アクティブではありません。**」は、指定されたDNSプロバイダーが見つからないか、システムで非アクティブである場合に報告されます。
- 「**設定CA IDが空であるか、存在しません。**」は、CA設定IDが不足しているか、既存の設定と一致しない場合に報告されます。

## ゼロタッチ証明書管理

NetScaler Consoleでは、ビルド**14.1-34.x**以降を実行している管理対象のNetScalerインスタンスで、ゼロタッチ証明書管理を構成できます。ゼロタッチ証明書管理を使用すると、手動による介入を排除し、アプリケーション要求に対応するためのインメモリゼロタッチ証明書ストアを構築できます。NetScaler Consoleにすべての証明書とキーをアップロードし、管理対象のNetScalerインスタンスで有効にするには、 **> >** に移動します。NetScalerは定期的に証明書リポジトリをポーリングし、必要に応じて必要な証明書を配信します。

ゼロタッチ証明書管理では、次のプロセスがNetScaler®によって自動的に実行されます。

- 証明書の追加、バインド、およびリンク
- 特定の順序で、またはまとめて証明書とキーを提供する
- 要求に基づいて適切な証明書をインストールして使用する
- 定期的なポーリングサイクル中に期限切れの証明書を削除する

NetScalerインスタンスでのゼロタッチ証明書の動作の詳細については、「NetScaler zero touch certificate management」を参照してください。

管理者として、NetScaler Consoleで次のことを確認する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScalerインスタンスがビルド14.1-34.x以降を実行しており、NetScaler Consoleで管理されていること。
- 証明書（任意の形式）とキーをアップロードします。次に、管理対象のNetScalerインスタンスでゼロタッチを有効にします。
- NetScaler Consoleに有効なCA証明書が存在することを確認します。更新されたConsole CA証明書がある場合は、管理対象のNetScalerインスタンスでゼロタッチを有効にする前に証明書をアップロードしてください。NetScaler ConsoleにCA証明書がない場合、次のエラーメッセージが表示されます。



### 証明書のアップロード

1. **インフラストラクチャ > SSLダッシュボード > ゼロタッチ証明書管理** に移動します。
2. **開始**をクリックします。

   開始](/en-us/netscaler-application-delivery-management-software/media/zero-touch-certificate.png)

3. ビルド14.1-34.x以降を実行しているNetScalerインスタンスが一覧表示されます。**ゼロタッチを構成**をクリックしてゼロタッチを有効にするか、**スキップ**をクリックして次のステップに進むことができます。
4. すべての証明書（.pem、.cer、.crtなど、任意の形式で構いません）をアップロードするには、**アップロード**をクリックします。

**注:**

- 証明書またはキーファイルは8192バイト未満である必要があります。
- 複数の証明書またはキーファイルをアップロードする場合、サポートされる最大サイズは50000バイトです。
- 証明書またはキーファイルがパスワードで保護されている場合は、パスワードを指定してください。パスワードが指定されていない場合、証明書またはキーファイルはアップロードされません。

### ゼロタッチ証明書管理を有効にする

証明書をアップロードした後、管理対象のNetScalerインスタンスでゼロタッチを有効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **ゼロタッチ証明書管理**ページから、**ゼロタッチを構成**をクリックします。

   構成](/en-us/netscaler-application-delivery-management-software/media/configure-zero-touch.png)

2. **インスタンスの追加**をクリックし、インスタンスを選択してから、**有効にする**をクリックします。

   ゼロタッチを有効にする](/en-us/netscaler-application-delivery-management-software/media/enable-zero-touch.png)

NetScaler Consoleは、デフォルトのポーリング間隔を使用して、NetScalerインスタンスからすべての証明書をポーリングします。**今すぐポーリング**オプションを使用して、すぐにポーリングできます。

**SSLダッシュボード**では、アクティブおよび非アクティブな証明書に関する詳細を示すゼロタッチ証明書の使用状況も表示できます。

SSLダッシュボードビュー(/en-us/netscaler-application-delivery-management-software/media/zero-touch-ssl-dashboard.png)

### SSLフィルターモードのサポート

NetScalerインスタンスは、特定のSSL証明書と秘密キーのメタデータをフェッチします。この最小特権アプローチにより、インスタンスは必要なアセットのみにアクセスし、1つのインスタンスの侵害が証明書インフラストラクチャ全体を公開するのを防ぎます。この機能は、複数の管理者が異なる目的でNetScalerインスタンスのグループを管理する環境で特に役立ちます。

利点の一部を以下に示します。

- **セキュリティセグメンテーション** - 攻撃対象領域を最小限に抑え、組織のセキュリティポリシーを遵守するために、NetScalerごとのレベルでメタデータアクセスを制限します。
- **合理化された管理者エクスペリエンス** - 管理者にNetScalerインスタンスのグループに関連するアセットのみを表示することで、マルチテナントまたは部門展開の複雑さを軽減します。
- **最適化されたリソース利用** - 必要なSSL証明書と秘密キーのメタデータのみをフェッチすることで、システムメモリの肥大化を防ぎます。

フィルターモード構成は、NetScalerインスタンスとSSLファイルが特定の同期タイプを介してどのように相互作用するかを定義します。これらの設定はNetScaler Consoleを通じて管理でき、各インスタンスが必要なメタデータのみをフェッチするようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| コンポーネント | 同期タイプ | 説明 |
| --- | --- | --- |
| NetScalerインスタンス | カスタム同期 | このモードのNetScalerインスタンスは、インスタンスに具体的にマッピングされた証明書とキーのメタデータのみをフェッチします。 |
| NetScalerインスタンス | グローバル同期 | このモードのNetScalerインスタンスは、アップロードされたすべての証明書と秘密鍵のメタデータをフェッチします。 |
| SSLファイル | カスタムファイル | これらのファイルは、カスタム同期モードのNetScalerインスタンスに具体的にマッピングされます。 |
| SSLファイル | グローバルファイル | これらのファイルのメタデータは、グローバル同期モードのすべてのNetScalerインスタンスによってフェッチされます。 |

### フィルターモード設定の構成

フィルターモードを構成するには、インスタンスとファイルの同期タイプを定義します。これにより、機密性の高いメタデータの安全かつ最適化された配布が保証されます。

SSLダッシュボードの**証明書ファイル**および**NetScalerインスタンス**セクションにあるアップロードボタンを使用して、証明書と秘密鍵を直接アップロードできます。

GUIを使用して構成するには：

1. **新しいファイルをアップロードする（初日）** - 新しいアセットを追加するには、**証明書ファイルとNetScalerインスタンス > アップロード**に移動します。

   次の同期タイプのいずれかを選択します。

   - **グローバル** - グローバル同期モードを使用し、アップロードを完了するには、これを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **カスタム** - カスタム同期モードを使用し、マッピングする特定のインスタンスを選択してからファイルをアップロードするには、これを選択します。

2. **既存ファイルを移動 (N日目)** - 証明書とキーをグローバル同期モードからカスタム同期モードに移行するには、ターゲットのNetScalerインスタンスを選択し、「**既存ファイルを追加**」をクリックします。
3. **ドメインを選択** - インスタンスが選択されたら、移行をトリガーする関連ドメインを選択します。NetScaler Consoleは、対応する証明書と秘密鍵ファイルを自動的に検出し、カスタム同期モードに移行します。
4. **アセットを表示** - ランディングページに移動して、カスタム同期モードで各NetScalerインスタンスにマッピングされているすべての証明書と秘密鍵ファイルを表示します。
5. **同期モードを切り替える** - インスタンスをグローバル同期モードに戻すには、ランディングページで「**グローバル同期に切り替える**」をクリックします。

## SSLダッシュボードを使用する

NetScaler ConsoleのSSL証明書ダッシュボードを使用すると、証明書発行者、キー強度、署名アルゴリズムを追跡するのに役立つグラフを表示できます。SSL証明書ダッシュボードには、次のことを示すグラフも表示されます。

- 証明書の有効期限が切れるまでの日数
- 使用済みおよび未使用の証明書の数
- 自己署名証明書とCA署名証明書の数
- 発行者の数
- 署名アルゴリズム
- SSLプロトコル
- 使用中の証明書の数による上位10インスタンス

### SSL証明書を監視するには

会社にSSLポリシーがあり、すべての証明書が最低2048ビットのキー強度を持ち、信頼できるCA機関によって承認される必要があるなど、特定のSSL証明書要件を定義している場合、NetScaler ConsoleのSSLダッシュボードを使用して証明書を監視できます。

別の例として、新しい証明書をアップロードしたが、仮想サーバーにバインドするのを忘れた場合が考えられます。SSLダッシュボードは、使用されているSSL証明書と使用されていないSSL証明書を強調表示します。**使用状況**セクションでは、インストールされている証明書の数と、使用さ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

れている証明書の数を確認できます。さらにグラフをクリックすると、証明書の名前、使用されているインスタンス、その有効性、署名アルゴリズムなどを確認できます。

NetScaler ConsoleでSSL証明書を監視するには、**インフラストラクチャ > SSLダッシュボード**に移動します。

SSLダッシュボードの画像(/en-us/netscaler-application-delivery-management-software/media/nmas-ssl-dashboard-1.png)

NetScaler Consoleでは、SSL証明書をポーリングし、インスタンスのすべてのSSL証明書をNetScaler Consoleに即座に追加できます。これを行うには、,

1. 「**Infrastructure > SSL Dashboard**」に移動します。
2. 「**Poll Now**」をクリックします。

   「**Poll Now**」ページで、管理対象のすべてのNetScalerインスタンスをポーリングするか、特定のインスタンスを選択できます。
3. 「**Start Polling**」をクリックします。

**SSL Dashboard**では、NetScaler SSL証明書、SSL仮想サーバー、およびSSLプロトコルを監視できます。

ダッシュボードのメトリックをクリックすると、SSL証明書、SSL仮想サーバー、またはSSLプロトコルに関連する詳細を表示できます。

たとえば、ダッシュボードの「**Self signed vs CA signed**」の下の数字をクリックすると、NetScaler Console GUIにNetScalerインスタンス上のすべてのSSL証明書が表示されます。

NetScalerインスタンス上のSSL証明書(/en-us/netscaler-application-delivery-management-software/media/nmas-ssl-dashboard-2.png)

NetScaler Console SSLダッシュボードには、仮想サーバーで実行されているSSLプロトコルの分布も表示されます。管理者は、SSLポリシーを通じて監視するプロトコルを指定できます。詳細については、「Configuring SSL Policies」を参照してください。サポートされているプロトコルは、SSLv2、SSLv3、TLS 1.0、TLS 1.1、TLS 1.2、およびTLS 1.3です。仮想サーバーで使用されているSSLプロトコルは、棒グラフ形式で表示されます。特定のプロトコルをクリックすると、そのプロトコルを使用している仮想サーバーのリストが表示されます。

SSLダッシュボードでDiffie-Hellman (DH) またはEphemeral RSAキーが有効または無効になると、ドーナツグラフが表示されます。これらのキーは、サーバー証明書がエクスポートクライアントをサポートしていない場合でも（1024ビット証明書の場合など）、エクスポートクライアント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

との安全な通信を可能にします。適切なグラフをクリックすると、DHまたはEphemeral RSAキーが有効になっている仮想サーバーのリストが表示されます。

### SSL証明書の監査証跡を表示するには

NetScaler ConsoleでSSL証明書のログの詳細を表示できるようになりました。ログの詳細には、NetScaler ConsoleでSSL証明書を使用して実行された操作（SSL証明書のインストール、SSL証明書のリンクとリンク解除、SSL証明書の更新、SSL証明書の削除など）が表示されます。監査証跡情報は、複数の所有者がいるアプリケーションで実行されたSSL証明書の変更を監視する際に役立ちます。

SSL証明書を使用してNetScaler Consoleで実行された特定の操作の監査ログを表示するには、**Infrastructure > SSL Dashboard** \> に移動し、**Audit Logs** をクリックします。

監査ログ(/en-us/netscaler-application-delivery-management-software/media/sslaudittrails.png)

SSL証明書を使用して実行された特定の操作について、そのステータス、開始時刻、終了時刻を表示できます。さらに、操作が実行されたインスタンスと、そのインスタンスで実行されたコマンドを表示できます。

「SSL監査証跡」(/en-us/netscaler-application-delivery-management-software/media/sslaudittrails1.png)

### SSLダッシュボードでSSL証明書を削除するには

NetScaler 14.1-38.x以降では、選択したSSL証明書の設定を削除する際に、NetScalerから関連するSSL証明書ファイルを削除するオプションが提供されます。SSL証明書を削除するには：

1. **Infrastructure > SSL Dashboard**に移動します。
2. SSL証明書の詳細が表示される**SSL Certificates**セクションで、**Unused**ラベルのリンクをクリックします。
3. 未使用の証明書の一覧が表示されたページが表示されます。
4. 削除したい未使用の証明書を1つ以上選択します。

   「SSL監査証跡」(/en-us/netscaler-application-delivery-management-software/media/unused-certificates.png)
5. **Delete**をクリックします。
6. **Confirm**ダイアログボックスが表示され、NetScaler®から証明書ファイルを削除するための以下のオプションが提供されます。

   - **Do Not Delete**: NetScalerからの証明書ファイルの削除をスキップします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Delete**: 期限切れおよび期限切れでない証明書の両方について、NetScalerから証明書ファイルを削除します。
- **Delete if Expired**: 期限切れの証明書のみについて、NetScalerから証明書ファイルを削除します。

> **注：**
>
> NetScaler 14.1-38.xより前のバージョンでは、3つのオプションすべてで証明書ファイルの削除はスキップされます。 設定とともに証明書ファイルを削除するオプションは、NetScaler 14.1-38.x以降にのみ適用されます。

7. ニーズに基づいて適切なオプションを選択します。
8. 証明書を削除するには**はい**をクリックし、変更せずにワークフローを終了するには**いいえ**をクリックします。

### SSLダッシュボードでデフォルトのNetScaler証明書を除外するには

NetScaler Consoleでは、設定に基づいて、SSLダッシュボードのグラフに表示されるデフォルトのNetScaler証明書を表示または非表示にできます。デフォルトでは、すべての証明書（デフォルトの証明書を含む）がSSLダッシュボードに表示されます。

SSLダッシュボードでデフォルトの証明書を表示または非表示にするには：

1. NetScaler Console GUIで、**Infrastructure > SSL Dashboard**に移動します。
2. **SSL Dashboard**ページで、**Settings**をクリックします。
3. **Settings**ページで、**General**を選択します。
4. 証明書の有効期限が切れる日数（証明書の有効期限に関する通知を受け取るため）を入力します。
5. 通知方法を選択し、それぞれのプロファイルを作成します。
6. **Certificate Filter**セクションで、**Show Default Certificates**チェックボックスをオフにし、**Save and Exit**をクリックします。

### SSLファイルの表示、アップロード、ダウンロード

NetScaler ConsoleでSSLファイルを表示するには、**Infrastructure > SSL Dashboard > SSL Files on NetScaler Console**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console で、次のファイルを閲覧、アップロード、ダウンロードできます。

- SSL証明書
- SSLキー
- SSL CSR

NetScalerインスタンス上のSSLファイルを表示およびダウンロードするには、**Infrastructure > SSL Dashboard > SSL Files on NetScaler** に移動します。

SSLファイルには、NetScalerインスタンスが手動またはスケジュールされたバックアッププロセスによってバックアップされた後にのみアクセスできます。

**重要:**

NetScalerインスタンスからのSSLファイルのダウンロードを有効にするには、**Instance SSL certificates** 機能を有効にします。詳細については、「NetScaler Console機能の有効化または無効化」を参照してください。

### SSL証明書チェーンの表示

中間証明書からルートCA証明書までの完全な証明書チェーンを表示できます。

証明書チェーンを表示するには:

1. **Infrastructure > SSL Dashboard** に移動し、いずれかのタイルでSSL証明書をクリックします。
2. **SSL Certificates** ページで、証明書を選択し、**Details** をクリックします。証明書チェーンは **Links** の下に表示されます。



## SSL証明書の有効期限切れ通知を設定する

セキュリティ管理者として、証明書の有効期限が近づいていることを通知し、どのCitrix NetScalerインスタンスがそれらの証明書を使用しているかに関する情報を含めるように通知を設定できます。通知を有効にすることで、SSL証明書を期限内に更新できます。

たとえば、証明書の有効期限が切れる30日前に、電子メール通知を電子メール配布リストに送信するように設定できます。

**NetScaler Consoleから通知を設定するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**インフラストラクチャ > SSLダッシュボード**に移動します。
2. **SSLダッシュボード**ページで、**設定**をクリックします。
3. **SSL設定**ページで、**編集**アイコンをクリックします。
4. **通知設定**セクションで、有効期限の何日前に通知を送信するかを指定します。
5. 送信する通知の種類を選択します。ドロップダウンメニューから通知の種類と配布リストを選択します。通知の種類は次のとおりです。

   - **電子メール** – メールサーバーとプロファイルの詳細を指定します。証明書の有効期限が近づくと、電子メールがトリガーされます。
   - **SMS** – ショートメッセージサービス（SMS）サーバーとプロファイルの詳細を指定します。証明書の有効期限が近づくと、SMSメッセージがトリガーされます。
   - **Slack** - Slackプロファイルの詳細を指定します。
   - **PagerDutyアラート** - PagerDutyプロファイルを指定します。PagerDutyポータルで設定された通知設定に基づいて、証明書の有効期限が近づくと通知が送信されます。
   - **ServiceNow** - 証明書の有効期限が近づくと、デフォルトのServiceNowプロファイルに通知が送信されます。

     **重要**

     Citrix Cloud ITSM AdapterがServiceNow用に構成され、NetScaler Consoleと統合されていることを確認してください。詳細については、「NetScaler ConsoleとServiceNowインスタンスの統合」(/ja-jp/netscaler-application-delivery-management-software/current-release/configure/integrate-itsm-adapter-netscaler-adm-servicenow.html)を参照してください。

     SSL証明書の有効期限切れに関する通知(/en-us/netscaler-application-delivery-management-software/media/030_eventnot.png)

6. **保存して終了**をクリックします。

NetScaler Consoleは、SSL証明書の有効期限が近づくと、外部トラップ宛先サーバーにSSL証明書有効期限切れトラップを送信するようになりました。NetScaler Consoleは、次の2つの条件が満たされたときにトラップを送信します。

- SSLダッシュボード設定ページで、証明書の有効期限が切れるまでの日数を設定していること。
- トラップ宛先を追加していること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**設定 > SNMP > トラップ宛先**に移動して、トラップ宛先を設定できます。トラップが送信される宛先SNMPサーバーのIPアドレスを入力します。ポート番号を入力し、コミュニティ文字列として「public」（引用符なし）と入力します。

## インストール済み証明書を更新する

証明機関 (CA) から更新された証明書を受け取った後、個々のNetScalerインスタンスにログインして証明書を更新する必要はありません。NetScaler Consoleでは、証明書ストアの証明書を使用して既存の証明書を更新できます。

NetScaler ConsoleからSSL証明書を更新するには：

1. NetScaler Consoleで、**Infrastructure > SSL Dashboard**に移動します。
2. いずれかのグラフをクリックして、SSL証明書のリストを表示します。
3. **SSL証明書**ページで、証明書を選択し、**更新**をクリックします。または、SSL証明書をクリックしてその詳細を表示し、**SSL証明書**ページの右上隅にある**更新**をクリックします。
4. **SSL証明書の更新**ページで、**証明書**を選択して**証明書ストア**ページを表示します。

   
5. **証明書ストア**ページで、追加する証明書ファイルを選択します。**選択**をクリックします。

   
6. 新しい証明書のドメイン名が古い証明書と一致しない場合、サーバーに新しいドメインをホストさせたい場合は、**ドメインチェックなし**を選択します。

   

   **OK**をクリックします。この証明書がバインドされているすべてのSSL仮想サーバーが自動的に更新されます。

   **注：**

   証明書ストアの証明書チェーンで既存のSSL証明書を更新すると、既存の証明書はリンクされた証明書で更新されます。証明書を選択し、**詳細**をクリックして証明書チェーンを表示します。

## NetScalerインスタンスにSSL証明書をインストールする

Citrix NetScalerインスタンスにSSL証明書をインストールする前に、証明書が信頼できるCAによって発行されていることを確認してください。また、証明書キーのキー強度を2048ビット以上とし、キーが安全な署名アルゴリズムで署名されていることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**別のNetScalerインスタンスからSSL証明書をインストールするには：**

NetScaler Console GUIから、選択したNetScalerインスタンスから証明書をインポートし、他のターゲットNetScalerインスタンスに適用することもできます。

1. **Infrastructure > SSL Dashboard** に移動します。
2. **Install Certificate** をクリックします。
3. **Install SSL Certificate on NetScaler Instances** ページで、次のパラメータを指定します。
   a. **証明書ソース Import from Instance** オプションを選択します。
      - 証明書をインポートする**インスタンス**を選択します。
      - インスタンス上のすべてのSSL証明書ファイルの一覧から**証明書**を選択します。
   b. **証明書の詳細**
      - **証明書名**。証明書キーの名前を指定します。
      - **パスワード**。秘密キーを暗号化するためのパスワード。このオプションを使用して、暗号化された秘密キーをアップロードできます。
4. 証明書をインストールするNetScalerインスタンスを選択するには、**Select Instances** をクリックします。
5. 今後の使用のために設定を保存するには、**Save Configuration** チェックボックスをオンにします。
6. 「**OK**」をクリックします。

   別のインスタンスからSSL証明書をインポートする(/en-us/netscaler-application-delivery-management-software/media/import-ssl-from-ns.png)

**NetScaler ConsoleからSSL証明書をインストールするには：**

1. NetScaler Consoleで、**インフラストラクチャ > SSLダッシュボード**に移動します。
2. 「**証明書のインストール**」をクリックします。
3. **NetScalerインスタンスへのSSL証明書のインストール**ページで、次のパラメータを指定します。
   a. **証明書ソース 証明書ストアからインポート**オプションを選択します。
      - **証明書ファイル - ローカル**（お使いのローカルマシン）または**アプライアンス**（証明書ファイルはNetScaler Console仮想インスタンスに存在する必要があります）のいずれかを選択して、SSL証明書ファイルをアップロードします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **証明書の詳細**

- **証明書名** – 証明書キーの名前を指定します。

4. 「**インスタンスの選択**」をクリックして、証明書をインストールするNetScaler Consoleインスタンスを選択します。
5. 今後の使用のために構成を保存するには、「**構成の保存**」チェックボックスをオンにします。
6. 「**OK**」をクリックします。

ConsoleからSSL証明書をインストールする(/en-us/netscaler-application-delivery-management-software/media/installsslcert.png)

## 証明書署名要求 (CSR) を作成する

証明書署名要求 (CSR) は、証明書が使用されるサーバーで生成される暗号化されたテキストのブロックです。これには、組織名、共通名 (ドメイン名)、地域、国など、証明書に含まれる情報が含まれています。

**NetScaler Console を使用して CSR を作成するには:**

1. NetScaler Console で、 **>** の順に移動します。
2. いずれかのグラフをクリックして、インストールされている SSL 証明書のリストを表示し、CSR を作成する証明書を選択して、 リストから を選択します。
3. ページで、CSR の名前を指定します。
4. 次のいずれかを実行します。

- **キーをアップロードする** - オプションを選択します。キーファイルをアップロードするには、 (ローカルマシン) または (キーファイルは NetScaler Console 仮想インスタンスに存在する必要があります) のいずれかを選択します。
- **キーを作成する** - オプションを選択し、次のパラメータを指定します。

| | |
|---|---|
| **暗号化アルゴリズム** | キーの種類。例: RSA。 |
| **キーファイル名** | RSA キーが保存されているファイルの名前。 |
| **キーサイズ** | キーサイズ (ビット単位)。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| **公開指数値** | 提供されたドロップダウンリストから**3**または**F4**を選択します。この値は、RSAキーの作成に必要な暗号アルゴリズムの一部です。 |
| **キー形式** | デフォルトではPEMが選択されています。PEMはSSL証明書に推奨されるキー形式です。 |
| **PEMエンコードアルゴリズム** | ドロップダウンリストから、生成されたRSAキーの暗号化に使用するアルゴリズム（**DES**または**DES3**）を選択します。このアルゴリズムを選択した場合、PEMパスフレーズを提供する必要があります。 |
| **PEMパスフレーズ** | PEMエンコードアルゴリズムを選択した場合は、パスフレーズを入力します。 |
| **PEMパスフレーズの確認** | PEMパスフレーズを確認します。 |

5. **続行**をクリックします。
6. 次のページで、詳細情報を提供します。

   ほとんどのフィールドには、選択した証明書のサブジェクトから抽出されたデフォルト値が設定されています。サブジェクトには、コモンネーム、組織名、都道府県、国などの詳細が含まれています。

   **サブジェクト代替名**フィールドでは、単一の証明書でドメイン名やIPアドレスなど、複数の値を指定できます。サブジェクト代替名は、単一の証明書で複数のドメインを保護するのに役立ちます。

   ドメイン名とIPアドレスを次の形式で指定します。

   ```
   DNS:<Domain name>, IP:<IP address>
   ```

   この例では、`10.0.0.1` と `www.example.com` を保護します。

   フィールドを確認し、**続行** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

ほとんどのCAは、電子メールによる証明書の提出を受け付けています。CAは、CSRを提出した電子メールアドレスに有効な証明書を返送します。

## SSL証明書をリンクおよびリンク解除する

複数の証明書をリンクすることで、証明書バンドルを作成します。ある証明書を別の証明書にリンクするには、最初の証明書の発行者が2番目の証明書のドメインと一致している必要があります。たとえば、証明書Aを証明書Bにリンクしたい場合、証明書Aの「発行者」は証明書Bの「ドメイン」と一致している必要があります。

**NetScaler Consoleを使用して、あるSSL証明書を別の証明書にリンクするには：**

1. NetScaler Consoleで、**Infrastructure > SSL Dashboard**に移動します。
2. いずれかのグラフをクリックして、SSL証明書のリストを表示します。
3. リンクしたい証明書を選択し、**Action**ドロップダウンリストから**Link**を選択します。
4. 一致する証明書のリストから、リンクしたい証明書を選択し、**OK**をクリックします。

**注**

一致する証明書が見つからない場合、次のメッセージが表示されます: リンクする証明書が見つかりません。

**NetScaler Consoleを使用してSSL証明書のリンクを解除するには：**

1. NetScaler Consoleで、**Infrastructure > SSL Dashboard**に移動します。
2. いずれかのグラフをクリックして、SSL証明書のリストを表示します。
3. リンクされている証明書のいずれかを選択し、**Action**ドロップダウンリストから**Unlink**を選択します。
4. **OK**をクリックします。

**注**

選択した証明書が別の証明書にリンクされていない場合、次のメッセージが表示されます: 証明書にはCAリンクがありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## エンタープライズポリシーの構成

NetScaler Consoleで、エンタープライズポリシーを構成し、すべての信頼できるCA、セキュアな署名アルゴリズムを追加し、証明書キーに推奨されるキー強度を選択できます。Citrix NetScalerインスタンスにインストールされている証明書のいずれかがエンタープライズポリシーに追加されていない場合、SSL証明書ダッシュボードには、それらの証明書の発行元が**推奨されません**と表示されます。

また、証明書キーの強度がエンタープライズポリシーで推奨されるキー強度と一致しない場合、SSL証明書ダッシュボードには、それらのキーの強度が**推奨されません**と表示されます。

**NetScaler Consoleでエンタープライズポリシーを構成するには：**

1. NetScaler Consoleで、**Infrastructure** \> **SSL Dashboard** に移動し、**Settings** をクリックします。
2. SSL Settingsページで、**Edit** アイコンをクリックして、すべての信頼できるCA、セキュアな署名アルゴリズムを追加し、証明書とキーに推奨されるキー強度を選択します。サポートされるキー強度は、512、1024、2048、3072、4096ビットです。
   - **推奨されるキー強度** - アルゴリズムのセキュリティとキーのビット数を示します。
   - **推奨される署名アルゴリズム** - アプリケーションに発行される署名付きトークンを示します。
   - **推奨される信頼できるCA** - デジタル証明書を発行する信頼できるエンティティを示します。**+** アイコンをクリックして、さらにエンティティを追加します。
   - **推奨されるSSLプロトコル** - TLS/SSLバージョンを示します。
3. **Save** をクリックして、エンタープライズポリシーを保存します。

> **注**
>
> SSLダッシュボードには、**Settings** オプションで選択された**署名アルゴリズム**のみが表示され、その他は**推奨されません**と表示されます。

## NetScalerインスタンスからSSL証明書をポーリングする

NetScaler Consoleは、NITROコールとSecure Copy (SCP) プロトコルを使用して、24時間ごとに1回、SSL証明書を自動的にポーリングします。Citrix NetScalerインスタンスに新しく追加されたSSL証明書を検出するために、SSL証明書を手動でポーリングすることもできます。すべての

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスのSSL証明書をポーリングすると、ネットワークに大きな負荷がかかります。

すべてのNetScalerインスタンスのSSL証明書をポーリングする代わりに、選択した1つまたは複数のインスタンスのSSL証明書のみを手動でポーリングできます。

**NetScalerインスタンスでSSL証明書をポーリングするには:**

1. NetScaler Consoleで、**インフラストラクチャ > SSLダッシュボード** に移動します。
2. **SSLダッシュボード** ページの右上隅にある **今すぐポーリング** をクリックします。

   SSL証明書をポーリングする(/en-us/netscaler-application-delivery-management-software/media/nmas-ssl-dashboard-1.png)
3. **今すぐポーリング** ページがポップアップ表示され、ネットワーク内のすべてのNetScalerインスタンスをポーリングするか、選択したインスタンスをポーリングするかのオプションが提供されます。

   a. すべてのNetScalerインスタンスのSSL証明書をポーリングするには、**すべてのインスタンス** タブを選択し、**ポーリング開始** をクリックします。

      ポーリング開始(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now-1.png)

   b. 特定のインスタンスをポーリングするには、**選択 インスタンス** タブを選択し、リストからインスタンスを選択して、**今すぐポーリング** をクリックします。

      特定のインスタンスをポーリングする(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now-2.png)

## NetScaler Console証明書ストアを使用してSSL証明書を管理する

NetScaler Console証明書ストアは、SSL証明書を一元的に保存および管理するのに役立ちます。保存された証明書は、後でNetScalerの設定を構成するために使用できます。

証明書ストアでは、SSL証明書の追加、更新、削除が可能です。また、証明書ストアを使用して、NetScalerインスタンスから証明書をインポートし、他のターゲットNetScalerインスタンスに適用することもできます。

### 証明書ストアにSSL証明書を追加する

1. **Infrastructure > SSL Dashboard** に移動し、リストから **Manage Certificate Store** を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書ストア (/en-us/netscaler-application-delivery-management-software/media/certstore-list.png)

2. **Add** をクリックします。
3. **Add Certificate** ページで、次の詳細を入力します。

   - **Certkey Name** - 証明書の名前を入力します。名前はASCII英数字、アンダースコア、ハイフン文字のみを使用し、30文字未満である必要があります。証明書作成後に名前を変更することはできません。
   - **Certificate File** - ローカルドライブを参照して証明書ファイルをアップロードします。
   - **Key File** - ローカルコンピューターからキーファイルをアップロードします。
   - **Password** - PEM形式の暗号化された秘密キーがある場合は、秘密キーの暗号化に使用されたパスフレーズを入力します。
   - **Add Certificate Chain** - 証明書チェーンに証明書を追加するには、このオプションを選択します。
   - **Certificate Chain** - ローカルドライブを参照して証明書ファイルをアップロードします。
   - **Create** をクリックします。

### 証明書ストア内のSSL証明書を更新する

1. **Infrastructure > SSL Dashboard** に移動し、リストから **Manage Certificate Store** を選択します。
2. 更新したい証明書を選択し、**Update** をクリックします。
3. **Update Certificate** ページで、次の詳細を入力します。

   - **Certkey Name** - 更新するために選択した証明書の名前が表示されます。
   - **Certificate File** - 証明書ファイルを更新するには、証明書ファイルをアップロードします。
   - **Key File** - キーファイルを更新するには、ローカルコンピューターからキーファイルをアップロードします。
   - **Password** - PEM形式で暗号化された秘密鍵がある場合は、秘密鍵の暗号化に使用されたパスフレーズを入力します。
   - **Add Certificate Chain** - 証明書チェーンに証明書を追加するには、このオプションを選択します。
   - **Certificate Chain** - ローカルドライブを参照して証明書ファイルをアップロードします。
   - **OK** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 証明書ストアからSSL証明書を削除する

1. **Infrastructure > SSL Dashboard** に移動し、リストから **Manage Certificate Store** を選択します。
2. 証明書を選択し、**Delete** をクリックします。
3. プロンプトが表示されたら、証明書を削除するために **Yes** をクリックします。

### NetScaler® インスタンスにSSL証明書をインストールする

1. **Infrastructure > SSL Dashboard** に移動し、リストから **Manage Certificate Store** を選択します。
2. 証明書を選択し、**Install** をクリックします。
3. **Install SSL Certificate on NetScaler Instances** ページで、次の詳細を入力します。

   a. **証明書ソース**

   - **証明書** - 選択した証明書の名前が表示されます。

   b. **証明書の詳細**

   - **証明書名** - 証明書の名前が表示されます。
   - **構成を保存** - NetScaler の構成を保存するには、このオプションを選択します。証明書のインストール後に NetScaler の構成が保存されます。

4. **Select Instances** をクリックして、証明書をインストールする NetScaler インスタンスを選択します。

**OK** をクリックします。

### NetScaler インスタンスから証明書をインポートする

1. **Infrastructure > SSL Dashboard** に移動し、リストから **Manage Certificate Store** を選択します。
2. **Import NetScaler Certificates** をクリックします。
3. **Import NetScaler Certificates** ページで、次のいずれかのタブを選択できます。

   - **NetScaler証明書のインポート** - **ポーリング開始**をクリックして、すべてのNetScalerインスタンス上のすべてのSSL証明書をポーリングします。
   - **インスタンスの選択** - NetScalerインスタンスを選択し、**NetScaler証明書のインポート**をクリックして、選択したNetScalerインスタンスのみのSSL証明書をポーリングします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポーリング後、SSL証明書とキーファイルがダウンロードされ、証明書ストアに追加されます。

**注:**

ストアに同一の証明書名が存在する場合、証明書のインポート操作は失敗します。ただし、インポート操作は残りの証明書のポーリングを続行し、利用可能な場合はNetScaler証明書をストアに追加します。

## 中間アップロードなしでサーバー証明書を更新する

中間証明書を繰り返し再アップロードする手間をかけずに、証明書を更新できます。この機能強化により、手作業の負担が軽減され、構成エラーのリスクが最小限に抑えられます。

### 簡単な更新

NetScaler Consoleは、デフォルトで更新中に既存の証明書チェーンを保持します。これにより、新しいサーバーレベル証明書のみをアップロードした場合でも、チェーンは破損せず有効な状態を保ちます。

### 主な改善点

- **複雑さの軽減** - 標準的なサーバー証明書の更新時における必須の中間アップロードを排除します。
- **安全第一** - 自動チェーン保持により、「チェーンの破損」（SSLハンドシェイクエラーの一般的な原因）が防止されます。

### 中間アップロードなしでサーバー証明書を更新するには

1. **インフラストラクチャ > SSLダッシュボード > 証明書ストア**に移動します。
2. 更新する証明書を選択し、**更新**をクリックします。
3. **既存の証明書チェーンを上書き** - 更新で中間チェーンの変更が必要な場合は、このオプションを選択します。
    - **バンドルあり** - 既存のチェーンを新しくアップロードされたバンドルに置き換えます。
    - **バンドルなし** - 現在の証明書チェーンを完全に削除します。
4. **証明書チェーンを追加** - プライマリサーバー証明書ファイルに中間証明書が含まれていない場合は、このオプションを選択して手動でアップロードし、追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 例

最終的な証明書構造は、既存の証明書チェーンのステータスと、更新中に選択するオプションによって異なります。

#### シナリオ A: 既存の証明書にチェーンがない場合

| 更新アクション | 結果 |
| --- | --- |
| 新しくアップロードされた証明書にチェーンが含まれていない | サーバー証明書が更新されます。中間チェーンは追加されません。 |
| 新しくアップロードされた証明書にチェーンが含まれている | サーバー証明書が更新され、新しい中間チェーンがアタッチされます。 |

#### シナリオ B: 既存の証明書にチェーンがある場合

| 更新アクション | 結果 |
| --- | --- |
| 新しくアップロードされた証明書にチェーンが含まれている（既存の証明書チェーンを上書きが有効になっている場合） | サーバー証明書が更新され、既存の中間チェーンが新しいチェーンに置き換えられます。 |
| 新しくアップロードされた証明書にチェーンが含まれていない（既存の証明書チェーンを上書きが有効になっている場合） | サーバー証明書が更新され、既存の中間チェーンが明示的に削除されます。 |

## 高可用性展開におけるデータベースのカスタム証明書と暗号の管理

NetScaler Consoleでは、デフォルトで組み込まれているデータベース証明書を、信頼できる認証局からの独自の証明書に置き換えることができます。また、NetScaler Consoleデータベースで独自の暗号スイートを構成することもできます。この機能により、証明書管理のニーズに対してより高い柔軟性とセキュリティが提供され、信頼できるSSL証明書を使用してHAノード間のすべての通信が保護されます。

### NetScaler Consoleにデータベース証明書をインストールする

HAセットアップで証明書をインストールするには：

1. **Settings > HA Deployment** に移動し、**Database Certificates** をクリックします。
2. **Installed Certificate** タブをクリックし、**Install New Certificate** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Install Database Certificate on Application Delivery Management** ページで、ルート証明書、サーバー証明書、およびサーバーキーをアップロードします。次のいずれかの操作を実行できます。
   - ローカルマシンから証明書またはキーファイルをアップロードするには、**Choose File > Local** を選択します。
   - NetScaler Consoleに存在する証明書またはキーファイルをアップロードするには、**Choose File > Appliance** を選択します。
4. **Install** をクリックします。

データベース証明書をインストールする(/en-us/netscaler-application-delivery-management-software/media/ha-install-db-certs.png)

**注：**

複数のチェーン証明書がある場合は、それらを単一のファイルに結合する必要があります。中間証明書が最初に来て、その後にルート証明書が続くように、連結の順序が正しいことを確認してください。この順序は、証明書チェーンが正しく認識されるために不可欠です。

たとえば、次のコマンドは、各証明書ファイル（intermediate_certificate1.crt、intermediate_certificate2.crt、およびroot_certificate.crt）の内容をcombined_certs.crtという名前のファイルに追加します。

```
cat intermediate_certificate1.crt >> combined_certs.crt
cat intermediate_certificate2.crt >> combined_certs.crt
cat root_certificate.crt >> combined_certs.crt
```

### インストールされているデータベース証明書を管理する

インストールされている証明書を表示、ダウンロード、および削除するには：

1. **Settings > HA Deployment** に移動し、**Database Certificates** をクリックします。
2. **Certificate Files** タブをクリックし、**Root Certificates, Server Certificates**、または **Server Keys** を選択して、対応するファイルを表示します。
3. ファイルをローカルマシンにダウンロードするには、**Download** をクリックします。
4. 証明書ファイルを削除するには、ファイルを選択し、**Delete** をクリックします。表示される確認ダイアログボックスで、**OK** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### データベースの暗号スイートを構成する

HA展開の暗号スイートを構成するには：

1. **Settings > HA Deployment** に移動し、**Database Certificates** をクリックします。
2. **Ciphers** タブをクリックし、次に **Configure Cipher** をクリックします。
3. **Configure Cipher Suites** ページで、利用可能な暗号のリストから1つ以上の暗号を選択します。
4. **Configure** をクリックします。表示される確認ダイアログボックスで、暗号設定を変更するには **Yes** をクリックします。

暗号を設定(/en-us/netscaler-application-delivery-management-software/media/ha-configure-ciphers.png)

**注：**

暗号設定を変更すると、NetScaler Console のセカンダリノードとディザスタリカバリノードが再起動します。

# イベント

Citrix NetScalerインスタンスのIPアドレスがNetScaler Consoleに追加されると、NetScaler ConsoleはNITROコールを送信し、インスタンスがそのトラップまたはイベントを受信するためのトラップ宛先として自身を暗黙的に追加します。

イベントは、管理対象のNetScalerインスタンスで発生したイベントまたはエラーを表します。たとえば、システム障害や構成の変更があった場合、イベントが生成され、NetScaler Consoleサーバーに記録されます。NetScaler Consoleで受信したイベントは、イベント概要ページ (**インフラストラクチャ > イベント**) に表示され、すべてのアクティブなイベントはイベントメッセージページ (**インフラストラクチャ > イベント > イベントメッセージ**) に表示されます。

NetScaler Consoleは、インスタンスで生成されたイベントをチェックして、さまざまな重大度レベルのアラームを形成します。これらのアラームはメッセージとして表示され、その一部は即座の注意が必要となる場合があります。たとえば、システム障害は「重大」なイベント重大度として分類され、直ちに対処する必要があります。

特定のイベントを監視するためのルールを設定できます。ルールを使用すると、NetScalerインフラストラクチャ全体で生成される多数のイベントを簡単に監視できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

特定の条件を持つルールを設定し、そのルールにアクションを割り当てることで、一連のイベントをフィルタリングできます。生成されたイベントがルールのフィルター条件を満たすと、そのルールに関連付けられたアクションが実行されます。フィルターを作成できる条件は、重大度、NetScalerインスタンス、カテゴリ、障害オブジェクト、構成コマンド、およびメッセージです。

イベントがクリアされるまで、特定の時間間隔でイベントに対して複数の通知がトリガーされるようにすることもできます。追加の対策として、特定の件名とユーザーメッセージでメールをカスタマイズし、添付ファイルをアップロードできます。

## イベントダッシュボードを使用する

ネットワーク管理者として、NetScalerインスタンスでの構成変更、ログイン状況、ハードウェア障害、しきい値違反、エンティティ状態の変更などの詳細、および特定のインスタンスでのイベントとその重大度を表示できます。すべてのNetScalerインスタンスで生成された重大なイベントの重大度に関するレポートを表示するには、NetScaler Consoleのイベントダッシュボードを使用できます。

**イベントダッシュボードで詳細を表示するには：**

**Infrastructure > Events > Reports** に移動します。

ダッシュボードの「上位10デバイス」グラフには、生成されたイベント数による上位10インスタンスのレポートが表示されます。グラフ上のインスタンスをクリックすると、イベントの重大度の詳細を表示できます。

NetScalerインスタンスタイプ（**Infrastructure > Events > Reports** \> **NetScaler/ NetScaler SDX** ）に移動すると、以下の詳細を表示できます。

- ハードウェア障害による上位10デバイス
- 構成変更による上位10デバイス
- 認証失敗による上位10デバイス
- エンティティ状態の変更による上位10デバイス
- しきい値違反による上位10デバイス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## イベントのイベント期間を設定する

イベント期間オプションを設定して、時間間隔（秒単位）を指定できます。NetScaler Console は、設定された期間までアプライアンスを監視し、イベント期間が設定された期間を超過した場合にのみイベントを生成します。

注:

> イベント期間の最小値は60秒です。**イベント期間**フィールドを空白のままにした場合、イベント発生直後にイベントルールが適用されます。

例えば、さまざまなNetScalerアプライアンスを管理し、仮想サーバーのいずれかが60秒以上ダウンした場合にメールで通知を受け取りたいとします。必要なフィルターを使用してイベントルールを作成し、ルールのイベント期間を60秒に設定できます。その後、仮想サーバーが60秒以上ダウンしたままになると、エンティティ名、ステータス変更、時間などの詳細を含むメール通知が届きます。

**NetScaler Console でイベント期間を設定するには:**

1. NetScaler Console で、**Infrastructure > Events > Rules** に移動し、**Add** をクリックします。
2. **Create Rule** ページで、ルールパラメータを設定します。
3. イベント期間を秒単位で指定します。

   イベント期間を設定する際は、**Category** セクションで関連するすべてのトラップを設定し、**Severity** セクションでそれぞれの重要度も設定してください。前の例では、`entityup`、`entitydown`、および `entityofs` のトラップを選択します。

## イベントフィルターをスケジュールする

ルール用のフィルターを作成した後、生成されたイベントがフィルター条件を満たすたびにNetScaler Consoleサーバーが通知を送信するのを望まない場合、フィルターを毎日、毎週、毎月などの特定の時間間隔でのみトリガーするようにスケジュールできます。

たとえば、インスタンス上の異なるアプリケーションに対して異なる時間にシステムメンテナンスアクティビティをスケジュールしている場合、インスタンスは複数のアラームを生成する可能性があります。

これらのアラームに対してフィルターを設定し、これらのフィルターの電子メール通知を有効にしている場合、NetScaler Consoleがこれらのトラップを受信すると、サーバーは多数の電子メー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ル通知を送信します。サーバーがこれらの電子メール通知を特定の期間のみ送信するようにしたい場合は、フィルターをスケジュールすることでそれが可能です。

**NetScaler Consoleを使用してフィルターをスケジュールするには：**

1. NetScaler Consoleで、**Infrastructure > Events > Rules** に移動します。
2. フィルターをスケジュールしたいルールを選択し、**View Schedule** をクリックします。
3. **Scheduled Rule** ページで、**Schedule** をクリックし、次のパラメーターを指定します。
    - **Enable Rule** – スケジュールされたイベントルールを有効にするには、このチェックボックスを選択します。
    - **Recurrence** - ルールをスケジュールする間隔。特定の曜日または月の特定の日付のいずれかを選択します。
    - **Days**: ルールを実行する曜日を選択します。複数の曜日を選択できます。
    - **Dates**: 日付を入力します。複数の日付をコンマ区切りの値として入力できます。
    - **Scheduled Time Interval (Hours)** – ルールをスケジュールする時間（24時間形式を使用）。
4. **Schedule** をクリックします。

## イベントのメール通知を繰り返し設定する

すべての重要なイベントが対処され、重要なメール通知が見逃されないようにするため、選択した条件を満たすイベントルールに対して、繰り返しメール通知を送信するように選択できます。たとえば、ディスク障害を伴うインスタンスのイベントルールを作成し、問題が解決されるまで通知を受け取りたい場合、それらのイベントに関する繰り返しメール通知を受け取るように選択できます。

これらのメール通知は、受信者が通知を確認したことを承認するか、イベントルールがクリアされるまで、事前定義された間隔で繰り返し送信されます。

**注**

イベントは、同等の「クリア」トラップが設定され、NetScalerインスタンスから送信された場合にのみ自動的にクリアできます。

イベントを手動でクリアするには、次の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Infrastructure > Events > Event Summary** に移動し、**Category** を選択してカテゴリ内のイベントを選択し、**Clear** をクリックします。
- または、**Infrastructure > Events > Event Messages** に移動します。インスタンスタイプを選択し、下のグリッドからイベントを選択して、**Clear** をクリックします。

**NetScaler Console から繰り返しメール通知を設定するには：**

1. NetScaler Console で、**Infrastructure > Events > Rules** に移動し、**Add** をクリックしてルールを作成します。
2. **Create Rule** ページで、ルールパラメーターを設定します。
3. **Event Rule** Actions で、**Add Action** をクリックします。次に、**Action Type** ドロップダウンリストから **Send e-mail Action** を選択し、**Email Distribution List** を選択します。
4. また、受信イベントが設定されたルールと一致した場合に、カスタマイズされた件名とユーザーメッセージを追加し、メールに添付ファイルをアップロードすることもできます。
5. **Repeat Email Notification until the event is cleared** チェックボックスをオンにします。



## イベントを抑制する

イベントアクションとして**抑制アクション**を選択すると、イベントが抑制またはドロップされる期間を分単位で設定できます。イベントは最低1分間抑制できます。

注:

> 抑制時間を0分に設定することもでき、これは無限の時間を意味します。時間期間を指定しない場合、NetScaler Consoleは抑制時間をゼロとみなし、期限切れになることはありません。

**NetScaler Consoleを使用してイベントを抑制するには:**

1. NetScaler Consoleで、**インフラストラクチャ > イベント > ルール**に移動します。**追加**をクリックします。
2. ルールを作成するために必要なすべてのパラメータを指定します。
3. **イベントルールアクション**で、**アクションの追加**をクリックして、イベントの通知アクションを割り当てます。
4. **イベントアクションの追加**ページで、**アクションタイプ**ドロップダウンリストから**抑制アクション**を選択し、イベントを抑制する期間を分単位で指定します。
5. **OK**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イベントを抑制する(/en-us/netscaler-application-delivery-management-software/media/createer11.png)

## イベントルールを作成する

特定のイベントを監視するためのルールを設定できます。ルールを使用すると、インフラストラクチャ全体で生成される多数のイベントを簡単に監視できます。

特定の条件でルールを設定し、ルールにアクションを割り当てることで、一連のイベントをフィルタリングできます。生成されたイベントがルールのフィルタ条件を満たすと、ルールに関連付けられたアクションが実行されます。フィルタを作成できる条件は、重大度、Citrix Application Delivery Controller (NetScaler) インスタンス、カテゴリ、障害オブジェクト、構成コマンド、およびメッセージです。

イベントには次のアクションを割り当てることができます。

- **電子メール送信アクション**: フィルタ条件に一致するイベントに対して電子メールを送信します。
- **トラップ送信アクション**: SNMPトラップを外部トラップ宛先に送信または転送します。
- **コマンド実行アクション**: 受信イベントが設定されたルールを満たした場合にコマンドを実行します。
- **ジョブ実行アクション**: 指定したフィルタ条件に一致するイベントに対してジョブを実行します。
- **抑制アクション**: 特定の期間、イベントのドロップを抑制します。
- **Slack通知の送信**: フィルタ条件に一致するイベントについて、設定されたSlackチャネルに通知を送信します。
- **PagerDuty通知の送信**: フィルタ条件に一致するイベントについて、PagerDutyの設定に基づいてイベント通知を送信します。
- **ServiceNow通知の送信**: フィルタ条件に一致するイベントについて、ServiceNowインシデントを自動生成します。

詳細については、「イベントルールアクションの追加」を参照してください。

イベントがクリアされるまで、指定された間隔で通知を再送信することもできます。また、特定の件名、ユーザーメッセージ、添付ファイルを使用して電子メールをカスタマイズすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、管理者として、特定のNetScalerインスタンスで「CPU使用率が高い」イベントがインスタンスの停止につながる可能性がある場合、それらのイベントを監視したいと考えるかもしれません。次のことができます。

- インスタンスを監視するルールを作成し、「CPU使用率が高い」カテゴリのイベントが発生したときにメール通知を送信するアクションを指定します。
- イベントが生成されるたびに通知されないように、ルールを特定の時間（午前11時から午後11時までなど）に実行するようにスケジュールします。

イベントルールを設定するには、次のタスクが含まれます。

1. ルールを定義する(#step-1---define-an-event-rule)
2. ルールが検出するイベントの重大度を選択する(#step-2---choose-the-severity-of-the-event)
3. イベントのカテゴリを指定する(#step-3---specify-the-event-category)
4. ルールが適用されるNetScalerインスタンスを指定する(#step-4---specify-citrix-adc-instances)
5. 障害オブジェクトを選択する(#step-5---select-failure-objects)
6. 詳細フィルターを指定する(#step-6---specify-advanced-filters)
7. ルールがイベントを検出したときに実行するアクションを指定する(#step-7---add-event-rule-actions)

### ステップ1 - イベントルールを定義する

**Infrastructure > Events > Rules** に移動し、**Add** をクリックします。ルールを有効にする場合は、**Enable Rule** チェックボックスをオンにします。

**Event Age** オプションを設定して、NetScaler Console がイベントルールを更新するまでの時間間隔（秒単位）を指定できます。

注:

> イベント期間の最小値は60秒です。**イベント期間**フィールドを空白のままにすると、イベント発生直後にイベントルールが適用されます。

上記の例に基づくと、NetScalerインスタンスで60秒以上の「CPU使用率が高い」イベントが発生するたびに、電子メールで通知を受け取りたい場合があります。イベント期間を60秒に設定すると、NetScalerインスタンスで60秒以上の「CPU使用率が高い」イベントが発生するたびに、イベントの詳細が記載された電子メール通知が届きます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleがイベントを受信するNetScalerインスタンスを追跡するために、**インスタンスファミリー**でイベントルールをフィルタリングすることもできます。

アスタリスク (*) パターンマッチング以外の正規表現を含める場合は、**正規表現マッチングによる高度なフィルターを有効にする**を選択します。

### ステップ2 - イベントの重大度を選択する

デフォルトの重大度設定を使用するイベントルールを作成できます。重大度は、イベントルールを追加したいイベントの現在の重大度を指定します。

次の重大度レベルを定義できます: 重大、メジャー、マイナー、警告、クリア、情報。



**注**

一般的なイベントと高度なイベントの両方で重大度を設定できます。NetScaler Consoleで管理されているNetScalerインスタンスのイベント重大度を変更するには、**インフラストラクチャ > イベント > イベント設定**に移動します。イベント重大度を設定したい**カテゴリ**を選択し、**重大度の設定**をクリックします。新しい重大度レベルを割り当てて、**OK**をクリックします。

### ステップ3 - イベントカテゴリを指定する

NetScalerインスタンスによって生成されるイベントのカテゴリを指定できます。すべてのカテゴリはNetScalerインスタンスで作成されます。これらのカテゴリは、イベントルールを定義するために使用できるNetScaler Consoleにマッピングされます。考慮したいカテゴリを選択し、**利用可能**テーブルから**設定済み**テーブルに移動します。

上記の例では、表示されたテーブルからイベントカテゴリとして「cpuUsageHigh」を選択する必要があります。



### ステップ 4 - NetScalerインスタンスの指定

イベントルールを定義するNetScalerインスタンスのIPアドレスを選択します。**インスタンス**セクションで、**インスタンスの選択**をクリックします。**インスタンスの選択**ページで、インスタンスを選択し、**選択**をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ステップ 5 - 障害オブジェクトの選択

提供されたリストから障害オブジェクトを選択するか、イベントが生成された障害オブジェクトを追加できます。正規表現を指定して障害オブジェクトを追加することもできます。指定された正規表現に応じて、障害オブジェクトは自動的にリストに追加されます。障害オブジェクトとは、イベントが生成されたエンティティインスタンスまたはカウンターです。

**重要**

正規表現を使用して障害オブジェクトを一覧表示するには、ステップ 1で**正規表現マッチングによる詳細フィルターを有効にする**を選択します。

障害オブジェクトは、イベントの処理方法に影響を与え、通知された正確な問題を反映するようにします。このフィルターを使用すると、障害オブジェクトに関する問題を迅速に追跡し、問題の原因を特定できます。たとえば、ユーザーがログインの問題を抱えている場合、ここでの障害オブジェクトは、`nsroot`のようなユーザー名またはパスワードです。

このリストには、すべてのしきい値関連イベントのカウンター名、すべてのエンティティ関連イベントのエンティティ名、証明書関連イベントの証明書名などが含まれます。



### ステップ 6 - 詳細フィルターの指定

イベントルールは、次の方法でさらにフィルターできます。

- **構成コマンド** - 完全な構成コマンドを指定するか、正規表現を指定してイベントをフィルターできます。

  コマンドの認証ステータスや実行ステータスによって、イベントルールをさらにフィルターできます。たとえば、`NetscalerConfigChange event`の場合は、`[.]*bind system global policy_name[.]*`と入力します。

  

- **メッセージ** - 完全なメッセージ記述を指定するか、イベントをフィルタリングするための正規表現を指定できます。たとえば、`NetscalerConfigChange`イベントの場合は、`[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress : \^([.]*10.122.132.142[.]*)`と入力します。

  詳細メッセージフィルター(/en-us/netscaler-application-delivery-management-software/media/advance-filters-messages.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ステップ7 - イベントルールアクションの追加

イベントの通知アクションを割り当てるために、イベントルールアクションを追加できます。これらの通知は、イベントが上記で設定した定義済みフィルター条件を満たした場合に送信または実行されます。次のイベントアクションを追加できます。

- メール送信アクション
- トラップ送信アクション
- コマンド実行アクション
- ジョブ実行アクション
- 抑制アクション
- Slack通知の送信
- PagerDuty通知の送信
- ServiceNow通知の送信

#### メールイベントルールアクションを設定するには

「メール送信アクション」イベントアクションタイプを選択すると、イベントが定義されたフィルター条件を満たしたときにメールがトリガーされます。メールサーバーまたはメールプロファイルの詳細を提供してメール配布リストを作成するか、以前に作成したメール配布リストを選択する必要があります。

NetScaler Consoleで多数の仮想サーバーが構成されているため、毎日大量のメールを受信する可能性があります。メールには、イベントの重大度、イベントのカテゴリ、および障害オブジェクトに関する情報を提供するデフォルトの件名行があります。しかし、件名行には、これらのイベントが発生した仮想サーバーの名前に関する情報は含まれていません。影響を受けるエンティティの名前、障害オブジェクトの名前など、追加情報を含めるオプションが利用できるようになりました。

カスタマイズされた件名とユーザーメッセージを追加し、受信イベントが設定されたルールと一致した場合に、メールに添付ファイルをアップロードすることもできます。

イベント通知のメールを送信する際、設定が正しく機能するかどうかを確認するためにテストメールを送信したい場合があります。「テスト」ボタンを使用すると、メールサーバー、関連する配信リスト、およびその他の設定を構成した後でテストメールを送信できます。この機能により、設定が正常に機能していることを確認できます。

また、選択した条件を満たすイベントルールに対して繰り返しメール通知を送信するために、「**イベントがクリアされるまでメール通知を繰り返す**」チェックボックスを選択することで、すべての重要なイベントが処理され、重要なメール通知が見逃されないようにすることもできます。た

© 1997–2026 Citrix Systems, Inc. All rights reserved.

とえば、ディスク障害を含むインスタンスのイベントルールを作成し、問題が解決するまで通知を受け取りたい場合、それらのイベントに関する繰り返しメール通知を受け取ることを選択できます。

メールイベントルールアクションの設定(/en-us/netscaler-application-delivery-management-software/media/event-rules-send-mails-action.png)

**トラップイベントルールアクションを設定するには**

**トラップ送信アクション**イベントアクションタイプを選択すると、SNMPトラップが外部トラップ宛先に送信または転送されます。トラップ配信リスト（またはトラップ宛先とトラッププロファイルの詳細）を定義することで、イベントが定義されたフィルター条件を満たした場合に、トラップメッセージが特定のトラップリスナーに送信されます。

**コマンド実行アクションを設定するには**

**コマンド実行アクション**イベントアクションを選択すると、特定のフィルター条件に一致するイベントに対してNetScaler Consoleで実行できるコマンドまたはスクリプトを作成できます。

**コマンド実行アクション**スクリプトに対して、以下のパラメーターを設定することもできます。

| パラメーター | 説明 |
| --- | --- |
| $ソース | このパラメーターは、受信したイベントの送信元IPアドレスに対応します。 |
| $カテゴリ | このパラメーターは、フィルターのカテゴリで定義されたトラップのタイプに対応します。 |
| エンティティ | このパラメーターは、イベントが生成されたエンティティインスタンスまたはカウンターに対応します。これには、すべてのしきい値関連イベントのカウンター名、すべてのエンティティ関連イベントのエンティティ名、およびすべての証明書関連イベントの証明書名を含めることができます。 |
| 重大度 | このパラメーターは、イベントの重大度に対応します。 |
| $失敗オブジェクト | 障害オブジェクトは、イベントの処理方法に影響を与え、通知されたとおりに障害オブジェクトが正確な問題を反映するようにしま |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| | |
|---|---|
| | す。これは、単に生のイベントを報告するのではなく、問題を迅速に追跡し、障害の原因を特定するために使用できます。 |

**注**

コマンド実行中、これらのパラメーターは実際の値に置き換えられます。

たとえば、負荷分散仮想サーバーのステータスが**ダウン**したときに、実行コマンドアクションを設定したいとします。管理者として、別の仮想サーバーを追加することで、迅速な回避策を提供することを検討するかもしれません。NetScaler Consoleでは、次のことができます。

- スクリプト (.sh) ファイルを作成します。

  以下はスクリプト (.sh) ファイルの例です。

```
#!/bin/sh

source=$1

failureobj=$2

payload='{"params":{"warning":"YES"},"lbvserver":
{"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"
80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog
":"ENABLED","

bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":""}}'

url="http://$source/nitro/v1/config/lbvserver"

curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/
json" -X POST -d $payload $url
```

- NetScalerエージェント上の永続的な場所に.shファイルを保存します。例: `/var`。
- ルール条件が満たされたときに実行されるように、NetScaler Consoleで.shファイルの場所を指定します。

新しい仮想サーバーを作成するための**コマンド実行**アクションを設定するには:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ルールを定義する
2. イベントの重大度を選択します。
3. イベントカテゴリ「**entitydown**」を選択します。
4. 仮想サーバーが構成されているインスタンスを選択します。
5. 仮想サーバーの障害オブジェクトを選択または作成します。
6. 「**イベントルールアクション**」で、「**アクションの追加**」をクリックし、「**アクションタイプ**」リストから「**コマンドアクションの実行**」を選択します。
7. 「**コマンド実行リスト**」で、「**追加**」をクリックします。

   コマンド配布リストの作成ページが表示されます。

   a. 「**プロファイル名**」に任意の名前を指定します。

   b. 「**コマンドの実行**」で、スクリプトを実行する必要があるNetScalerエージェントの場所を指定します。例: `/sh/var/demo.sh $source $failureobj`。

   c. 「**出力の追加**」と「**エラーの追加**」を選択します。

   > **注**
   >
   > コマンドスクリプトを実行したときに生成された出力とエラー（存在する場合）をNetScaler Consoleサーバーのログファイルに保存する場合は、「**出力の追加**」と「**エラーの追加**」オプションを有効にできます。これらのオプションを有効にしない場合、NetScaler Consoleはコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

   d. 「**作成**」をクリックします。

8. 「**イベントアクションの追加**」ページで、「**OK**」をクリックします。

> **注**
>
> NetScaler Consoleサーバーのログファイルにコマンドスクリプトを実行したときに生成された出力とエラー（もしあれば）を保存したい場合は、「**出力の追加**」と「**エラーの追加**」オプションを有効にできます。これらのオプションを有効にしない場合、NetScaler Consoleはコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### `Execute` ジョブアクションを設定するには

構成ジョブを含むプロファイルを作成することで、指定したフィルター条件に一致するイベントおよびアラームに対して、NetScalerおよびNetScaler SDXインスタンスの組み込みジョブまたはカスタムジョブとしてジョブが実行されます。

1. 「**イベントルールアクション**」の下で、「**アクションの追加**」をクリックし、「**アクションタイプ**」ドロップダウンリストから「**ジョブアクションの実行**」を選択します。
2. イベントが定義されたフィルター条件を満たしたときに実行したいジョブを含むプロファイルを作成します。
3. ジョブの作成中に、プロファイル名、インスタンスタイプ、構成テンプレート、およびジョブのコマンドが失敗した場合に実行したいアクションを指定します。
4. 選択したインスタンスタイプと選択した構成テンプレートに基づいて、変数の値を指定し、「**完了**」をクリックしてジョブを作成します。

### サプレスアクションを設定するには

「**サプレスアクション**」イベントアクションを選択すると、イベントが抑制または破棄される期間を分単位で設定できます。イベントは最低1分間抑制できます。

### NetScaler ConsoleからSlack通知を設定するには

NetScaler Console GUIでプロファイル名とWebhook URLを指定して、必要なSlackチャネルを設定します。イベント通知はこのチャネルに送信されます。これらの通知を受信するために複数のSlackチャネルを設定できます。

1. NetScaler Consoleで、「**インフラストラクチャ > イベント > ルール**」に移動し、「**追加**」をクリックしてルールを作成します。
2. 「**Create Rule**」ページで、重要度やカテゴリなどのルールパラメータを設定します。監視する必要があるインスタンスと障害オブジェクトを選択します。
3. 「**Event Rule Actions**」で、「**Add Action**」をクリックします。次に、「**Action Type**」リストから「**Send Slack Notifications**」を選択し、「**Slack Profile List**」を選択します。
4. 「**Slack Profile List**」フィールドの横にある「**Add**」をクリックして、Slackプロファイルリストを追加することもできます。
5. プロファイルリストを作成するには、次のパラメータを入力します。
   a. **Profile Name**。NetScaler Consoleで構成するプロファイルリストの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **Channel Name**。イベント通知の送信先となるSlackチャネルの名前を入力します。

c. **Webhook URL**。以前に入力したチャネルのWebhook URLを入力します。受信Webhookは、外部ソースからSlackにメッセージを投稿する簡単な方法です。URLはチャネル名に内部的にリンクされており、すべてのイベント通知はこのURLに送信され、指定されたSlackチャネルに投稿されます。Webhookの例は次のとおりです。`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

6. 「**Create**」をクリックし、「**Add Event Action**」ウィンドウで「**OK**」をクリックします。

**注記:**

「**System**」\>「**Notifications**」\>「**Slack Profiles**」に移動して、Slackプロファイルを追加することもできます。「**Add**」をクリックし、前のセクションで説明したようにプロファイルを作成します。

作成したSlackプロファイルのステータスを表示できます。

これで、適切なフィルタと明確に定義されたイベントルールアクションを持つイベントルールが作成されました。

### NetScaler ConsoleからPagerDuty通知を設定するには

PagerDutyの構成に基づいてインシデント通知を監視するために、NetScaler Consoleのオプションとして PagerDutyプロファイルを追加できます。PagerDutyを使用すると、登録された番号に電子メール、SMS、プッシュ通知、電話で通知を構成できます。

NetScaler ConsoleにPagerDutyプロファイルを追加する前に、PagerDutyで必要な構成が完了していることを確認してください。詳細については、PagerDutyドキュメントを参照してください。

以下の機能の通知を受け取るオプションの1つとして、PagerDutyプロファイルを選択できます。

- **イベント** – NetScalerインスタンス用に生成されたイベントのリスト。
- **ライセンス** – 現在アクティブなライセンス、期限切れ間近のライセンスなどのリスト。
- **SSL証明書** – NetScalerインスタンスに追加されたSSL証明書のリスト。

### NetScaler ConsoleでPagerDutyプロファイルを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **設定 > 通知 > PagerDutyプロファイル**に移動します。
3. **追加**をクリックして新しいプロファイルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. PagerDutyプロファイルの作成ページで：

   a. 任意のプロファイル名を入力します。

   b. **統合キー**を入力します。

      統合キーはPagerDutyポータルから取得できます。

   c. **作成**をクリックします。

   **ユースケース：**

   次のシナリオを検討してください。

   - PagerDutyプロファイルに通知を送信したい。
   - PagerDutyで通知を受け取るオプションとして電話を設定している。
   - NetScalerイベントの電話アラートを受け取りたい。

   設定するには：

   a. **イベント** > **ルール** に移動します。

   b. **ルールの作成** ページで、ルールを作成するための他のすべてのパラメータを設定します。

   c. **ルールアクションの作成** で、**アクションの追加** をクリックします。

      **イベントアクションの追加** ページが表示されます。

      i. **アクションタイプ** で、**PagerDuty通知の送信** を選択します。

      ii. PagerDutyプロファイルを選択し、**OK** をクリックします。

   設定が完了すると、NetScalerインスタンスで新しいイベントが生成されるたびに電話がかかってきます。その電話から、次のことを決定できます。

   - イベントを承認する
   - 解決済みとしてマークする
   - 別のチームメンバーにエスカレートする

**NetScaler ConsoleからServiceNowインシデントを自動生成するには**

NetScaler Console GUIでServiceNowプロファイルを選択することで、NetScaler ConsoleイベントのServiceNowインシデントを自動生成できます。イベントルールを設定するには、NetScaler ConsoleでServiceNowプロファイルを選択する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ServiceNowインシデントを自動生成するイベントルールを設定する前に、NetScaler ConsoleをServiceNowインスタンスと統合します。詳細については、ServiceNow 用 ITSM アダプターを構成するを参照してください。

イベントルールを設定するには、**Events** > **Rules** に移動します。

1. **ルールの作成**ページで、ルールを作成するための他のすべてのパラメータを設定します。
2. **ルールアクションの作成**の下で、**アクションの追加**をクリックします。

   **イベントアクションの追加**ページが表示されます。

   a. **アクションタイプ**で、**ServiceNow通知の送信**を選択します。
   b. **ServiceNowプロファイル**で、リストから**Citrix_Workspace_SN**プロファイルを選択します。
   c. **OK**をクリックします。

## NetScalerインスタンスで発生するイベントの報告された重大度を変更する

すべてのデバイスで生成されるイベントのレポートを管理できるため、特定のインスタンスで特定のイベントに関するイベントの詳細を表示し、イベントの重大度に基づいてレポートを表示できます。デフォルトの重大度設定を使用するイベントルールを作成でき、重大度設定を変更できます。汎用イベントと企業固有のイベントの両方で重大度を設定できます。

次の重大度レベルを定義できます: Critical、Major、Minor、Warning、およびClear。

**イベントの重大度を変更するには:**

1. **Infrastructure > Events > Event Settings** に移動します。
2. 変更するNetScalerインスタンスタイプのタブをクリックします。次に、リストからカテゴリを選択し、**Configure Severity** をクリックします。
3. **Configure Event Severity** で、ドロップダウンリストから重大度レベルを選択します。
4. **OK** をクリックします。

   イベントの重大度を変更する(/en-us/netscaler-application-delivery-management-software/media/nmas-configure-severity.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## イベント概要の表示

NetScaler Consoleサーバーで受信したイベントとトラップを監視するためのイベント概要ページを表示できるようになりました。**インフラストラクチャ > イベント** に移動します。イベント概要ページには、以下の情報が表形式で表示されます。

- **NetScaler Consoleが受信したすべてのイベントの概要**。イベントはカテゴリ別に一覧表示され、異なる重大度が異なる列に表示されます: 重大、主要、軽微、警告、クリア、情報。たとえば、NetScalerインスタンスがダウンし、NetScaler Consoleサーバーへの情報送信を停止すると、重大なイベントが発生します。イベント発生中、インスタンスがダウンした理由、ダウンしていた時間などが記載された通知が管理者に送信されます。その後、イベントはイベント概要ページに記録され、そこで概要を表示したり、イベントの詳細にアクセスしたりできます。

  

- **カテゴリごとに受信したトラップの数**。受信したトラップの数で、重大度別に分類されます。デフォルトでは、NetScalerインスタンスからNetScaler Consoleに送信される各トラップには重大度が割り当てられていますが、ネットワーク管理者として、NetScaler Console GUIでその重大度を指定できます。

カテゴリタイプまたはトラップをクリックすると、 **イベント**ページに移動し、カテゴリや重大度などのフィルターが事前に選択されます。このページには、NetScalerインスタンスのIPアドレスとホスト名、トラップが受信された日付、カテゴリ、障害オブジェクト、実行された構成コマンド、メッセージ通知など、イベントに関する詳細情報が表示されます。



## イベントメッセージを表示

NetScaler® Consoleで受信したすべてのアクティブなイベントは、**インフラストラクチャ > イベント > イベントメッセージ**ページに表示されます。

**イベントメッセージ**ページでは、インスタンスのリストと、重大度、カテゴリ、イベント発生日時、障害オブジェクトなどのイベントの詳細を表示できます。

イベントは、過去30分、1時間、1日など、発生した時間に基づいてフィルタリングできます。また、好みに応じてカスタム時間を選択することもできます。

NetScaler ConsoleはカスタムSNMPトラップをサポートしており、これらは**イベントメッセージ**の下で**カスタム**としてタグ付けされます。この**カスタム**タグは、デフォルトのSNMPアラートと区別するのに役立ちます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

# イベントの重要度とSNMPトラップの詳細を表示

NetScaler Consoleでイベントとその設定を作成すると、イベントサマリーページでイベントをすぐに表示できます。同様に、NetScaler Consoleサーバーに追加されたすべてのCitrix NetScalerインスタンスの健全性、稼働時間、モデル、およびバージョンを、インフラストラクチャダッシュボードで詳細に表示および監視できます。

インフラストラクチャダッシュボードでは、関連性のない値をマスクできるようになり、重要度別のイベント、健全性、稼働時間、モデル、NetScalerインスタンスのバージョンなどの情報をより簡単に詳細に表示および監視できます。

たとえば、**Critical**（重大）の重要度レベルのイベントはめったに発生しないかもしれません。しかし、これらの重大なイベントがネットワークで発生した場合、イベントがどこでいつ発生したかをさらに調査、トラブルシューティング、監視したいと思うかもしれません。Critical以外のすべての重要度レベルを選択すると、グラフには重大なイベントの発生のみが表示されます。また、グラフをクリックすると、**Severity based events**（重要度ベースのイベント）ページに移動し、選択した期間に重大なイベントが発生した時期に関するすべての詳細（インスタンスソース、日付、カテゴリ、重大なイベント発生時に送信されたメッセージ通知）を確認できます。

同様に、ダッシュボードでNetScaler VPXインスタンスの健全性を表示できます。インスタンスが稼働していた時間をマスクし、サービス停止中の時間のみを表示できます。グラフをクリックすると、そのインスタンスのページに移動し、*out of service*（サービス停止中）フィルターがすでに適用されており、ホスト名、1秒あたりのHTTPリクエスト数、CPU使用率などの詳細を確認できます。インスタンスを選択して、特定のCitrixインスタンスのダッシュボードで詳細を確認することもできます。

**NetScaler Consoleで重要度別に特定のイベントを選択するには：**

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Infrastructure > Dashboard** に移動します。

   または、,

   **Infrastructure > Events > Reports** に移動します。
3. ページの右上隅にあるメニューから、重要度別にイベントを表示したい期間を選択します。

   イベントの重要度別(/en-us/netscaler-application-delivery-management-software/media/masvc-events-report-severity-mask.png)
4. **Events by Severity**（重要度別イベント）ドーナツチャートは、すべてのイベントを重要度別に視覚的に表示します。異なる種類のイベントは異なる色のセクションとして表され、各セクションの長さはその重要度タイプのイベントの総数に対応します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. ドーナツチャートの各セクションをクリックすると、対応する**Severity based events**（重要度ベースのイベント）ページが表示され、選択した期間の選択した重要度に関する以下の詳細が表示されます。

   - インスタンスソース
   - イベントのデータ
   - NetScalerインスタンスによって生成されたイベントのカテゴリ
   - 送信されたメッセージ通知

   **注**

   ドーナツチャートの下には、チャートに表示されている重要度の一覧が表示されます。デフォルトでは、ドーナツチャートはすべての重要度タイプのすべてのイベントを表示するため、リスト内のすべての重要度タイプが強調表示されます。選択した重要度をより簡単に表示および監視するために、重要度タイプを切り替えることができます。

   重要度タイプ(/en-us/netscaler-application-delivery-management-software/media/nsmas-events-report-masking.png)

**NetScaler ConsoleでNetScaler SNMPトラップの詳細を表示するには：**

**イベント設定**ページで、管理対象のNetScalerインスタンスから受信した各SNMPトラップの詳細をNetScaler Consoleサーバーで表示できるようになりました。**インフラストラクチャ > イベント > イベント設定**に移動します。インスタンスから受信した特定のトラップについて、以下の詳細を表形式で表示できます。

- **カテゴリ** - イベントが属するインスタンスのカテゴリを指定します。
- **重要度** - イベントの重要度は、色とその重要度タイプによって示されます。
- **説明** - イベントに関連付けられたメッセージを指定します。

たとえば、トラップカテゴリが**monRespTimeoutBelowThresh**のイベントの場合、トラップの説明は「このトラップは、モニタープローブの応答タイムアウトが正常に戻り、設定されたしきい値を下回ったときに送信されます。」と表示されます。

## NetScaler syslogメッセージの表示とエクスポート

NetScaler Consoleから、Citrix NetScalerインスタンスで生成されたsyslogイベントを監視できます。そのためには、NetScaler ConsoleをNetScalerインスタンスのsyslogサーバーとして構成する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

必要があります。NetScaler Consoleを構成すると、すべてのsyslogメッセージはNetScalerインスタンスからNetScaler Consoleにリダイレクトされます。

### NetScaler Consoleをsyslogサーバーとして構成する

NetScaler Consoleをsyslogサーバーとして構成するには、次の手順に従います。

1. NetScaler Console GUIから、**Infrastructure > Instances**に移動します。
2. syslogメッセージを収集してNetScaler Consoleに表示したいNetScalerインスタンスを選択します。
3. **Select Action**リストで、**Configure Syslog**を選択します。
4. **Enable**をクリックします。
5. **Facility**ドロップダウンリストで、ローカルまたはユーザーレベルのファシリティを選択します。
6. syslogメッセージの必要なログレベルを選択します。
7. **OK**をクリックします。

NetScaler Consoleでsyslogを構成する(/en-us/netscaler-application-delivery-management-software/media/configure-syslog-adm.png)

これらの手順により、NetScalerインスタンス内のすべてのsyslogコマンドが構成され、NetScaler Consoleはsyslogメッセージの受信を開始します。

### syslogメッセージの表示と検索

管理対象のNetScalerインスタンスで生成されたすべてのsyslogメッセージを表示できます。syslogメッセージはデータベースに一元的に保存され、監査目的で**Infrastructure > Events > Syslog Messages**で利用できます。このログ情報を組み合わせて、収集されたデータから分析用のレポートを作成できます。

さらに、フィルターを使用してsyslogメッセージの検索結果を絞り込み、探しているものをリアルタイムで正確に見つけることができます。**ヘルプが必要ですか？**をクリックして、組み込みの検索ヘルプを開きます。



次に、検索語を追加します。一部のカテゴリでは、事前に入力された検索語のリストが表示されます。デフォルトでは、検索期間は1日です。下矢印をクリックして、時間と日付の範囲を変更できます。**Syslog Summary**ペインからオプションを選択することで、検索をさらに絞り込むことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### syslogメッセージのエクスポートとスケジュール

NetScaler Consoleにログインすることなく、サーバーで受信したすべてのsyslogメッセージのエクスポートをスケジュールすることで、syslogメッセージを表示できます。NetScalerインスタンスで生成されたsyslogメッセージをPDF、CSV、PNG、JPEG形式でエクスポートできます。これらのレポートのエクスポートを、指定されたメールアドレスまたはSlackアカウントにさまざまな間隔でスケジュールできます。

ログメッセージをエクスポートおよびスケジュールするには、右上隅にある矢印アイコンをクリックします。

- ログメッセージをエクスポートするには、**Export Reports > Export Now**をクリックし、必要な形式を選択してから、**Export**をクリックします。
- syslogメッセージのエクスポートをスケジュールするには、**Export Reports > Schedule Report**をクリックし、必要なパラメーターを設定します。レポートはメールまたはSlackで受け取ることができます。

## syslogメッセージを抑制する

syslogサーバーとして構成されている場合、NetScaler Consoleは、構成されたNetScalerインスタンスから送信されるすべてのsyslogメッセージを受信します。表示したくない多数のメッセージが存在する可能性があります。たとえば、すべての情報レベルのメッセージを表示することに興味がない場合があります。関心のないsyslogメッセージの一部を破棄できるようになりました。NetScaler Consoleに入ってくるsyslogメッセージの一部は、フィルターを設定することで抑制できます。NetScaler Consoleは、基準に一致するすべてのメッセージを破棄します。これらの破棄されたメッセージはNetScaler Console GUIに表示されず、顧客のNetScaler Consoleデータベースにも保存されません。

NetScaler Consoleに入ってくるログに記録されたsyslogメッセージの一部は、フィルターを設定することで抑制できます。syslogメッセージの抑制に使用できる2つのフィルターは、重大度とファシリティです。特定のNetScalerインスタンスまたは複数のインスタンスから送信されるメッセージを抑制することもできます。NetScaler Consoleがメッセージを検索して抑制するためのテキストパターンを提供することもできます。NetScaler Consoleは、基準に一致するすべてのメッセージを破棄します。これらの破棄されたメッセージはNetScaler Console GUIに表示されず、顧客データベースにも保存されません。したがって、ストレージサーバーのスペースを大幅に節約できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

syslogメッセージを抑制するためのいくつかのユースケースは次のとおりです。

- すべての情報レベルのメッセージを無視したい場合は、レベル6（情報）を抑制します。
- ファイアウォールのエラー状態のみを記録したい場合は、レベル3（エラー）以外のすべてのレベルを抑制します。

### フィルターを作成してsyslogメッセージを抑制する

1. NetScaler Consoleで、**インフラストラクチャ > イベント > Syslogメッセージ** \> **抑制フィルター** の順に移動します。
2. ページで、次の情報を更新します。

   a. - フィルターの名前を入力します。

   > **注**
   >
   > 複数のNetScalerインスタンスに対して異なるユーザーが異なるアクセス権を持っている場合、ユーザーはアクセス権を持つすべてのインスタンスのフィルターのみを表示できるため、インスタンスごとに異なるフィルターを作成する必要があります。

   b. - メッセージを抑制する必要があるログレベルを選択して追加します。たとえば、入ってくる情報メッセージを表示したくない場合は、 を選択してそれらのメッセージを抑制できます。

   c. - syslogメッセージが構成されているNetScalerインスタンスを選択します。

   d. **ファシリティ** - メッセージを生成するソースに基づいて、メッセージを抑制するファシリティを選択します。

   e. **メッセージパターン** - アスタリスク (*) で囲まれたテキストパターンを入力して、メッセージを抑制することもできます。メッセージはテキストパターン文字列で検索され、このパターンを含むメッセージは抑制されます。

   フィルターファシリティの抑制(/en-us/netscaler-application-delivery-management-software/media/suppress-filter-facilities.png)

### フィルターの無効化

NetScaler Console でメッセージを表示できるようにするには、フィルターを無効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Infrastructure > イベント > Syslog メッセージ** \> **抑制フィルター** に移動し、**抑制フィルター** ページでフィルターを選択して**編集**をクリックします。
2. **抑制フィルターの構成**ページで、**フィルターを有効にする**チェックボックスをオフにしてフィルターを無効にします。

## インスタンスイベントのパージ設定を構成する

NetScaler Consoleサーバーによって管理されているCitrix NetScalerインスタンスは、NetScaler Consoleに保存されるようにイベントメッセージデータを継続的に送信します。NetScaler Consoleがネットワークレポートデータ、イベント、監査ログ、タスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと（00:00）にパージされます。

**注**

指定できる値は、40日を超えることも、1日未満にすることもできません。

**インスタンスイベントのパージ設定を構成するには:**

1. **System** \> **System Administration** に移動します。
2. **Prune Settings** で、**Instance Events Prune Settings** をクリックします。
3. NetScaler Consoleサーバーでデータを保持する期間（日数）を入力し、**OK**をクリックします。

# ネットワーク機能

ネットワーク機能機能を使用すると、管理対象のCitrix NetScalerインスタンスに構成されているエンティティの状態を監視できます。トランザクションの詳細、接続の詳細、ロードバランシング仮想サーバーのスループットなどの統計情報を表示できます。メンテナンスを計画する際に、エンティティを有効または無効にすることもできます。

ネットワーク機能ダッシュボードには、次のグラフが表示されます。

- クライアント接続数が最も多い仮想サーバー上位5件
- サーバー接続数が最も多い仮想サーバー上位5件
- スループットが最大（MB/秒）の仮想サーバー上位5件
- スループットが最小（MB/秒）の仮想サーバー下位5件
- 仮想サーバーが最も多いインスタンス上位5件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 仮想サーバーの状態
- ロードバランシング仮想サーバーの健全性
- プロトコル

## ロードバランシングエンティティのレポートを生成する

NetScaler Consoleでは、Citrix NetScalerインスタンスエンティティのレポートをすべてのレベルで表示できます。NetScaler Console \> ネットワーク機能でダウンロードできるレポートには、統合レポートと個別レポートの2種類があります。

**統合レポート**: NetScalerインスタンスで管理されているすべてのエンティティについて、統合または要約されたレポートをダウンロードして表示できます。

このレポートにより、NetScalerインスタンス、パーティション、およびネットワーク内に存在する対応するロードバランシングエンティティ（仮想サーバー、サービスグループ、サービス）間のマッピングを大まかに把握できます。

次の図は、要約レポートの例を示しています。

要約レポートの例(/en-us/netscaler-application-delivery-management-software/media/load-balancing-report.png)

統合レポートはCSV形式です。各列のエントリは次のとおりです。

- **NetScaler IPアドレス**: NetScalerインスタンスのIPアドレスがレポートに表示されます。
- **NetScaler® ホスト名**: ホスト名がレポートに表示されます。
- **パーティション**: 管理パーティションのIPアドレスが表示されます。
- **仮想サーバー**: \<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **サービス**: \<name_of_the_service\>#service-IP_address:port_number
- **サービスグループ**: \<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

**注**

- ホスト名が利用できない場合は、対応するIPアドレスが表示されます。
- 空白の列は、それぞれのエンティティがそのNetScalerインスタンスに対して構成されていないことを示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**個別のレポート**: すべてのインスタンスとエンティティの独立したレポートをダウンロードして表示することもできます。たとえば、ロードバランシング仮想サーバー、ロードバランシングサービス、またはロードバランシングサービスグループのみのレポートをダウンロードできます。

NetScaler Consoleでは、レポートを即座にダウンロードできます。また、レポートを1日1回、週1回、または月1回、決まった時間に生成するようにスケジュールすることもできます。

### 結合されたロードバランシングレポートを生成する

1. NetScaler Consoleで、**インフラストラクチャ > ネットワーク機能 > 負荷分散**に移動します。
2. **Load Balancing**ページで、
   
   をクリックします。
3. 開いた**Export**ページには、レポートを表示するための2つのオプションがあります。
   a. **Export Now**タブを選択し、**OK**をクリックします。

      統合レポートがシステムにダウンロードされます。
   b. **Schedule Report**タブを選択して、レポートの生成とエクスポートを定期的にスケジュールします。レポート生成の繰り返し設定を指定し、レポートのエクスポート先となるメールプロファイルを作成します。

      i. **Recurrence** - ドロップダウンリストボックスから**Daily**、**Weekly**、または**Monthly**を選択します。
      ii. **Recurrence time** - 時:分を24時間形式で入力します。
      iii. **Email Profile** - ドロップダウンリストボックスからプロファイルを選択するか、**+**をクリックしてメールプロファイルを作成します。

> **注**
>
> **Weekly**の繰り返しを選択する場合は、レポートをスケジュールする曜日を選択していることを確認してください。

結合された負荷分散レポートを生成する(/en-us/netscaler-application-delivery-management-software/media/load-balancing-scheduled-report.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注**
>
> **月次**の繰り返しを選択した場合は、レポートをスケジュールするすべての日をコンマで区切って入力してください。

### 個別の負荷分散エンティティレポートを生成する

インスタンスに関連付けられた特定の種類のエンティティについて、個別のレポートを生成およびエクスポートできます。たとえば、ネットワーク内のすべての負荷分散サービスの一覧を表示したいシナリオを考えてみましょう。

1. NetScaler Consoleで、**インフラストラクチャ > ネットワーク機能 > 負荷分散 > サービス**に移動します。
2. **サービス**ページで、右上隅にある**エクスポート**ボタンをクリックします。
   a. この時点でレポートを生成して表示したい場合は、**今すぐエクスポート**タブを選択します。
   b. 定期的にレポートの生成とエクスポートをスケジュールするには、**エクスポートのスケジュール**を選択します。

> **注**
>
> レポートをダウンロードするか、メールの添付ファイルとしてエクスポートすることのみ可能です。NetScaler Console GUIでレポートを表示することはできません。

## ネットワーク機能レポートのエクスポートまたはエクスポートのスケジュール設定

NetScaler Consoleでは、ロードバランシング、コンテンツスイッチング、キャッシュリダイレクション、グローバルサーバーロードバランシング (GSLB)、認証、NetScaler Gatewayなどの選択されたネットワーク機能について、包括的なレポートを生成できます。このレポートにより、NetScalerインスタンス、パーティション、およびネットワーク内に存在する対応するバインドされたエンティティ (仮想サーバー、サービスグループ、サービス) 間のマッピングを大まかに把握できます。これらのレポートは.csvファイル形式でエクスポートできます。

レポートには、次の仮想サーバーデータが表示されます。

- NetScaler® IPアドレス
- ホスト名

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- パーティションデータ
- 仮想サーバー名
- 仮想サーバーのタイプ
- 仮想サーバー
- ターゲットLB仮想サーバー

**注**

コンテンツスイッチングおよびキャッシュリダイレクション仮想サーバーの場合、「ターゲットLB仮想サーバー」列には、デフォルトサーバーとポリシーベースサーバーの両方を含むすべてのLBサーバーが一覧表示されます。

- サービス名
- サービスグループ名

これらのレポートは、指定されたメールアドレスに異なる間隔でエクスポートするようにスケジュールできます。

**注**

- GSLB仮想サーバーの場合、ネットワーク機能レポートにはGSLB仮想サーバーと関連サービスのみが表示されます。
- コンテンツスイッチングおよびキャッシュリダイレクション仮想サーバーの場合、レポートには関連するLBサーバーへのバインディングのみが表示されます。
- SSL仮想サーバーは、NetScaler ConsoleでSSL仮想サーバーの個別のリストが管理されていないため、このレポートには表示されません。
- 新しいレポートが生成されると、古いレポートはアカウントから自動的にパージされます。
- HAProxyのネットワーク機能レポートを生成することはできません。

**ネットワーク機能レポートをエクスポートおよびスケジュールするには:**

1. **Infrastructure > Network Functions** に移動します。
2. **ネットワーク機能**ページで、右ペインのページの右上隅にある**レポートの生成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **レポートの生成**ページには、次の2つのオプションがあります。

   a. **今すぐエクスポート**タブを選択し、**OK**をクリックします。レポートがシステムにダウンロードされます。

   次の図は、ネットワーク機能レポートの例を示しています。

   

   b. **レポートのスケジュール**タブを選択して、定期的にレポートの生成とエクスポートをスケジュールします。レポート生成の繰り返し設定を指定し、レポートがエクスポートされるメールプロファイルを作成します。

      i. **繰り返し** - ドロップダウンリストボックスから**毎日**、**毎週**、または**毎月**を選択します。

      ii. **繰り返し時間** - 24時間形式で、時:分 の形式で時間を入力します。

      iii. **メールプロファイル** - ドロップダウンリストボックスからプロファイルを選択するか、**+** をクリックしてメールプロファイルを作成します。

**スケジュールを有効にする** をクリックしてレポートをスケジュールし、次に **OK** をクリックします。**スケジュールを有効にする** チェックボックスをクリックすると、選択したレポートを生成できます。

# ネットワークレポート

NetScaler Application Delivery Management (NetScaler Console) でネットワークレポートを監視することで、リソースの使用状況を最適化できます。複数の場所に多くのアプリケーションが展開されている分散展開環境があるかもしれません。アプリケーションの最適なパフォーマンスを確保するために、トラフィックの負荷分散、コンテンツスイッチ、または圧縮を行うために、複数のCitrix Application Delivery Controller (NetScaler) インスタンスも展開しています。ネットワークパフォーマンスはアプリケーションパフォーマンスに影響を与える可能性があります。アプリケーションのパフォーマンスを維持し続けるには、ネットワークパフォーマンスを定期的に監視し、すべてのリソースが最適に使用されていることを確認する必要があります。

NetScaler Consoleでは、グローバルレベルのインスタンスだけでなく、仮想サーバーやネットワークインターフェイスなどのエンティティについてもレポートを生成できるようになりました。インスタンスファミリーはNetScalerインスタンスで構成されます。レポートを生成できる仮想サーバーは次のとおりです。

- 負荷分散サーバー、サービス、およびサービスグループ
- コンテンツスイッチングサーバー
- キャッシュリダイレクションサーバー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- グローバルサービス負荷分散 (GSLB)
- 認証
- NetScaler ゲートウェイ

NetScaler Consoleのネットワークレポートダッシュボードは、高度にカスタマイズ可能です。さまざまなインスタンス、仮想サーバー、およびその他のエンティティに対して複数のダッシュボードを作成できるようになりました。

## ネットワークレポートダッシュボード

次の画像は、ダッシュボードのさまざまな機能を示しています。



- 左側のサイドパネルには、NetScaler Consoleで作成されたすべてのカスタムダッシュボードが表示されます。いずれかをクリックすると、そのダッシュボードを構成するさまざまなレポートを表示できます。たとえば、TCPおよびSSLダッシュボードには、TCPおよびSSLプロトコルに関連するさまざまなレポートが含まれています。
- 各ダッシュボードは、複数のウィジェットでカスタマイズして、さまざまなレポートを表示できます。ウィジェットはダッシュボード上のレポートを表し、それはより関連性の高いレポートの集合体です。たとえば、圧縮TCPバイト使用量レポートには、1秒あたりに転送および受信された圧縮TCPバイトに関するレポートが含まれています。
- レポートは1時間、1日、1週間、または1か月間表示できます。さらに、NetScaler Consoleで生成されるレポートの期間をカスタマイズするために、タイムラインスライダーオプションを使用できるようになりました。
- 「X」をクリックしてレポートを削除できます。レポートを.pdf、.jpeg、.png、または.csv形式でシステムにエクスポートすることもできます。レポートを生成する時間と繰り返しをスケジュールすることもできます。レポートを送信する電子メール配布リストを設定することもできます。
- ダッシュボード上部の「インスタンス」セクションには、レポートが生成されるすべてのインスタンスのIPアドレスが一覧表示されます。
- 「X」をクリックしてインスタンスを削除するか、レポートにインスタンスを追加できます。ただし、現在NetScaler Consoleでは10個のインスタンスのレポートを表示できます。
- ダッシュボード全体を.pdf、.jpeg、.png、または.csv形式でシステムにエクスポートすることもできます。ダッシュボードに加えた変更はすべて保存する必要があります。変更を保存するには、をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次のセクションでは、ダッシュボードの作成、レポートの生成、およびレポートのエクスポートに関するタスクについて詳しく説明します。

**ダッシュボードを表示または作成するには：**

1. NetScaler Consoleで、**インフラストラクチャ > ネットワークレポート**に移動します。

   ダッシュボードを作成(/en-us/netscaler-application-delivery-management-software/media/nw-dash.png)
2. 既存のダッシュボードを表示するには、**をクリックします。ネットワークレポートのダッシュボード**ページが開き、すべてのダッシュボードとレポートウィジェットを表示できます。
3. ダッシュボードを作成するには、****をクリックします。ページが開きます。 基本設定(/en-us/netscaler-application-delivery-management-software/media/nw-dash-create-new.png)
4. タブで、次の詳細を入力します。

   a. **名前**。ダッシュボードの名前を入力します。

   b. **インスタンスファミリ**。インスタンスのタイプ（NetScalerまたはNetScaler SDX）を選択します。

   c. **タイプ**。レポートを生成するエンティティタイプを選択します。この例では、負荷分散仮想サーバーを選択します。

   d. **説明**。ダッシュボードの分かりやすい説明を入力します。
5. **次へ**をクリックします。インスタンスと特定のエンティティでサポートされているすべてのレポートが表示されます。
6. **レポートの選択**タブで、必要なレポートを選択します。この例では、トランザクション、接続、スループットを選択できます。**次へ**をクリックします。

ネットワークレポートの選択(/en-us/netscaler-application-delivery-management-software/media/nw-dash-rprt.png)

1. **エンティティの選択**タブで、**追加**をクリックします。

   **基本設定**タブで選択したエンティティタイプに応じて、エンティティリストを含むウィンドウが表示されます。この例では、**LB仮想サーバーの選択**ウィンドウが表示されます。
2. 監視するエンティティを選択します。

   ネットワークエンティティの選択(/en-us/netscaler-application-delivery-management-software/media/nw-dash-entities.png)
3. **作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ダッシュボードが作成され、選択したすべてのレポートが表示されます。

**注**

現在、凡例またはフィルターに加えた変更は保存できません。

## ネットワークレポートのエクスポート

ウィジェットレポートは.pdf、.png、.jpeg、または.csv形式でエクスポートできますが、ダッシュボード全体は.pdf、.jpeg、または.png形式でのみエクスポートできます。

**注**

読み取り専用権限がある場合、NetScaler Consoleでレポートをエクスポートすることはできません。NetScaler Consoleでファイルを作成し、エクスポートするには、編集権限が必要です。

**ダッシュボードレポートをエクスポートするには:**

1. **Infrastructure > Network Reporting** に移動します。
2. 作成したすべてのダッシュボードを表示するには、**View Dashboards** をクリックします。
3. 左ペインでダッシュボードをクリックします。この例では、**Dashboard 1** をクリックします。
4. ページ右上のエクスポートボタンをクリックします。
5. **Export Now** タブで、必要な形式を選択し、**Export** をクリックします。

   **Export** ページで、次のいずれかを実行できます。
6. **Export Now** タブを選択します。レポートをPDF、JPEG、PNG、またはCSV形式で表示および保存します。
7. **Schedule Export** タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、メールまたはSlackメッセージでレポートを送信します。

   **Network Reporting** ダッシュボードページのエクスポートを定期的にスケジュールできます。たとえば、特定の時間に過去1時間分のダッシュボードレポートを毎週生成するオプションを設定できます。レポートは毎週生成され、ダッシュボードのステータスが表示されます。ユーザーによって設定された場合、レポートは時刻と日付のスタンプを上書きします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

- 毎週の繰り返しを選択する場合は、レポートをスケジュールする曜日を選択していることを確認してください。
- 毎月の繰り返しを選択する場合は、レポートをスケジュールするすべての日をコンマで区切って入力していることを確認してください。

ネットワークレポートをスケジュールする際、**Subject** フィールドにテキスト文字列を入力することで、レポートの見出しをカスタマイズできます。スケジュールされた時間に作成されるレポートには、この文字列が名前として使用されます。

例えば、特定の仮想サーバーから発信されるネットワークレポートの場合、件名に「authentication-reports-10.106.118.120」と入力できます。ここで、10.106.118.120は監視対象の仮想サーバーのIPアドレスです。

**注**

現在、このオプションはレポートのエクスポートをスケジュールする場合にのみ利用可能です。レポートを即座にエクスポートする際には、見出しを追加することはできません。

## 集計を適用してネットワークレポートデータを表示する

ネットワークパフォーマンスデータに集計を適用し、ダッシュボードでアプリケーションパフォーマンスを表示できます。要件に基づいて結果をエクスポートすることもできます。データに適用されたこれらの集計を使用することで、すべてのリソースが最適に利用されているかを分析し、確認できます。**Network > Network Reporting** に移動し、**View By** オプションを取得するために1日以上の期間を選択します。

既存の平均データでは、**View By** リストからオプションを選択して集計を適用できます。集計を適用すると、ダッシュボードの各メトリックのデータが更新されます。**Settings** をクリックし、**Aggregation Filters** を選択します。

集計フィルター(/en-us/netscaler-application-delivery-management-software/media/aggregation-filters.png)

追加できる集計は次のとおりです。

- カウント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 最大値
- 最小値
- 合計
- 標準偏差
- 分散
- 最頻値
- 中央値
- 25パーセンタイル
- 75パーセンタイル
- 95パーセンタイル
- 99パーセンタイル
- 最初
- 最後

ダッシュボードには最大4つの集計オプションを追加できます。集計オプションを追加すると、NetScaler Consoleは選択された集計オプションのレポートを生成するのに約1時間かかります。

**ウィジェットレポートをエクスポートするには：**

1. **インフラストラクチャ > ネットワークレポート**に移動します。
2. **ダッシュボードの表示**をクリックして、作成したすべてのダッシュボードを表示します。
3. 左ペインでダッシュボードをクリックします。この例では、**Skype for Business**もクリックします。
4. ウィジェットを選択します。たとえば、**負荷分散仮想サーバートランザクション**を選択します。
5. ページ右上のエクスポートボタンをクリックします。
6. **今すぐエクスポート**タブで、必要な形式を選択し、**エクスポート**をクリックします。

   ウィジェットレポートをエクスポート(/en-us/netscaler-application-delivery-management-software/media/nw-dash-widget-export.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScaler Consoleでネットワークレポートのしきい値を管理する方法

NetScalerインスタンスの状態を監視するには、カウンターにしきい値を設定し、しきい値を超過したときに通知を受け取ることができます。NetScaler Consoleでは、しきい値を構成し、表示、編集、削除できます。

たとえば、コンテンツスイッチング仮想サーバーの接続カウンターが指定された値に達したときに、電子メール通知を受け取ることができます。特定のインスタンスタイプにしきい値を定義できます。また、選択したインスタンスから特定のカウンターメトリックに対して生成するレポートを選択することもできます。

カウンターの値がしきい値を超過または下回った場合（ルールで指定されている場合）、パフォーマンス関連の問題を示す指定された重大度のイベントが生成されます。カウンター値が正常と見なされる値に戻ると、イベントはクリアされます。これらのイベントは、**インフラストラクチャ > イベント > レポート**に移動して表示できます。レポートページで、**重大度別イベント**ドーナツをクリックすると、重大度別にイベントを表示できます。

しきい値が侵害されたときに電子メールまたはSMSメッセージを送信するなど、しきい値にアクションを関連付けることもできます。

**しきい値を作成するには：**

1. NetScaler Consoleで、**インフラストラクチャ > ネットワークレポート > しきい値**に移動します。**しきい値**の下で、**追加**をクリックします。
2. **しきい値の作成**ページで、次の詳細を指定します。
   - **名前**。しきい値の名前。
   - **インスタンスタイプ**。NetScalerを選択します。
   - **レポート名**。このしきい値に関する情報を提供するパフォーマンスレポートの名前。
3. イベントを生成またはクリアするタイミングを指定するルールを設定することもできます。**ルールの構成**セクションで、次の詳細を指定できます。
   - **メトリック**。しきい値を設定するメトリックを選択します。
   - **比較演算子**。監視対象の値がしきい値以上であるか、しきい値以下であるかを確認する比較演算子を選択します。
   - **しきい値**。イベントの重大度が計算される値を入力します。たとえば、監視対象の現在のクライアント接続の値が80パーセントに達した場合に、重大なイベント重大度でイベントを生成したいとします。この場合、しきい値として80と入力します。「重大な重大度」のイベントは、**Infrastructure > イベント > レポート**に移動して表示できます。レポート

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ページで、**重大度別イベント**ドーナツをクリックすると、重大度別のイベントを表示できます。

- **クリア値**。値をクリアするタイミングを示す値を入力します。たとえば、監視対象の値が50パーセントに達したときに、現在のクライアント接続のしきい値をクリアしたいとします。この場合、クリア値として50と入力します。
- **イベントの重大度**。しきい値に設定するセキュリティレベルを選択します。

4. しきい値を設定するインスタンスとエンティティを選択できます。**インスタンス**セクションで、次のいずれかのオプションを選択します。

   - **すべてのインスタンス**。すべてのインスタンスにしきい値が設定されます。
   - **特定のインスタンス**。特定のインスタンスにしきい値が設定されます。右矢印を使用して、**利用可能**リストから**構成済み**リストにインスタンスを移動します。しきい値は、**構成済み**リストのインスタンスに設定されます。
   - **特定のエンティティ**。特定のエンティティにしきい値が設定されます。

     エンティティを選択するには、**追加**をクリックします。

     **レポート名**フィールドで選択されたレポートタイプに応じて、エンティティリストを含むウィンドウが表示されます。この例では、**LB仮想サーバーの選択**ウィンドウが表示されます。

     エンティティを追加(/en-us/netscaler-application-delivery-management-software/media/choose-lb-servers-entities.png)

     しきい値を設定するエンティティを選択します。**選択**をクリックします。選択したエンティティが**インスタンス**セクションに表示されます。

     **注**

     **特定のエンティティ**オプションは、**レポート名**でvserverベースのレポートを選択した場合にのみ表示されます。たとえば、**LBサービス統計**を選択した場合などです。

5. **イベントメッセージ**を追加することもできます。しきい値に達したときに表示したいメッセージを入力します。NetScaler Consoleは、監視対象の値としきい値をこのメッセージに追加します。
6. アラームを生成するしきい値を有効にするには、**有効にする**を選択します。
7. 任意で、メールまたはSlack通知、あるいはメールとSlackの両方の通知などの**アクション**を設定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. **作成**をクリックします。

### ネットワークレポートのパフォーマンスポーリング間隔を設定する

デフォルトでは、5分ごとにNITRO呼び出しがネットワークレポートのパフォーマンスデータを収集します。NetScaler Consoleは、カウンター情報などのインスタンス統計を取得し、1分ごと、1時間ごと、1日ごと、または1週間ごとに集計します。この集計データは、事前定義されたレポートで表示できます。

パフォーマンスポーリング間隔を設定するには、**インフラストラクチャ > ネットワークレポート**に移動し、**ポーリング間隔の構成**をクリックします。ポーリング間隔は5分未満または60分を超えることはできません。



### ネットワークレポートのプルーニング設定

NetScaler Consoleでネットワークレポートデータのパージ間隔を設定できます。この設定により、NetScaler Consoleサーバーのデータベースに保存されるネットワークレポートデータの量が制限されます。デフォルトでは、ネットワークレポートの履歴データは24時間ごと（01:00）にプルーニングされます。

**注**

指定できる値は、30日を超えることも、1日未満にすることもできません。

## 構成ジョブ

NetScaler Application Delivery Management (NetScaler Console) の構成管理プロセスは、ネットワーク内の複数のCitrix NetScalerインスタンス全体で、構成変更の適切なレプリケーション、システムアップグレード、およびその他のメンテナンスアクティビティを保証します。

NetScaler Consoleでは、複数のデバイスでこれらすべての活動を単一のタスクとして簡単に実行できる構成ジョブを作成できます。構成ジョブとテンプレートは、NetScaler Consoleで最も反復的な管理タスクを単一のタスクに簡素化します。構成ジョブには、1つまたは複数の管理対象デバイスで実行できる一連の構成コマンドが含まれています。

構成ジョブは、SSHコマンドを使用して構成コマンドを実行するか、SCPを使用してローカルから、あるいは別の機器にファイルをコピーできます。たとえば、HAフェイルオーバーやHAアップグレードをスケジュールできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注：**

アップグレードのために任意の数のNetScalerインスタンスを選択できますが、NetScaler Consoleオンプレミスは、最大40の同時アップグレードスレッドをサポートします。これは、同時にアップグレードできるインスタンスが40のみであることを意味します。

NetScaler Consoleで、次の4つのオプションのいずれかを使用して構成ジョブを作成できます。これらのいずれかを使用して、構成ジョブを実行するためのコマンドと指示の再利用可能なソースを作成します。

1. 構成テンプレート
2. インスタンス
3. ファイル
4. 記録と再生

## 構成テンプレート

ジョブの作成中に構成テンプレートを作成し、一連の構成コマンドをテンプレートとして保存できます。これらのテンプレートをページに保存すると、ページに自動的に表示されます。

**注** デフォルトの構成テンプレートでは、**名前の変更**オプションは無効になっています。ただし、カスタム構成テンプレートの名前を変更できます。

次のいずれかのテンプレートを使用できます。

**構成エディター**：構成エディターを使用してCLIコマンドを入力し、構成をテンプレートとして保存し、ジョブの構成に使用できます。

**組み込みテンプレート**：構成テンプレートのリストから選択できます。これらのテンプレートはCLIコマンドの構文を提供し、変数に値を指定できます。組み込みテンプレートは、以下の表に説明とともにリストされています。組み込みテンプレートオプションを使用してジョブをスケジュールできます。ジョブとは、1つ以上の管理対象インスタンスで実行できる構成コマンドのセットです。たとえば、組み込みテンプレートオプションを使用して、syslogサーバーを構成するジョブをスケジュールできます。また、ジョブをすぐに実行するか、後で実行するようにスケジュールすることもできます。

## インスタンス

NetScalerリリース11.0以降を実行しているNetScaler SDXインスタンスのシングルバンドルアップグレードを実行できます。シングルバンドルアップグレードを実行するには、NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consoleの組み込みタスクを使用します。また、実行中の構成または保存された構成を抽出し、同じタイプの別のNetScalerインスタンスでコマンドを実行することで、NetScalerインスタンスをアップグレードすることもできます。これにより、あるインスタンスの構成を別のインスタンスに複製できます。

## ファイル

ローカルマシンから構成ファイルをアップロードしてジョブを作成できます。

ファイルを使用する利点

- 任意のテキストファイルを使用して、再利用可能な構成コマンドのソースを作成できます。
- いかなる種類の書式設定も不要です。
- ファイルはローカルマシンに保存できます。

新しいファイルを作成して保存するか、既存のファイルをインポートしてコマンドを実行できます。

## 記録と再生

ジョブの作成機能を使用すると、独自のCLIコマンドを入力するか、記録と再生ボタンを使用してNetScalerセッションからコマンドを取得できます。ジョブを実行すると、選択したインスタンスのns.confへの変更が記録され、NetScaler Consoleにコピーされます。

### 関連情報

- 構成ジョブでSCP (put) コマンドを使用する方法
- 構成ジョブで変数を使用する方法
- 修正コマンドから構成ジョブを作成する方法
- 構成テンプレートを使用して監査テンプレートを作成する方法
- 記録と再生を使用して構成ジョブを作成する方法
- NetScaler Consoleでマスター構成テンプレートを使用する方法

## 構成ジョブの作成

ジョブとは、1つまたは複数の管理対象インスタンスで作成および実行できる一連の構成コマンドです。インスタンス全体で構成変更を行うジョブを作成したり、ネットワーク上の複数のインスタンスで構成を複製したり、NetScaler Console GUIを使用して構成タスクを記録および再生してCLIコマンドに変換したりできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleの構成ジョブ機能を使用して、構成ジョブを作成し、電子メール通知を送信し、作成されたジョブの実行ログを確認できます。

**NetScaler Consoleで構成ジョブを作成するには:**

1. **インフラストラクチャ > 構成 > 構成ジョブ** に移動します。
2. **Create Job** をクリックします。
3. **Create Job** ページの **Select Configuration** タブで、ジョブ名を指定し、リストから **Instance Type** を選択します。
4. **Configuration Source** リストで、作成する構成ジョブテンプレートを選択します。選択したテンプレートのコマンドを追加します。

    - コマンドを入力するか、保存されている構成テンプレートから既存のコマンドをインポートできます。
    - 構成ジョブでジョブを作成する際に、構成エディターで異なる種類の複数のテンプレートを追加することもできます。
    - **Configuration Source** リストから、異なるテンプレートを選択し、それらのテンプレートを構成エディターにドラッグします。テンプレートの種類は、**Configuration Template**、**In built Template**、**Master Configuration**、**Record and Play**、**Instance**、**File** です。

    **注**

    `Deploy Master Configuration Job` テンプレートを初めて追加し、その後異なる種類のテンプレートを追加すると、ジョブテンプレート全体が `Master Configuration` タイプになります。

    構成エディターでコマンドを並べ替えたり、順序を変更したりすることもできます。コマンド行をドラッグアンドドロップすることで、ある行から別の行にコマンドを移動できます。また、テキストボックスのコマンド行番号を変更するだけで、ある行から任意のターゲット行にコマンド行を移動または並べ替えることもできます。構成ジョブの編集中にコマンド行を並べ替えたり、順序を変更したりすることもできます。

    これらのパラメータに異なる値を割り当てたり、複数のインスタンスでジョブを実行したりできる変数を定義できます。構成ジョブの作成または編集時に定義したすべての変数を、統合された単一のビューで確認できます。**Preview Variables** タブをクリックすると、構成ジョブの作成または編集時に定義した変数を統合された単一のビューでプレビューできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成エディターのすべてのコマンドに対して、ロールバックコマンドをカスタマイズできます。カスタマイズしたコマンドを指定するには、カスタムロールバックオプションを有効にします。

**重要**

カスタムロールバックを有効にするには、**ジョブの作成**ウィザードを完了します。そして、**実行**タブで、**コマンド失敗時**リストから**成功したコマンドをロールバック**オプションを選択します。

5. **インスタンスの選択**タブで、構成監査を実行するインスタンスを選択します。
   a. NetScalerの高可用性ペアでは、プライマリノードまたはセカンダリノードで構成ジョブを実行できます。ジョブを実行するノードを選択します。
      - **プライマリノードで実行** - このオプションを選択すると、ジョブはプライマリノードでのみ実行されます。
      - **セカンダリノードで実行** - このオプションを選択すると、ジョブはセカンダリノードでのみ実行されます。

      同じ構成ジョブを実行するために、プライマリノードとセカンダリノードの両方を選択することもできます。プライマリノードまたはセカンダリノードのいずれも選択しない場合、構成ジョブは自動的にプライマリノードで実行されます。
6. **変数値を指定**タブには、2つのオプションがあります。
   a. 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。
   b. すべてのインスタンスに対して定義した変数に共通の値を入力します
   c. **次へ**をクリックします。

**ジョブのメールおよびSlack通知を送信するには:**

ジョブが実行またはスケジュールされるたびに、メールとSlack通知が送信されるようになりました。通知には、ジョブの成功または失敗などの詳細と、関連する詳細が含まれます。

1. **インフラストラクチャ > 構成 > 構成ジョブ**に移動します。
2. メールとSlack通知を有効にしたいジョブを選択し、**編集**をクリックします。
3. **実行**タブで、**実行レポートの受信方法**ペインに移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **メール**チェックボックスを選択し、実行レポートを送信したいメール配布リストを選択します。

  メール配布リストを追加したい場合は、**追加**をクリックし、メールサーバーの詳細を指定します。
- **Slack**チェックボックスを選択し、実行レポートを送信したいSlackチャンネルを選択します。

  Slackプロファイルを追加したい場合は、**追加**をクリックし、必要なSlackチャンネルの**プロファイル名、チャンネル名、トークン**を指定します。

  Slackプロファイル(/en-us/netscaler-application-delivery-management-software/media/configjobemail-slack-added.png)

4. **完了**をクリックします。

**ジョブのメールおよびSlack通知を送信するには：**

ジョブが実行またはスケジュールされるたびに、メールとSlack通知が送信されるようになりました。通知には、ジョブの成功または失敗などの詳細と関連情報が含まれます。

1. **インフラストラクチャ > 構成 > 構成ジョブ**に移動します。
2. メールとSlack通知を有効にしたいジョブを選択し、**編集**をクリックします。
3. **実行**タブで、**実行レポートの受信方法**ペインに移動します。

   - **メール**チェックボックスを選択し、実行レポートを送信したいメール配布リストを選択します。

     メール配布リストを追加したい場合は、**追加**をクリックし、メールサーバーの詳細を指定します。
   - 「**Slack**」チェックボックスを選択し、実行レポートを送信するSlackチャネルを選択します。

     Slackプロファイルを追加する場合は、「**追加**」をクリックし、必要なSlackチャネルの「**プロファイル名**」、「**チャネル名**」、および「**トークン**」を指定します。

4. 「**完了**」をクリックします。

**実行サマリーの詳細を表示するには：**

1. 「**インフラストラクチャ > 構成 > 構成ジョブ**」に移動します。
2. 実行サマリーを表示するジョブを選択し、「**詳細**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「**実行サマリー**」をクリックして、以下を表示します。

   - ジョブを実行したインスタンスのステータス
   - ジョブで実行されたコマンド
   - ジョブの開始時刻と終了時刻、および
   - インスタンスユーザーの名前

   「サマリー」(/en-us/netscaler-application-delivery-management-software/media/instanceuser.png)

## 記録と再生を使用して構成ジョブを作成する

NetScaler GUIを使用してNetScalerインスタンスを構成することに慣れている場合、構成タスクを作成し、複数のNetScalerインスタンスで実行するための正確なCLIコマンドを思い出すのが難しいと感じることがあります。

NetScaler Consoleを使用すると、NetScalerインスタンスのGUIを使用して実行された構成タスクを記録し、CLIコマンドに変換できます。その後、これらのCLIコマンドから構成タスクを作成し、このタスクを複数のインスタンスで実行できます。

### GUI構成を記録して構成タスクに変換するには

1. **Infrastructure > Configuration Jobs** に移動し、**Create Job** をクリックします。
2. ジョブ名とインスタンスの種類を指定します。
3. **Configuration Source** リストから **Record and Play** を選択し、構成を記録するソースインスタンスを選択します。**Record** をクリックします。

   GUI構成を記録(/en-us/netscaler-application-delivery-management-software/media/createjob_record1.png)
4. **NetScaler GUI** が開きます。構成タスクに含める機能と設定を構成します。その後、NetScaler GUIウィンドウを閉じ、**Configuration Editor** で **Stop** をクリックします。コマンドは左ペインにリンクとして表示されます。コマンドを右ペインにドラッグし、**Next** をクリックします。

   その後、必要に応じて構成エディターでコマンドを並べ替えたり、順序を変更したりできます。コマンド行をドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。また、テキストボックスのコマンド行番号を変更するだけで、コマンド行をある行から任意のターゲット行に移動または再配置することもできます。
5. 構成ジョブの作成中または編集中に定義したすべての変数を、統合された単一のビューでレビューできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 統合された単一のビューですべての変数を表示するには、次のいずれかを実行します。

   - 構成ジョブの作成中に、**Infrastructure > Configuration Jobs** に移動し、**Create Job** を選択します。**Create Job** ページで、構成ジョブの作成中に追加したすべての変数をレビューできます。
   - 構成ジョブの編集中に、**Network \> Configuration Jobs** に移動し、ジョブ名を選択して **Edit** をクリックします。**Configure Job** ページで、構成ジョブの作成中に追加されたすべての変数をレビューできます。

7. その後、**Preview Variables** タブをクリックして、構成ジョブの作成中または編集中に定義した変数を統合された単一のビューでプレビューできます。
8. 新しいポップアップウィンドウが表示され、Name、Display Name、Type、default valueなどの変数のすべてのパラメータが表形式で表示されます。これらのパラメータを編集および変更することもできます。いずれかのパラメータを編集または変更した後、**Done**ボタンをクリックします。

   

9. **Add Instances**をクリックし、構成ジョブを実行するインスタンスを選択します。**OK**をクリックし、次に**Next**をクリックします。

   

10. コマンドで変数を指定した場合は、**Specify Variable Values**タブで、インスタンスの変数を指定するために次のいずれかのオプションを選択します。

    - **変数値の入力ファイルをアップロード: Download Input Key** Fileをクリックして入力ファイルをダウンロードします。入力ファイルに、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。
    - **すべてのインスタンスに共通の変数**: 変数の値を入力します。変数は選択したテンプレートによって異なります。

    変数値を含む入力ファイルは、構成ジョブに (同じファイル名で) 保持されます。構成ジョブの作成または編集時に以前使用およびアップロードしたこれらの入力ファイルを表示および編集できます。

    構成ジョブの作成中に実行構成ジョブを表示するには、**Network \> Configuration Jobs**に移動し、**Create Job**をクリックします。**Create Job**ページで、**Specify Variable Values**タブの**Common Variable Values for all Instances**オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してアップロードします (同じファイル名を保持します)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ジョブの編集中に既に実行された構成ジョブを表示するには、**Network \> Configuration Jobs**に移動し、ジョブ名を選択して**Edit**をクリックします。**Configure Job**ページで、**Specify Variable Values**タブの**Common Variable Values for all Instances**オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してアップロードします (同じファイル名を保持します)。10. **Job Preview**タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。

11. **Job Preview**タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
12. **Execute**タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合にNetScaler Consoleが実行するアクションを選択することもできます。

    承認されたユーザーが管理対象インスタンスでジョブを実行できるように選択することもできます。また、ジョブの成功または失敗に関する電子メール通知を、その他の詳細とともに送信するかどうかを選択することもできます。

    
13. **Jobs**ページで、すべてのインスタンスでの構成タスク実行の進行状況を表示できます。

## 構成ジョブを使用して、あるインスタンスから複数のインスタンスに構成をレプリケートする

NetScaler Console の構成ジョブ機能を使用すると、NetScaler インスタンスから特定の構成を抽出し、複数のインスタンスにレプリケートできます。

たとえば、展開のために NetScaler インスタンスで負荷分散とフロントエンド最適化 (FEO) の両方を構成したとします。しかし、今では FEO 構成のみを他の NetScaler インスタンスにレプリケートしたいと考えています。

**あるインスタンスから他の NetScaler インスタンスに構成を取得してレプリケートするには:**

1. **>** の順に移動し、 をクリックします。
2. ジョブ名とインスタンスのタイプを指定します。
3. として を選択し、構成をレプリケートするソースインスタンスを選択します。抽出する構成のタイプを選択します。「Configuration by time duration」を選択した場合は、この構成を実行した期間を設定し、 をクリックします。

   選択した期間にそのインスタンスで実行されたコマンドの数が、次の画像で強調表示されているように画面に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. コマンドを右ペインの フィールドにドラッグします。

   FEO に関連するコマンドのみを保持し、負荷分散に関連するコマンド、またはその他の構成に関連するコマンドを手動で削除してから、 をクリックします。

5. をクリックし、FEO 構成を適用するインスタンスを追加します。 をクリックし、 をクリックします。
6. コマンドに変数を指定した場合は、 タブで をクリックします。ダウンロードしたファイルで変数の値を指定し、ファイルを NetScaler Console にアップロードします。
7. タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
8. 「**Execute**」タブで、「**Finish**」をクリックして、選択したNetScalerインスタンスでジョブを実行します。

### 構成ジョブで変数を使用する

構成ジョブとは、1つ以上の管理対象インスタンスで実行できる一連の構成コマンドです。複数のインスタンスで同じ構成を実行する場合、構成で使用されるパラメーターに異なる値を使用したい場合があります。これらのパラメーターに異なる値を割り当てたり、複数のインスタンスでジョブを実行したりできる変数を定義できます。

たとえば、ロードバランシング仮想サーバーを追加し、2つのサービスを追加し、そのサービスを仮想サーバーにバインドする基本的なロードバランシング構成を考えてみましょう。ここで、2つのインスタンスで同じ構成を持ちたいが、仮想サーバーとサービスの名前およびIPアドレスには異なる値を使用したい場合があります。構成ジョブ機能を使用すると、変数を使用して仮想サーバーとサービスの名前およびIPアドレスを定義することで、これを実現できます。

この例では、次のコマンドと変数が使用されています。

```
add lb vserver <servername> HTTP <ipaddress> <portnumber>
```

```
add service <servicename1> <ipaddress1> HTTP 80
```

```
add service <servicename2> <ipaddress2> HTTP 80
```

```
bind lb vserver <servername> <servicename1>
```

```
bind lb vserver <servername> <servicename2>
```

#### NetScaler Consoleで変数を定義して構成ジョブを作成するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Infrastructure > Configuration Jobs** に移動します。
2. **Create Job** をクリックします。
3. **Create Job** ページで、ジョブ名、インスタンスタイプ、構成タイプなどのカスタムジョブパラメーターを選択します。
4. 構成エディターで、ロードバランシング仮想サーバーを追加し、2つのサービスを追加し、そのサービスを仮想サーバーにバインドするコマンドを入力します。変数に変換したい値をダブルクリックして選択し、**Convert to Variable** をクリックします。たとえば、ロードバランシングサーバーのIPアドレス `*ipaddress*` を選択し、**Convert to Variable** をクリックします。
5. 変数の値がドル記号で囲まれていることを確認したら、その変数をクリックして、名前、表示名、タイプなどの変数の詳細をさらに指定します。変数のデフォルト値をさらに指定したい場合は、**Advanced** オプションをクリックすることもできます。**Save** をクリックし、次に **Next** をクリックします。

   残りのコマンドを入力し、すべての変数を定義します。
6. 設定ジョブの作成中または編集中に定義したすべての変数を、統合された単一のビューで確認できます。
7. 統合された単一のビューですべての変数を表示するには、次のいずれかを実行します。

   - 設定ジョブの作成中に、**Infrastructure > Configuration Jobs** に移動し、**Create Job** を選択します。**Create Job** ページで、設定ジョブの作成中に追加したすべての変数を確認できます。
   - 設定ジョブの編集中に、**Network \> Configuration Jobs** に移動し、ジョブ名を選択して **Edit** をクリックします。**Configure Job** ページで、設定ジョブの作成中に追加されたすべての変数を確認できます。
8. その後、**Preview Variables** タブをクリックして、設定ジョブの作成中または編集中に定義した変数を統合された単一のビューでプレビューできます。
9. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメーターが表形式で表示されます。これらのパラメーターを編集および変更することもできます。いずれかのパラメーターを編集または変更した後、**Done** ボタンをクリックします。

   
10. その後、設定エディターでコマンドを適切に並べ替えたり、順序を変更したりできます。コマンド行をドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

また、テキストボックスのコマンド行番号を変更するだけで、コマンド行をある行から任意のターゲット行に移動または再配置することもできます。

11. 設定ジョブを実行するインスタンスを選択します。
12. **Specify Variable Values** タブで、**Upload input file for variable values** オプションを選択し、**Download Input Key File** をクリックします。この例では、各インスタンスのサーバー名、サーバーとサービスの IP アドレス、ポート番号、およびサービス名を指定する必要があります。ファイルを保存してアップロードします。値が正確に定義されていない場合、システムはエラーをスローする可能性があります。
13. 入力キーファイルはローカルシステムにダウンロードされ、以前に選択した各NetScalerインスタンスの変数値を指定して編集し、**Upload** をクリックして入力キーファイルをNetScaler Consoleにアップロードできます。**Next** をクリックします。入力キーファイルはローカルシステムにダウンロードされ、以前に選択した各NetScalerインスタンスの変数値を指定して編集できます。

**注**

. 入力キーファイルでは、変数は次の3つのレベルで定義されます。

- グローバルレベル
- インスタンスグループレベル
- インスタンスレベル

グローバル変数は、すべてのインスタンスに適用される変数値です。インスタンスグループレベルの変数値は、グループで定義されているすべてのインスタンスに適用されます。インスタンスレベルの変数値は、特定のインスタンスにのみ適用されます。

NetScaler Consoleは、インスタンスレベルの値に最優先順位を付けます。個々のインスタンスの変数に値が指定されていない場合、NetScaler Consoleはグループレベルで指定された値を使用します。グループレベルで値が指定されていない場合、NetScaler Consoleはグローバルレベルで指定された変数値を使用します。3つのすべてのレベルで変数に入力を指定した場合、NetScaler Consoleはインスタンスレベルの値をデフォルト値として使用します。

14. **アップロード**をクリックして、入力キーファイルをNetScaler Consoleにアップロードします。**次へ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要**

MacからCSVファイルをアップロードすると、MacはCSVファイルをコンマではなくセミコロンで保存します。これにより、入力ファイルをアップロードしてジョブを実行する際に、構成が失敗します。Macを使用している場合は、テキストエディターを使用して必要な変更を加えてからファイルをアップロードしてください。

15. すべてのインスタンスに共通の変数値を与え、**アップロード**をクリックして、入力キーファイルをNetScaler Consoleにアップロードすることもできます。

    変数値を含むキー入力ファイルは、構成ジョブに（同じファイル名で）保持されます。構成ジョブの作成または編集時に以前使用およびアップロードしたこれらの入力ファイルを表示および編集できます。

    構成ジョブの作成中に実行構成ジョブを表示するには、**ネットワーク \> 構成ジョブ**に移動し、**ジョブの作成**をクリックします。**ジョブの作成**ページで、**変数値の指定**タブで、**すべてのインスタンスの共通変数値**オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してから（同じファイル名を保持して）ファイルをアップロードします。

    構成ジョブの編集中に既に実行された構成ジョブを表示するには、**ネットワーク \> 構成ジョブ**に移動し、ジョブ名を選択して**編集**をクリックします。**ジョブの構成**ページで、**変数値の指定**タブで、**すべてのインスタンスの共通変数値**オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してから（同じファイル名を保持して）ファイルをアップロードします。

16. **ジョブプレビュー**タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。

17. **実行**タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。また、コマンドが失敗した場合にNetScaler Consoleが取るべきアクションや、ジョブの成功または失敗に関するメール通知を他の詳細とともに送信するかどうかも選択できます。

ジョブを構成して実行した後、**インフラストラクチャ > 構成ジョブ**に移動し、構成したばかりのジョブを選択することで、ジョブの詳細を表示できます。**詳細**をクリックし、次に**変数詳細**をクリックして、ジョブに追加された変数の一覧を表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

**STEP 5**で変数に指定した値は、ジョブを保存して終了したとき、または後で実行するようにジョブをスケジュールしたときに、NetScaler Consoleによって保持されます。

### 修正コマンドから構成ジョブを作成する

NetScaler Consoleの監査テンプレート機能を使用して、管理対象のNetScalerインスタンス全体の構成変更を監視し、構成エラーをトラブルシューティングできます。

監査テンプレートを使用した構成変更の監査の一般的なワークフローは、次のステップで構成されます。

1. インスタンス構成を監査するために、有効/期待されるNetScalerコマンドのセットを含む監査テンプレートを作成します。
2. 実行中の構成と期待される構成との間の違いを確認するために、監査テンプレートを実行するNetScalerインスタンスを選択します。
3. 差分/修正コマンドを理解し、「ジョブの作成」機能を利用して、インスタンスの構成を目的の状態にします。

複数の管理者が5つのNetScalerインスタンスを管理しているシナリオを考えてみましょう。これらの管理者はすべて、必要な変更があるたびに既存のインスタンス構成を更新します。スーパー管理者は、他の管理者によって行われる変更に関係なく、特定の重要な構成セットが変更されないままであることを確認したいと考えています。このユースケースでは、スーパー管理者はNetScalerインスタンスに存在すると予想される構成のテンプレートを作成し、それをインスタンスに対して実行します。NetScaler Consoleは、監査テンプレート構成を実行中の構成と比較し、不一致があれば**構成監査**ダッシュボードに報告します。

一部のインスタンスの構成に変更があることに気づいた場合、NetScaler Consoleの修正コマンド機能を使用して、特定のNetScalerインスタンス向けに変更および修正された構成コマンドを含む構成ジョブを作成できます。

監査テンプレート構成と実行中の構成の間に違いがある場合、**監査レポート**ページに**差分が存在します**というステータスメッセージが表示されます。**差分が存在します**リンクをクリックすると、**構成差分**ページに移動し、修正コマンドを表示できます。これらの修正コマンドを使用して構成ジョブを作成し、特定のNetScalerインスタンスで実行して、目的の構成に戻すこともできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NetScaler Consoleで修正コマンドから構成ジョブを作成するには**

1. **インフラストラクチャ > 構成監査**に移動します。
2. **構成監査**ページで、2つのドーナツチャートのいずれかをクリックして**監査レポート**ページにアクセスします。
3. 構成コマンドを修正したいインスタンスについて、**差分が存在します**リンク (テーブルの**保存済みと実行中の差分**列の下) をクリックします。そのインスタンスの保存済み構成、実行中の構成、および修正構成間の違いを一覧表示する**構成差分**ページが表示されます。

   構成の差分(/en-us/netscaler-application-delivery-management-software/media/auditreports.png)
4. **ジョブの作成**をクリックして**ジョブの作成**ページに移動します。このページには修正コマンドが事前に入力されています。構成ジョブの作成方法については、「NetScaler Consoleで構成ジョブを作成する方法」を参照してください。

## あるNetScalerインスタンスから別のインスタンスへ、実行中および保存済みの構成を複製する

May 24, 2018

NetScalerインスタンスの構成を他のインスタンスに複製できるようになりました。NetScaler Consoleでジョブを構成する際、インスタンスを構成ソースとして選択し、選択したインスタンスの実行中または保存済みの構成を選択します。

たとえば、**実行中の構成**を選択して**抽出**をクリックすると、NetScaler Consoleは選択したNetScalerインスタンスに実行中の構成を検索するリクエストを送信し、それをテンプレートとして表示します。テンプレートを右側のペインの**コマンド**フィールドにドラッグできます。コマンド、パラメータ、およびインスタンスを変更できます。

**NetScaler Consoleで、あるインスタンスの実行中および保存済みの構成コマンドを別のインスタンスに複製するには：**

1. **インフラストラクチャ > 構成ジョブ**に移動し、**ジョブの作成**をクリックします。
2. ジョブ名とインスタンスの種類を指定します。たとえば、ジョブ名として*NetScaler Running Config1*を、インスタンスの種類として*NetScaler*を指定します。
3. **インスタンス**を**構成ソース**として選択し、その構成を他のインスタンスに複製したいソースインスタンスを選択します。
4. 次の3つのオプションが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 実行中の構成
- 保存済みの構成
- 期間による構成

5. **実行中の構成**を選択し、**抽出**をクリックします。そのインスタンスで実行された実行中の構成コマンドの数が表示されます。

   実行中および保存済みの構成を複製する(/en-us/netscaler-application-delivery-management-software/media/replicate1.png)

6. 右ペインの**コマンド**フィールドにコマンドをドラッグします。
7. 「コマンド」フィールドでコマンドを編集できます。例えば、抽出されたコマンドがNetScalerインスタンスをセットアップするためのものである場合、パーティションの追加、ロードバランシングの設定、ロードバランシングサーバーとサービスとのバインドなどが含まれることがあります。新しいNetScalerインスタンスをパーティションなしでセットアップするために、コマンドを編集したい場合があります。そのため、パーティションを削除するには、パーティションの作成に関連するコマンドを手動で削除し、**次へ**をクリックします。
8. **インスタンスの追加**をクリックし、実行中の構成コマンドを適用するインスタンスを追加します。**OK**をクリックし、次に**次へ**をクリックします。
9. コマンドに変数を指定している場合は、**変数値の指定**タブで**入力キーファイルのダウンロード**をクリックします。ダウンロードしたファイルで変数に値を指定し、そのファイルをNetScaler Consoleにアップロードします。
10. **ジョブプレビュー**タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。

11\. **実行**タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合にNetScaler Consoleが実行するアクションや、ジョブの成功または失敗に関するメール通知をその他の詳細とともに送信するかどうかも選択できます。

### 実行済み構成ジョブを再利用する

構成ジョブを使用すると、1つ以上の管理対象インスタンスで実行できる構成コマンドのセットを作成できます。コマンド、パラメータ、構成ソース、およびジョブ内のインスタンスを変更した後、保存された構成ジョブの同じセットを再度実行することもできます。これは、同じコマンドセットを別のインスタンスで実行する必要がある場合、またはジョブがエラーに遭遇し、それ以上の実行を停止する場合に役立ちます。

NetScaler Consoleは、完了したジョブを再度実行する機能を提供します。この機能により、完全に実行されたジョブは、ジョブ名を変更せずに再度実行できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

実行モードが「今すぐ」である場合に実行されたジョブのみを再実行できます。

**完了したジョブを編集するには:**

1. NetScaler Consoleのホームページから、**インフラストラクチャ > 構成ジョブ**に移動します。
2. **ジョブ**ページで、実行サマリーが「完了」と表示されているジョブを選択し、**編集**をクリックします。スケジュールされた構成ジョブを編集することもできます。
3. **ジョブの構成**ページで、ジョブ名とインスタンスタイプが編集できないことがわかります。構成ソース、インスタンスの追加、変数値の編集、実行設定など、他のフィールドを変更できます。
4. **完了**をクリックして、構成ジョブを再度実行します。

**注**

ジョブを選択して**実行**を再度クリックすることもできます。これにより、ソース、インスタンス、およびコマンドを変更せずにジョブを実行できます。これは、同じインスタンスで同じコマンドセットを実行する必要がある場合に役立ちます。ジョブがサーバー側から一時的なエラーに遭遇する場合があります。その場合、ジョブを再度実行する必要があるかもしれません。

ジョブを実行する(/en-us/netscaler-application-delivery-management-software/media/executecompletedjob.png)

## 構成ジョブでSCP (put) コマンドを使用する

NetScaler Consoleの構成ジョブ機能を使用して、構成ジョブを作成し、電子メール通知を送信し、作成されたジョブの実行ログを確認できます。ジョブとは、単一の管理対象インスタンスまたは複数の管理対象インスタンスで作成および実行できる一連の構成コマンドです。たとえば、デバイスのアップグレードに構成ジョブを使用できます。

NetScaler Consoleの構成ジョブは、Secure Shell (SSH) コマンドを使用してインスタンスを構成します。構成ジョブを設定して、セキュアコピー (SCP) を使用してファイルを安全に転送できます。SCPはSSHプロトコルに基づいています。構成ジョブに含めることができる**SCP**コマンドの1つは、「put」コマンドです。「put」コマンドを構成ジョブで使用すると、システム上のローカルディレクトリに保存されている1つ以上のファイルをNetScaler Consoleにアップロードまたは転送し、その後NetScalerインスタンスのディレクトリに転送できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

ファイルはNetScaler Consoleにアップロードされ、その後選択されたNetScalerインスタンスにコピー（put）されます。アップロードされたファイルはNetScaler Consoleに保存され、ジョブが削除された場合にのみ削除されます。これは、後で実行するようにスケジュールされたジョブに必要です。

コマンドの構文は次のとおりです。

```
put <local_filename> <remote_path/remote_filename>
```

ここで、,

\<local_filename\> は、アップロードするローカルファイルの名前です。

\<remote_path / remote_filename\> は、リモートディレクトリへのパスと、そのディレクトリにコピーされたときにファイルに割り当てる名前です。

**注:**

リモートディレクトリにローカルファイルと同じ名前のファイルが含まれている場合、putコマンドはリモートファイルを上書きします。

構成ジョブの作成中に、ローカルおよびリモートファイル名のパラメータを変数に変換できます。これにより、ジョブを実行するたびに、同じNetScalerインスタンスのセットに対してこれらのパラメータに異なるファイルを割り当てることができます。また、ジョブ内の複数の場所でファイルを使用し、そのファイルの名前を変更したい場合は、すべての場所でファイル名を変更する代わりに、変数を再定義できます。

**構成ジョブでputコマンドを使用してファイルをアップロードするには:**

1. **Infrastructure > Configuration Jobs** に移動します。
2. **Jobs**ページで、**Create Job**をクリックします。
3. **Create Job**ページで、Job nameフィールドにジョブの名前を入力し、**Configuration Editor**ペインに「put」コマンドを入力します。

   たとえば、ローカルシステムに保存されているSSL証明書ファイルを複数のNetScalerインスタンスにコピーする構成ジョブを作成する場合、特定のファイル名の代わりに変数を使用する「put」コマンドを追加し、変数タイプを「file」として定義できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`put scp-file /nsconfig/scp-file`

この例では、,

- `scp-file` - これは、NetScalerインスタンスにアップロードする必要があるファイルの名前です。
- `/nsconfig/scp-file` - これは、タスクの実行後に`scp-file`が配置されるインスタンス上の宛先フォルダです。

4. 入力したコマンドで、変数に変換するファイル名を選択し、次の図に示すように**Convert to Variable**をクリックします。

   (/en-us/netscaler-application-delivery-management-software/media/configjobs-put-command1.png)

5. ファイル名がドル記号で囲まれていること（変数になったことを示す）を確認し、変数をクリックします。
6. 名前、表示名、タイプなど、変数の詳細を指定します。
7. **Type**ドロップダウンリストから**File**を選択します。**Save**をクリックします。変数を「File」タイプとして宣言すると、NetScaler Consoleにファイルをアップロードできます。

   (/en-us/netscaler-application-delivery-management-software/media/configjobs-put-command2.png)

8. **Next**をクリックし、ファイルをコピーするNetScalerインスタンスを選択します。
9. **Specify Variable Values**タブで、**Common Variables Values for all Instances**セクションを選択し、システム上のローカルストレージからファイルを選択し、**Upload**をクリックしてNetScaler Consoleにファイルをアップロードし、**Next**をクリックします。

   

10. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
11. 「**実行**」タブで、ジョブを今すぐ実行するか、後で実行するようにスケジュールできます。コマンドが失敗した場合にNetScaler Consoleが実行すべきアクションを選択することもできます。ジョブの成功または失敗、およびその他の詳細に関する通知を受け取るための電子メール通知を作成することもできます。「**完了**」をクリックします。
12. 「**インフラストラクチャ > 構成ジョブ**」に移動し、設定したジョブを選択することで、ジョブの詳細を表示できます。「**詳細**」をクリックし、次に「**変数詳細**」をクリックして、ジョブに追加された変数を一覧表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 構成テンプレートを使用する

構成テンプレートを使用すると、一連の構成コマンドを保存して再利用できるため、NetScalerインスタンス全体に一貫した構成を適用できます。以下のトピックは、構成テンプレートの作成と管理に役立ちます。

- マスター構成テンプレートを使用する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/use-master-configuration-template.html)
- 組み込みテンプレートを使用して作成されたジョブをスケジュールする(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-schedule-jobs-created-using-built-in-templates.html)
- NetScalerからPrometheusへのメトリクスエクスポートを構成するジョブをスケジュールする(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/built-in-template-prometheus-export.html)
- 構成テンプレートを使用して監査テンプレートを作成する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/use-configuration-templates-to-create-audit-templates.html)
- 組み込みテンプレートを使用して構成されたジョブを再スケジュールする(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reschedule-jobs.html)
- 構成ジョブで構成監査テンプレートを再利用する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reuse-configuration-audit-templates.html)
- 構成テンプレートのインポートとエクスポート(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-import-and-export-configuration-templates.html)

## マスター構成テンプレートを使用する

メイン構成テンプレートを使用すると、複数のNetScalerインスタンスにマスター構成を作成および展開するための柔軟なオプションが得られます。

管理者として、NetScalerインスタンスで構成変更を行い、ライセンス、証明書、その他のファイルを保存したい場合があります。新しい構成は、マスター構成テンプレート（.confファイル）として保存できます。

NetScalerインスタンスからマスター構成テンプレートを保存するには、次のいずれかの操作を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- コマンドプロンプトで「**save ns config**」と入力します。構成は、インスタンスのFLASHメモリ内の/nsconfig/ns.confファイルに保存されます。
- インスタンスのGUIから、**Diagnostics** \> **View Configuration** に移動します。保存したい構成の種類を選択します。たとえば、インスタンスの保存済み構成を保存したい場合は、**Saved configuratio**n を選択します。「**Save text to a file**」リンクをクリックして、「ns.conf」ファイルをローカルマシンに保存します。

ジョブの作成時に「DeployMasterConfiguration」構成テンプレートを使用してマスター構成テンプレートを展開する場合、コマンドを追加したり、既存のコマンドを変更したり、入力ファイルに異なる変数値を指定したりすることで、特定のNetScalerインスタンスごとにさらにカスタマイズできます。

たとえば、管理者として、ns.confファイルに加えて証明書キーをNetScalerインスタンスにアップロードし、それらにマスター構成を展開したい場合があります。

**重要**

DeployMasterConfigurationテンプレートを使用する構成ジョブは、NetScaler CPXインスタンス、クラスターで構成されたインスタンス、またはパーティション化されたNetScalerインスタンスでは実行できません。

**NetScaler Consoleでマスター構成テンプレートを使用して構成ジョブを作成するには：**

1. NetScaler Consoleで、**Infrastructure > Configuration Jobs** に移動し、**Create Job** をクリックします。
2. **Create Job** ページの**Select Configuration**タブで、**Job Name** を指定し、ドロップダウンリストから**Instance Type** を選択します。
3. **Configuration Source** ドロップダウンリストから**Master Configuration** を選択します。DeployMasterConfigurationテンプレートのコマンドを右ペインにドラッグします。右ペインでコマンドを追加、変更、または削除することもできます。**Next** をクリックします。

   **注**

   テンプレートに入力ファイルを追加するには、***put*** コマンドを追加できます。この例では、構成テンプレートファイルと変数入力ファイルに加えて、証明書ファイルとキーファイルをアップロードする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

入力ファイルの追加(/en-us/netscaler-application-delivery-management-software/media/master-config.png)

4. 構成ジョブの作成または編集時に定義したすべての変数を、統合された単一のビューで確認できます。
5. すべての変数を統合された単一のビューで表示するには、次のいずれかを実行します。

   - 構成ジョブの作成中に、**Infrastructure > Configuration Jobs** に移動し、**Create Job** を選択します。**Create Job** ページで、構成ジョブの作成中に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、**Network \> Configuration Jobs** に移動し、ジョブ名を選択して **Edit** をクリックします。**Configure Job** ページで、構成ジョブの作成中に追加されたすべての変数を確認できます。

6. その後、**Preview Variables** タブをクリックして、構成ジョブの作成または編集時に定義した変数を統合された単一のビューでプレビューできます。

   変数のプレビュー(/en-us/netscaler-application-delivery-management-software/media/master-config-preview.png)

7. 新しいポップアップウィンドウが表示され、名前、表示名、タイプ、デフォルト値などの変数のすべてのパラメーターが表形式で表示されます。これらのパラメーターを編集および変更することもできます。いずれかのパラメーターを編集または変更した後、**Done** ボタンをクリックします。

   パラメーターの編集(/en-us/netscaler-application-delivery-management-software/media/master-config-preview-1.png)

8. 構成ジョブを実行するインスタンスを選択し、**Next** をクリックします。
9. **Specify Variable Values** タブで、以下をアップロードします。

   - **構成テンプレートファイル (.conf)** - NetScaler インスタンスから抽出した .conf ファイルをアップロードします。
   - **入力ファイル (.xml/csv) のアップロード** - コマンドで定義した変数の値を含む入力ファイルをアップロードします。

   使用のためにサンプル XML ファイルがここに提供されています。XML ファイルに、使用している NetScaler インスタンスに対応する詳細が含まれていることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
parameters and values.

If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence over the
instance group. The instance group specific parameters value will take
precedence over global parameters in the execution.

-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters and
value.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence in the
execution.



-  name. This attribute represents the IP Address of the instance. Host
name is not supported for the attibute.



HA pair should be represented as <primaryip>-<secondaryip>. Example
10.102.2.1-10.102.2.2



In the template file, the parameter name must be specified within the
dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters names are
case sensitive.

-->



<global>



</global>

<devicegroup name="BLR_DEVS">

</devicegroup>

<device name="10.106.101.209">

<param name="IP" value="10.106.101.209"/>

</device>



<!-- HA PAIR-->
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<!--<device name="10.102.43.154-10.102.43.155">

<param name="NSIP" value="10.102.43.154"/>

<param name="HostName" value="NS43HA"/>

<param name="LBSERVER" value="haserver43http"/>

<param name="SNMPTrapDest" value="10.102.43.130"/>

</device>-->

</properties>
```

10. 「**次へ**」をクリックします。

ファイルのアップロード(/en-us/netscaler-application-delivery-management-software/media/master-config-create-newpng.png)

変数を含む入力ファイルは、構成ジョブに（同じファイル名で）保持されます。構成ジョブの作成または編集時に以前使用およびアップロードしたこれらの入力ファイルを表示および編集できます。

構成ジョブの作成中に実行された構成ジョブを表示するには、**Network \> Configuration Jobs** に移動し、**Create Job** をクリックします。**Create Job** ページで、**Specify Variable Values** タブで **Common Variable Values for all Instances** オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してファイルをアップロードします（同じファイル名を維持します）。

構成ジョブの編集中にすでに実行された構成ジョブを表示するには、**Network \> Configuration Jobs** に移動し、ジョブ名を選択して **Edit** をクリックします。**Configure Job** ページで、**Specify Variable Values** タブで **Common Variable Values for all Instances** オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してファイルをアップロードします（同じファイル名を維持します）。

1. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証し、「**次へ**」をクリックできます。

   ジョブプレビュー(/en-us/netscaler-application-delivery-management-software/media/dmc4.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 「**実行**」タブで、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合にNetScaler Consoleが実行するアクションを選択することもできます。

   承認されたユーザーが管理対象インスタンスでジョブを実行することを許可することも選択でき、ジョブの成功または失敗に関する電子メール通知を他の詳細とともに送信するかどうかを選択できます。

   ジョブの実行(/en-us/netscaler-application-delivery-management-software/media/dmc5.png)

ジョブを実行した後、**Infrastructure > Configuration Jobs** に移動し、構成したジョブを選択することで、ジョブの詳細を確認できます。**Details** をクリックし、次に **Execution Summary** をクリックしてジョブの詳細を確認します。インスタンスをクリックして **Command Logs** を表示し、ジョブで実行されたコマンドを確認します。

コマンドログの表示(/en-us/netscaler-application-delivery-management-software/media/dmc6.png)

## 組み込みテンプレートを使用して作成されたジョブをスケジュールする

組み込みテンプレートオプションを使用してジョブをスケジュールできます。ジョブとは、1つ以上の管理対象インスタンスで実行できる構成コマンドのセットです。たとえば、組み込みテンプレートオプションを使用して、syslogサーバーを構成するジョブをスケジュールできます。ジョブをすぐに実行するか、後で実行するようにスケジュールすることもできます。

### NetScaler Consoleで組み込みテンプレートを使用してジョブをスケジュールするには

1. NetScaler Consoleで、**Infrastructure > Configuration Jobs** に移動し、**Create Job** をクリックします。
2. **Create Job** ページの **Select Configuration** タブで、**Job Name** を指定し、ドロップダウンリストから **Instance Type** を選択します。
3. **Configuration Source** ドロップダウンリストから **Inbuilt Template** を選択します。
   ***NSConfigureSyslogServer** コマンドを右ペインにドラッグし、**Next** をクリックします。

   組み込みテンプレートを使用する(/en-us/netscaler-application-delivery-management-software/media/createjobinbuilttemp1.png)
4. **Select Instances** タブで、**Add Instances** をクリックし、ジョブを実行するインスタンスを選択して、**OK** をクリックします。
5. **Next** をクリックします。**Specify Variable Values** タブで、インスタンスの変数を指定するために、次のいずれかのオプションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **入力ファイルからの変数値** - 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力します。その後、ファイルをNetScaler Consoleサーバーにアップロードします。
- **すべてのインスタンスに共通の変数値** – syslogサーバーのIPアドレスとポートを指定します。

6. **Job Preview** タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
7. **Next** をクリックします。
8. **Execute** タブで、次の条件を設定します。

   - **コマンド失敗時** - コマンドが失敗した場合、エラーを無視してジョブの実行を続行するか、ジョブのそれ以上の実行を停止するかを選択できます。ドロップダウンリストから実行したいアクションを選択します。
   - **実行モード** - ジョブを今すぐ実行するか、後で実行するようにスケジュールできます。ジョブを後でスケジュールする場合は、そのジョブの実行頻度設定を指定する必要があります。ドロップダウンリストから、ジョブに適用するスケジュールを選択します。

9. **実行設定**で必要な方法を選択することで、一連のインスタンスでジョブを順次または並行して実行することもできます。いずれかのインスタンスでジョブの実行が失敗した場合、残りのインスタンスでは続行されません。

   承認されたユーザーが管理対象インスタンスでジョブを実行できるように選択できます。ジョブの成功または失敗に関する電子メール通知も、その他の詳細とともに送信できます。

10. **完了**をクリックします。

### NetScalerからPrometheusへのメトリクスエクスポートを設定するジョブをスケジュールする

`NSConfigurePrometheusAnalyticsProfile`テンプレートを使用すると、デフォルトスキーマまたは変更されたパラメータを持つカスタムスキーマのいずれかを使用し、すべての管理対象インスタンスに対してジョブを実行できます。

#### 前提条件

管理対象のNetScalerが**13.1 build 39-27以降**であることを確認してください。

#### ジョブをスケジュールするには：

1. NetScaler Consoleで、**Infrastructure > Configuration > Configuration Jobs**に移動し、**Create Job**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Create Job**ページで、ジョブの名前を指定し、**Instance Type**リストから**NetScaler**を選択します。
3. **Configuration Source**リストから**Inbuilt Template**を選択します。*NSConfigurePrometheusAnalyticsProfile*コマンドを右ペインにドラッグし、**Next**をクリックします。**+**をクリックしてテンプレートを追加することもできます。

   

4. デフォルトスキーマで続行する場合は：

   a. ステップ3 (`put $Schema_file /var/metrics.conf/$schema_filename$`) を削除します。マウスカーソルをステップ3に置き、次のようにします：

      - Windowsでは、Control + Aを押してからDeleteを押します。
      - Macでは、Command + Aを押してからDeleteを押します。

   b. 削除後、**Next**をクリックします。

   c. **Select Instances**タブで、**Add Instances**をクリックし、ジョブを実行するインスタンスを選択して、**Next**をクリックします。

   d. 「**変数値を指定**」タブで、「**すべてのインスタンスの共通変数値**」を選択します。

      - **Analytics TimeSeries プロファイル名** - 分析プロファイル名を指定します。詳細については、`https://docs.netscaler.com/ja-jp/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`を参照してください。
      - **NetScalerにアップロードするスキーマファイル名** - このファイル名をデフォルトファイルである`schema.json`として保持します。

        

   e. ステップ6から先に進みます。

5. カスタムスキーマカウンターで続行する場合は、次の手順を実行します。

   a. 「**構成ソース**」リストから「**組み込みテンプレート**」を選択します。`NSConfigurePrometheusAnalyticsProfile`コマンドを右ペインにドラッグし、「**次へ**」をクリックします。+をクリックしてテンプレートを追加することもできます。

   b. 「**インスタンスの選択**」タブで、「**インスタンスの追加**」をクリックし、ジョブを実行するインスタンスを選択して、「**次へ**」をクリックします。

   c. 「**変数値を指定**」タブで、「**すべてのインスタンスの共通変数値**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScalerカウンタースキーマファイル(.json)** - パラメータで変更したスキーマファイルを選択します。NetScalerでは、サポートされているすべてのカウンターを含む参照ファイル`reference_schema.json`がパス`/var/metrics_conf/`の下にあります。

  FTPクライアントを使用してファイルをローカルにコピーし、必要なパラメータを編集して保存し、アップロードできます。

- **NetScalerにアップロードするスキーマファイル名** - NetScalerにアップロードするスキーマファイル名を指定します。
- **Analytics TimeSeries プロファイル名** - 分析プロファイル名を指定します。詳細については、`https://docs.netscaler.com/ja-jp/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`を参照してください。

6. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
7. 「**次へ**」をクリックします。
8. 「**実行**」タブで、次の条件を設定します。

   - **コマンド失敗時** - コマンドが失敗した場合、エラーを無視してジョブの実行を続行するか、ジョブのそれ以上の実行を停止するかを選択できます。ドロップダウンリストから実行するアクションを選択します。
   - **実行モード** - ジョブを今すぐ実行するか、後で実行するようにスケジュールできます。ジョブを後でスケジュールする場合は、そのジョブの実行頻度設定を指定する必要があります。ドロップダウンリストから、ジョブに適用するスケジュールを選択します。

9. また、「**実行設定**」で必要な方法を選択することにより、一連のインスタンスでジョブを順次または並行して実行することもできます。いずれかのインスタンスでジョブの実行が失敗した場合、残りのインスタンスでは続行されません。

   承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることも選択でき、ジョブの成功または失敗に関する通知を、その他の詳細とともに送信するかどうかも選択できます。

10. 「**完了**」をクリックします。

    組み込みテンプレートを使用してジョブをスケジュールする(/en-us/netscaler-application-delivery-management-software/media/dmc5.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 構成テンプレートを使用して監査テンプレートを作成する

以前に構成テンプレートとして保存された構成コマンドを使用して、特定のNetScalerインスタンスに適用できる監査テンプレートを作成できるようになりました。監査テンプレートの作成中に、以前に保存した構成テンプレートをコマンドフィールドにドラッグし、要件に合わせてテンプレートを編集できます。その後、監査テンプレートを特定のNetScalerインスタンスに適用できます。NetScaler Consoleはこれらのインスタンスを監査テンプレートと比較し、不一致を報告します。このプロセスは、エラーを特定し、タイムリーに修正するのに役立ちます。

ジョブの作成中に構成テンプレートを作成し、一連の構成コマンドをテンプレートとして保存できます。これらのテンプレートを**Create Jobs**ページに保存すると、**Create Template**ページに自動的に表示されます。

たとえば、ロードバランシング仮想サーバーを追加し、2つのサービスを追加し、それらのサービスを仮想サーバーにバインドする基本的なロードバランシング構成を考えてみましょう。

この例では、次のコマンドを使用します。

```
add lb vserver >servername> HTTP <ipaddress portnumber>
```

```
add service <servicename1 ipaddress1> HTTP 80
```

```
add service <servicename2 ipaddress2> HTTP 80
```

```
bind lb vserver <servername servicename1>
```

```
bind lb vserver <servername servicename2>
```

**NetScaler Consoleで構成テンプレートを保存するには：**

1. **Infrastructure > Configuration Jobs**に移動し、**Create Job**をクリックします。
2. **Create Job**ページで、ジョブ名とインスタンスタイプを指定します。
3. 構成ソースとして**Configuration Template**を選択し、**Commands**フィールドに上記の例のようなコマンドを入力します。
4. **Save as Configuration Template**チェックボックスをオンにし、テンプレートの名前を指定します。同じ名前で存在する他のテンプレートを上書きすることもできます。
5. **保存**をクリックします。

   構成テンプレートの画像(/en-us/netscaler-application-delivery-management-software/media/audittemplates1.png)

**NetScaler Consoleで構成テンプレートを使用して監査テンプレートを作成するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Infrastructure > Configuration Audit > Audit Templates**に移動し、**追加**をクリックします。
2. **テンプレートの作成**ページで、テンプレートの名前を指定し、説明を入力します。
3. 「**構成ソース**」リストから「**構成テンプレート**」を選択し、テンプレートを右ペインのコマンドフィールドにドラッグします。構成を編集して、別の名前でテンプレートを保存することもできます。「**次へ**」をクリックします。
4. **インスタンスの選択**タブで、**インスタンスの追加**をクリックし、構成を実行するインスタンスを追加します。**OK**をクリックします。
5. **完了**をクリックします。

   監査テンプレートの画像(/en-us/netscaler-application-delivery-management-software/media/audittemplates2.png)

監査テンプレートは監査テンプレートリストに表示され、指定されたインスタンスの構成に対して12時間ごとに実行されます。

## 組み込みテンプレートを使用して構成されたジョブを再スケジュールする

NetScaler Console の組み込みテンプレートを使用してスケジュールしたジョブを再スケジュールできます。たとえば、コマンドが失敗した場合に NetScaler Console が実行する必要があるアクションを変更できます。以前にエラーを無視して続行することを選択していた場合、コマンドが失敗したときにすべての成功したコマンドをロールバックするように変更できます。

### NetScaler Console の組み込みテンプレートを使用して構成されたジョブを再スケジュールするには

1. NetScaler Console で、**インフラストラクチャ > 構成ジョブ** に移動します。
2. 編集するジョブを選択し、インスタンスを追加または削除し、変数値を指定してから、実行アクションと設定を変更します。
3. **完了** をクリックしてジョブを再スケジュールします。

**注**

ジョブを選択して **再実行** をクリックすると、ソース、インスタンス、コマンドを変更せずにジョブを実行することもできます。この機能は、同じインスタンスで同じコマンドセットを実行する必要がある場合に役立ちます。ジョブがサーバー側から一時的なエラーに遭遇し、ジョブを再度実行する必要がある場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 構成ジョブで構成監査テンプレートを再利用する

管理者として、ジョブを作成して構成監査を実行する際に、構成コマンドを再利用可能な構成テンプレートのセットとして保存できるようになりました。構成ジョブで作成および保存された構成テンプレートは、特定のNetScalerインスタンスに適用できる監査テンプレートを作成するために、構成監査で利用できます。同様に、構成監査モジュールで作成された監査テンプレートは構成ジョブで利用できるため、テンプレートを構成ジョブとして実行できます。テンプレートに加えられた変更は、構成ジョブと構成監査の両方のモジュールで表示されるようになりました。

以前は、同じ構成に対して構成ジョブと構成監査テンプレートを個別に作成し、異なるファイルとして保存する必要がありました。これにより、テンプレートの作成と保守に労力の重複が生じていました。

NetScaler Consoleでは、このテンプレートをシステムに保存できるため、監査テンプレートは構成ジョブでも利用できます。これで、監査テンプレートを使用して構成ジョブを作成できるようになりました。このようにして、テンプレートは構成ジョブと構成監査の間で相互に利用できます。

たとえば、基本的な負荷分散構成を考えてみましょう。これには、負荷分散仮想サーバーを追加し、2つのサービスを追加し、そのサービスを仮想サーバーにバインドします。

この例では、次のコマンドを使用します。

```
add lb vserver servername HTTP ipaddress portnumber


add service servicename1 ipaddress1 HTTP 80


add service servicename2 ipaddress2 HTTP 80


bind lb vserver servername servicename1


bind lb vserver servername servicename2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 構成監査でテンプレートを作成し、構成ジョブで再利用する

構成監査モジュールでテンプレートを作成し、構成ジョブモジュールで同じものを再利用するには、次のタスクを実行します。

**監査テンプレートを作成するには:**

1. NetScaler Consoleで、**Infrasturcture > Configuration Audit > Audit Template**に移動し、**追加**をクリックします。
2. **テンプレートの作成**ページで、テンプレート名を指定します。**説明**フィールドにテンプレートに関する詳細情報を追加することもできます。
3. **コマンド**ペインで、例のコマンドを入力します。
4. **構成テンプレートとして保存**チェックボックスをオンにし、テンプレートの名前を指定します。たとえば、このテンプレートを「LBVariablesTemplate」と名付けることができます。同じ名前で存在する他のテンプレートを上書きすることもできます。

   **注:**
   監査テンプレート名は、構成テンプレート名と同じにすることができます。

5. **保存**をクリックし、**次へ**をクリックします。

   

6. 「**次へ**」をクリックします。
7. 「**インスタンスの選択**」タブで、これらの構成コマンドを実行する**NetScalerインスタンス**を選択し、「**完了**」をクリックします。新しいテンプレートが監査テンプレートのリストに表示されます。

   

8. これらの構成コマンドを実行する場合は、「**インフラストラクチャ > 構成ジョブ**」に移動し、「**ジョブの作成**」をクリックします。以前に作成した監査テンプレートが構成テンプレートとして表示されます。

**構成ジョブで監査テンプレートを再利用するには：**

1. ジョブの名前を入力し、インスタンスタイプを選択して、テンプレートをコマンドペインにドラッグします。

   構成ジョブの作成中に、ローカルおよびリモートのファイル名パラメータを変数に変換できます。これにより、ジョブを実行するたびに、同じNetScalerインスタンスのセットに対してこれらのパラメータに異なるファイルを割り当てることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 入力したコマンドで、変数に変換するファイル名を選択し、「**変数に変換**」をクリックします。
3. 「**インスタンスの選択**」タブで、これらのコマンドを実行するインスタンスを選択します。
4. コマンドに変数を指定している場合は、「**変数値の指定**」タブで、インスタンスの変数を指定するために次のいずれかのオプションを選択します。
   - 入力ファイルからの変数値 - 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。
   - すべてのインスタンスの共通変数値 – syslogサーバーのIPアドレスとポートを指定します。
5. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証し、「**次へ**」をクリックします。
6. 「**実行**」タブで、「**完了**」をクリックして構成ジョブを実行します。この負荷分散サーバーに別のサービスを追加し、そのサービスをサーバーにバインドする場合は、コマンドページでコマンドを編集して保存できます。
7. 「**監査テンプレート**」に移動し、「**追加**」をクリックします。
8. 「LBVariablesTemplate」テンプレートをコマンドペインにドラッグします。テンプレートが新しいコマンドで更新されていることがわかります。

監査テンプレートは監査テンプレートリストに表示され、指定されたインスタンスの構成に対して12時間ごとに実行されます。これで、テンプレートを作成し、構成ジョブと構成監査モジュール間で再利用できるようになります。

## 構成テンプレートのインポートとエクスポート

任意のNetScaler Consoleから構成テンプレートをエクスポートできます。また、将来いつでも同じまたは別のNetScaler Consoleにファイルをインポートすることもできます。構成テンプレートのデータ（構成コマンド、変数定義、パラメーターなど）は失われません。

構成テンプレートを **.json** ファイル形式でエクスポートし、ローカルフォルダーに保存できます。構成テンプレートの **.json** ファイルをNetScaler Consoleにインポートできます。このファイルは新規のものであるか、同じまたは別のNetScaler Consoleからエクスポートしたものである可能性があります。

**構成テンプレートをエクスポートするには：**

1. **インフラストラクチャ > 構成ジョブ > 構成テンプレート** に移動します。
2. **Add** ボタンをクリックして、構成テンプレートを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Create Configuration Template** ページで、構成テンプレート名を指定し、インスタンスタイプを選択します。**Configuration Editor** で、ドロップダウンメニューから構成ソースとして Configuration Template を選択します。既存の構成テンプレートを構成エディターにドラッグできます。**Create** をクリックします。

   構成テンプレートを作成する 2(/en-us/netscaler-application-delivery-management-software/media/import-export-1.png)

4. **Infrastructure > Configuration Jobs > Configuration Templates** に移動して、構成テンプレートのリストに作成されたテンプレートを表示します。

   作成されたテンプレートを表示(/en-us/netscaler-application-delivery-management-software/media/import-export-2.png)

5. 新しく作成した構成テンプレートを選択し、**Export** ボタンをクリックします。

対応する構成テンプレートが、**.json** 形式でローカルシステムにダウンロードされます。

**構成テンプレートをインポートするには：**

1. **Infrastructure > Configuration Jobs > Configuration Templates** に移動し、**Import** ボタンをクリックします。構成テンプレートの **.json** ファイルがあるパスを選択し、**.json** ファイルをアップロードします。すでにエクスポートした **.json** ファイルをアップロードすることをお勧めします。
2. Configuration Editor の **File** オプションを使用して、構成テンプレートをインポートすることもできます。
3. 「**Configuration Editor**」のドロップダウンメニューから「**ファイル**」を選択します。
4. ローカルシステムから「**ファイルの選択**」(**.json** ファイル) を選択し、設定テンプレートの **.json** ファイルをアップロードします。

   テンプレートのアップロード(/en-us/netscaler-application-delivery-management-software/media/import-export-5.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「

**注**

」

- 新しくインポートされたすべてのテンプレートは、新しいID文字列で保存されます。
- ファイルが **.json** 形式で保存されている場合にのみ、設定テンプレートをインポートできます。ローカルシステムから **.json** ファイル以外の設定テンプレートをインポートすると、エラーが表示され、ファイルのインポートに失敗します。

## 構成監査

このドキュメントには、次の方法に関するトピックが含まれています。

- 監査レポートの表示(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/audit-reports.html)
- インスタンス全体の構成変更を監査する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/nmas-audit-configuration-instance.html)
- ネットワーク構成に関する構成アドバイスを取得する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/get-configuration-advice-network-configuration.html)
- NetScalerインスタンスの構成監査をポーリングする(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/how-to-poll-configuration-audit-of-netscaler-instances.html)
- ConfigChange SNMPトラップの構成監査差分を生成する(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/generate-configuration-audit-diff-for-configchange-snmp-traps.html)

### 監査レポートの表示

(NetScaler Console) では、構成監査セクションで構成監査差分レポートを表示およびダウンロードできます。構成監査セクションでは、以下をエクスポートできます。

- インスタンスごとのすべてのインスタンスにわたるサマリーレポート
- 各インスタンスとテンプレートのペアの詳細な差分レポート

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「**監査テンプレート**」の監査テンプレートは、指定されたインスタンスの構成に対して、スケジュールされた時間に実行されます。「**NetScaler Config Drift**」チャートは、「**構成監査**」ダッシュボードに表示され、保存済み構成と未保存構成における構成変更に関する概要の詳細を示します。「**NetScaler Config Drift**」チャートをクリックすると、その後の「**監査レポート**」ページに、「"Diff Exists"」と「"No Diff"」の両方を示すインスタンスのリストが表示されます。NetScaler Console に表示される差分レポートをダウンロードできます。

NetScaler Console には、差分レポートをメール添付ファイルとして自動エクスポートするオプションも用意されています。

**構成監査レポートをエクスポートするには：**

1. NetScaler Console で、**インフラストラクチャ > 構成 > 構成監査** に移動します。
2. **Configuration Audit** ページで、**NetScaler® Config Drift** チャート内をクリックします。
3. **監査レポート**ページには、差分があるインスタンスが一覧表示されます。このページには、実行中の構成に差分がないインスタンスのリストも表示されます。

   監査レポート(/en-us/netscaler-application-delivery-management-software/media/nmas-view-config-audit-reports-1.png)

この画像では、一部のインスタンスでは**Saved Vs Running Diff** にのみ差分が存在し、一部のインスタンスでは**Template vs Running Diff** にのみ差分が存在することがわかります。一部のインスタンスでは、**Saved Vs Running Diff** と **Template vs Running Diff** の両方に差分が存在します。

**保存済みと実行中の差分**

インスタンスに保存されている構成と、インスタンスで現在実行されている構成との差分レポートを表示できます。

1. **Saved Vs Running Diff** の下のインスタンスについて、**Diff Exists** をクリックします。

   そのインスタンスの保存済み設定と実行中の設定の差分レポートを表示できます。
2. **差分レポートのエクスポート**をクリックして、差分レポートの.csvファイルをダウンロードします。また、**修正コマンドのエクスポート**をクリックして、コマンドを.txtファイルにエクスポートすることもできます。その後、関連するNetScaler Consoleインスタンスで構成ジョブからコマンドを実行し、そのインスタンスの構成を修正できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### テンプレートと実行中の差分

**テンプレートと実行中の差分**には、デフォルトのテンプレートである**保存済みと実行中の差分**以外のすべてのテンプレートが含まれます。テンプレートと実行中の構成の間に存在する差分を表示できます。

1. **テンプレートと実行中の差分**の下にあるインスタンスのいずれかで**差分が存在**をクリックします。

   

2. NetScaler Consoleインスタンスがテンプレートで指定された構成から逸脱している場合、テンプレートは差分を明らかにします。

   

3. もう一度**差分が存在**をクリックします。次の画像は、テンプレートが探している構成、実行中の構成、および構成を修正するために実行する修正構成またはコマンドを示しています。**実行中の構成**が空白の場合、コマンドが構成されていないか、削除されていることを意味します。

   

4. **差分レポートのエクスポート**をクリックして、差分レポートの.csvファイルをダウンロードします。また、**修正コマンドのエクスポート**をクリックして、コマンドを.txtファイルにエクスポートすることもできます。その後、CLIでコマンドを実行して、インスタンスの構成を修正できます。

   

テンプレートと実行中のドリフト設定、および実行中とテンプレートのドリフト設定を使用して、両方の方法で構成を比較することもできます。

- インスタンス上の実行中の構成と監査テンプレート構成を比較します。
- インスタンス上の実行中の構成と監査テンプレートを比較します。

デフォルトでは、テンプレートと実行中のドリフト設定が選択されています。ドリフト設定を変更するには、**構成監査**ページで**設定**を選択します。

双方向構成ドリフト設定(/en-us/netscaler-application-delivery-management-software/media/config-audit-drift-settings.png)

### ファイルステータス監査レポートを表示する

**NetScaler ファイルステータス**チャートを使用して、`nsconfig`フォルダーにファイルが追加、変更、または削除されたかどうかを監視します。たとえば、NetScaler インスタンスでライセンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ファイルが更新された場合、このファイルが最後に更新された日時を確認し、必要なアクションを実行できます。

1. **インフラストラクチャ > 構成 > 構成監査**に移動します。
2. **構成監査**ページで、**NetScaler 構成ファイルステータス**チャートをクリックします。

   **監査レポート**ページには、Diff ステータスのインスタンスが一覧表示されます。

   **Diff ステータス**は、**前回のポーリング時刻**から**最新のポーリング時刻**までの間隔で計算されます。**Diff ステータス**は次のいずれかになります。

   - **Diff が存在します** - このステータスは、**前回のポーリング時刻**以降、インスタンスの `nsconfig` フォルダー内のファイルが変更されたことを示します。ファイルで何が変更されたかを表示するには、**Diff が存在します**をクリックします。

     `nsconfig` フォルダーにDiffが存在します(/en-us/netscaler-application-delivery-management-software/media/config-audit-ns-files-diff.png)
   - **Diff なし** - このステータスは、 `nsconfig` フォルダー内のファイルが前回のポーリング時刻以降変更されていないことを示します。
   - **NA** - このステータスは、ファイルステータスの監視が適用されないことを示します。このステータスは、NetScaler Console がインスタンスをポーリングしない場合に表示されます。たとえば、インスタンスが新しく追加された場合や、インスタンスの状態が非アクティブな場合、インスタンスのポーリングは行われません。

### 構成監査からファイルを除外する

Config Auditから特定のファイルを除外して、変更が監視されないようにすることができます。システム生成ファイルや頻繁に更新されるファイル（例えば、毎日変更されるファイル）を除外することで、ノイズを減らし、監査結果における誤検出を回避できます。

Config Auditのファイル差分から除外するファイル名（または相対パス）の例：

- 有効なファイル名（または相対パス）
  - `ns.conf`, `ssl/ns.cert`
- 無効なファイル名（または相対パス）
  - `/ns.txt`, `\nsconfig\ns.conf` (除外するファイル名は相対パスである必要があります)
  - `ñs.conf` (除外するファイル名にはASCII文字のみを含める必要があります)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `C:/nsconfig/ns.conf` (除外するファイル名にはドライブレターパスを使用しないでください)
- `ssl/../../ns.conf` (除外するファイル名には親ディレクトリトラバーサル `..` を含めないでください)

Config Auditからファイルを除外するには、次の手順を実行します。

1. **インフラストラクチャ > 構成 > 構成監査** に移動します。
2. **Settings** を選択します。
3. **NetScaler Config File Settings** で、監査から除外するファイルパスを追加します。
4. **Save** をクリックします。

### インスタンス全体の構成変更を監査する

ネットワークの最適なパフォーマンスのために、特定の構成が特定のインスタンスで実行されていることを確認したいとします。また、管理対象のNetScalerインスタンス全体の構成変更を監視し、構成エラーをトラブルシューティングし、突然のシステムシャットダウン後に保存されていない構成を回復したい場合もあります。

特定のインスタンスで監査する特定の構成を持つ監査テンプレートを作成できます。NetScaler Consoleは、これらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合に報告します。構成差分レポートを使用すると、不要な構成変更をトラブルシューティングして修正できます。

監査テンプレートの実行は、次の方法で自動化できます。

- テンプレートを実行する必要がある時間をスケジュールする。
- NetScaler Consoleがテンプレートを実行する頻度を設定する。テンプレートは、毎日、週の特定の曜日、または月の特定の日に実行できます。

NetScaler Consoleによって生成された差分レポートを、設定可能な指定されたメールアドレスに送信するオプションもあります。このオプションを使用すると、ユーザーはレポートをメール添付ファイルまたはSlack通知として受け取ることができます。手動でレポートをエクスポートするためにNetScaler Consoleにログインする必要はありません。

**注:**

デフォルトの構成テンプレートでは、**名前の変更**オプションは無効になっています。ただし、カスタム構成テンプレートの名前は変更できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**監査テンプレートを作成するには:**

1. **Infrastructure > Configuration > Configuration Audit > Audit Templates** に移動し、**Add** をクリックします。
2. **Create Template** ページで、**Audit Commands** タブで、テンプレート名とその説明を指定します。
3. **Configuration Editor** ページで、コマンドを入力し、そのコマンドを構成テンプレートとして保存します。既存のテンプレートを左ペインからエディターにドラッグすることもできます。
4. 変数に変換したい値を選択し、**Convert to Variable** をクリックします。たとえば、ロードバランシングサーバーのIPアドレス「ipaddress1」を選択し、**Convert to Variable** をクリックします。変数は「$」で囲まれます。

   「**Define Variable**」ウィンドウで、この変数のプロパティ（名前、表示名、変数のタイプ）を設定します。変数のデフォルト値をさらに指定する場合は、「**Advanced**」オプションをクリックします。

   「監査テンプレート2を設定」(/en-us/netscaler-application-delivery-management-software/media/nmas-config-audit-template-2.png)

   コマンドを構成テンプレートとして保存することもできます。

   「コマンドを構成テンプレートとして保存」(/en-us/netscaler-application-delivery-management-software/media/config-audit-template-commands-advanced.png)
5. 「**Save**」をクリックし、次に「**Next**」をクリックします。
6. 「**Select Instances**」タブで、構成監査を実行するインスタンスを選択し、「**Next**」をクリックします。

   「インスタンスを選択」(/en-us/netscaler-application-delivery-management-software/media/config-audit-template-instances.png)
7. 「**Specify Variable Values**」タブには、次の2つのオプションがあります。

   a. 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力します。変数を入力したら、ファイルをNetScaler Consoleサーバーにアップロードします。

   「入力ファイルをアップロード」(/en-us/netscaler-application-delivery-management-software/media/config-audit-template-upload-input-file.png)

   a. すべてのインスタンスに対して定義した変数に共通の値を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「共通変数を入力」(/en-us/netscaler-application-delivery-management-software/media/config-audit-template-common-variables.png)

**注:**

各インスタンスを異なる値で監査する場合は、入力ファイルでインスタンスごとに個別の変数を作成する必要があります。

8. 「**Next**」をクリックします。
9. **Template Preview** タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。**Next** をクリックします。



10. **Schedule Template** タブには、テンプレートの実行をスケジュールし、差分レポートを送信するメールアドレスを設定するための次のオプションがあります。
    - **Use global polling interval**。このオプションを選択すると、NetScaler Console でグローバルに設定された時間にインスタンスでテンプレートが実行されます。
    - **Customize template schedule**。このオプションを使用して、テンプレートを実行する時間と頻度を設定します。
        - 監査テンプレートの実行頻度とタイミングを指定します。
    - **Enable exporting of reports**。このオプションを使用して、次の操作を行います。
        - **差分検出時のみ差分レポート送信**
        - **Send diff report through email** (メールで差分レポートを送信)。差分レポートをメール添付ファイルとして送信するメールプロファイルを構成します。
        - **Send diff report through slack** (Slack で差分レポートを送信)。差分レポートを通知として送信する Slack チャネルを構成します。



11. **Finish** をクリックします。

監査テンプレートは **Audit Templates** リストに表示され、指定されたインスタンスの構成に対してスケジュールされた時間に実行されます。

### 構成変更の表示

**Configuration Audit** ダッシュボードを使用して、次のような構成変更に関する高レベルの詳細を表示することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 設定変更による上位10インスタンス
- 保存済みおよび未保存の設定の数
- `nsconfig`フォルダーで追加、削除、または変更されたファイル

NetScaler Consoleでは、構成監査を手動でポーリングすることもでき、インスタンスのすべての構成監査をNetScaler Consoleに即座に追加します。これを行うには、**Infrastructure > Configuration > Configuration Audit**に移動し、**Poll Now**をクリックします。ポップアップページ**Poll Now**には、ネットワーク内のすべてのNetScalerインスタンスをポーリングするか、選択したインスタンスをポーリングするかのオプションが表示されます。

インスタンスで監査を強制することもできます。これを行うには、次のいずれかのグラフをクリックします。

- **NetScaler構成保存ステータス**
- **NetScaler構成ドリフト**

**監査レポート**ページでインスタンスを選択し、**アクション**リストで**Poll Now**を選択します。

**NetScaler構成ファイルステータス**グラフには、`nsconfig`フォルダーに存在するNetScalerファイルの状態が表示されます。NetScaler Consoleは、`nsconfig`フォルダー内のファイルの変更を記録および比較し、その違いを表示します。詳細については、ファイルステータス監査レポートの表示を参照してください。

#### 構成監査通知を設定する

1. **インフラストラクチャ > 構成 > 構成監査** に移動します。
2. **Configuration Audit**ページで、**Settings**をクリックします。
3. **Notification Settings**ページで、**Edit**アイコンをクリックして通知設定を有効にします。
4. 「**有効**」チェックボックスを選択します。ドロップダウンリストからメール配信リストを選択します。「**+**」アイコンをクリックしてメールサーバーの詳細を指定することで、メール配信リストを作成することもできます。

### ネットワーク構成に関する構成アドバイスを取得する

アプリケーションで最適なパフォーマンスを実現するために、NetScalerインスタンスを最適な構成でセットアップします。ただし、一部の構成は標準構成ではない可能性があり、アプリケーションのパフォーマンスに影響を与える可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリケーションのパフォーマンスを最適化するために、NetScaler ConsoleはNetScalerインスタンスの構成を分析し、推奨事項を提供します。NetScaler Consoleから推奨構成を適用できます。

**NetScalerインスタンスを分析するには:**

1. 「**インフラストラクチャ > 構成 > 構成監査 > 構成アドバイス**」に移動します。
2. 次のいずれかを実行します。

   - **Upload Configuration File** をクリックし、ネットワークインスタンスの構成ファイルをアップロードします。

   - **Select Device** をクリックし、分析するNetScalerインスタンスを選択します。

NetScaler Consoleはインスタンスの構成を分析し、次の図に示すように構成推奨事項のリストを提供します。構成アドバイスの横にあるチェックボックスをクリックして、修正コマンドを表示します。

修正コマンド (/en-us/netscaler-application-delivery-management-software/media/config-audit-template-configadvice.png)

構成を更新する場合は、修正コマンドの変数の値を指定し、**Apply Now** をクリックします。

**注:**

ここにリストされているコマンドは推奨事項にすぎません。読み取り/書き込みアクセス権を持つユーザーは、この機能を使用して任意のコマンドを編集できます。コマンドを編集すべきではないと考えるユーザーには、制限された特権アクセスを付与するようにしてください。

コマンドがネットワークインスタンスで正常に実行されると、アドバイスの横にあるチェックボックスが消えます。

成功したコマンド (/en-us/netscaler-application-delivery-management-software/media/mas-configuration-advice-6.png)

ネットワークインスタンスで実行されたコマンドの詳細を表示したい場合は、**Infrastructure > Instances >** `<Instance\_Type\>` に移動し、インスタンスのIPアドレスを選択して、**Actions** ドロップダウンリストから **Show Events** をクリックします。

**Events** ページで、構成変更の詳細を表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler® インスタンスの構成監査をポーリングする

NetScaler Consoleは、NetScalerインスタンスで発生する構成変更を探すために、10時間ごとに構成監査を自動的にポーリングします。最近の変更を検出するために、構成監査を手動でポーリングすることもできますが、すべてのNetScalerインスタンスの構成をポーリングすると、ネットワークに大きな負荷がかかります。

NetScalerインスタンスの構成監査全体をポーリングする代わりに、選択した1つまたは複数のインスタンスの構成監査のみを手動でポーリングできます。

**NetScaler インスタンスの構成監査をポーリングするには：**

1. ネットスケーラー コンソールで、**Infrastructure > Configuration > Configuration Audit** に移動します。
2. **Configuration Audit**で、**Poll Now**をクリックします。

   
3. **Poll Now**ページがポップアップ表示され、ネットワーク内のすべてのNetScalerインスタンスをポーリングするか、選択したインスタンスをポーリングするオプションが表示されます。

   a. すべてのNetScalerインスタンスをポーリングするには、**All Instances**タブを選択し、**Start Polling**をクリックします。

   

   b. 特定のインスタンスをポーリングするには、**Select Instances** タブを選択し、リストからインスタンスを選択して、**Poll Now** をクリックします。

   

### ConfigChange SNMPトラップの構成監査差分を生成する

ネットワーク内のNetScalerインスタンスで構成変更があるたびに、構成ファイルが更新されます。インスタンスはConfigChange SNMPトラップをNetScaler Consoleに送信します。インスタンスがConfigChange SNMPトラップを送信したときに、NetScaler Consoleでそのインスタンスの構成監査を実行するように有効にできます。

監査テンプレート構成と実行中の構成の間に差異がある場合、**監査レポート**ページに「Diff Exists」ステータスメッセージが表示されます。**Diff Exists**リンクをクリックすると、**構成差分**ページに移動し、修正コマンドを表示できます。これらの修正コマンドを使用して構成ジョブを作成し、特定のNetScalerインスタンスで実行できます。構成ジョブを実行すると、インスタンスは目的の構成に戻されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修正コマンドから構成ジョブを作成する方法の詳細については、「NetScaler Consoleで修正コマンドから構成ジョブを作成する方法」を参照してください。

**ConfigChange SNMPトラップを受信したときに構成監査テンプレートを実行するには：**

NetScaler Consoleでは、NetScaler Consoleで構成監査テンプレートを実行するオプションを有効にできます。

1. NetScaler Consoleで、**インフラストラクチャ > 構成 > 構成監査**に移動します。
2. **構成監査**ページで、**設定**をクリックします。
3. **「netScalerConfigChange」イベントの受信時に監査を実行**を選択します。

**注：**

NetScaler Consoleは、今後netScalerConfigChange SNMPトラップを受信するすべてのインスタンスに対して構成監査を実行します。

1. **監査テンプレートを実行する時間遅延**（分）フィールドに、分数を入力します。NetScaler Consoleは、そのインスタンスからConfigChange SNMPトラップを受信した後、この時間遅延後にNetScalerインスタンスで構成監査テンプレートを実行します。

# アップグレードジョブ

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、End of Life (EOL) はApril 15, 2026となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASとなり、NetScaler Flexedライセンス（Citrix Platform License/Universal Hybrid Multi-Cloud）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-prem の LAS サポートは、リリース 14.1-51.x 以降です。ただし、ファイルベースのライセンスは、Console on-prem リリース 14.1-51.x 以降および 13.1-60.x 以降では、April 15 2026 をもって非推奨となります。Console on-prem リリース 14.1-51.x またはリリース 13.1-60.x 以降にアップグレードした場合でも、15th April 2026 までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1 は LAS をサポートしていないため、15th April 2026 までに Console on-prem リリース 14.1-51.x 以降にアップグレードし、LAS に切り替える必要があります。

NetScaler仮想CPUライセンス（Pooled vCPU）、NetScaler VPX Check-In and Check-Out（CICO）、永続ライセンスなど、従来のNetScalerライセンスの他のすべての形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScaler Consoleを使用して、以下のメンテナンスジョブを作成できます。その後、特定の日付と時刻にメンテナンスジョブをスケジュールできます。

- NetScalerインスタンスのアップグレード
- NetScaler SDXインスタンスのアップグレード
- NetScaler BLXインスタンスをアップグレードする
- オートスケールグループ内のNetScalerインスタンスをアップグレードする
- NetScalerインスタンスのHAペアを構成する
- インスタンスのHAペアをクラスターに変換する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記:**

- アップグレードジョブが失敗した場合、NetScaler Consoleはビルドファイルおよびその他の抽出されたファイルを削除し、NetScalerインスタンスが次回のアップグレード試行に十分なディスク容量を確保できるようにします。
- アップグレードのために任意の数のNetScalerインスタンスを選択できますが、NetScaler Consoleオンプレミスは最大40の同時アップグレードスレッドをサポートしています。これは、同時にアップグレードできるインスタンスが40台のみであることを意味します。
- 非FIPSビルドからFIPSビルドへの移行、およびシーケンシャルアップグレードをスキップする直接バージョンアップグレード（例: バージョン13.0から14.1へのアップグレード）はサポートされていません。これらの制限は、ビルドタイプ間のアーキテクチャの違いと、メジャーバージョン間での必要な増分変更によるものです。アップグレードを成功させるには、新しいFIPSビルドを展開するか、すべての中間バージョンを経由するサポートされているシーケンシャルアップグレードパスに従う必要があります。

## アップグレード前の検証

NetScalerのアップグレードジョブ中に、NetScaler Consoleは次の検証を実行します。

- NetScaler Consoleによって実行されるアップグレード前チェック
- NetScalerによって実行されるアップグレード前チェック（NetScaler 14.1-66.x以降でサポート）

両方のソースからの結果は統合され、アップグレードの決定を導くための単一の応答として提示されます。NetScalerまたはNetScaler Consoleによって実行されるアップグレード前チェックを有効にするための追加設定は不要です。アップグレード前の検証には、次の利点があります。

- アップグレード中の信頼性と安全性の向上
- アップグレード開始前のブロック問題の早期検出
- サポートされているNetScalerバージョン全体で一貫した事前チェックエクスペリエンス

### NetScaler Consoleによって実行されるアップグレード前チェック

NetScaler Consoleは次のチェックを実行します。

- **`/var`のディスク空き容量**: イメージの抽出およびインストール操作を安全に実行するために、`/var`パーティションに十分な空き容量があることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **/flashのディスク空き容量**: インストール中に重要なシステム操作をサポートするために、`/flash`パーティションに最低限必要な空きディスク容量があることを確認します。
- **NSPEPI構成チェック**: インストールまたはアップグレード後の構成エラーを防ぐために、サポートされていないポリシーまたは無効なポリシーがないかNetScaler構成ファイルを検証します。
- **高可用性 (HA) 構成チェック**: 健全でサポートされているHAセットアップを確保するために、HAの状態とロールの一貫性を検証します。
- **SSH接続チェック**: リモートインストールおよび管理操作に必要なSSHアクセシビリティ、信頼性検証、およびターゲットデバイスへの接続を確認します。
- **ダウングレード用のns.confの一致**: 構成の非互換性を防ぐために、ダウングレードシナリオに適した互換性のある`ns.conf file`が利用可能であることを確認します。

すべての事前チェック結果は、次のように一様に分類されます。

- **重大 (ブロック)**: アップグレードはブロックされます。続行する前に、報告されたすべての問題を解決する必要があります。
- **警告**: 管理者の承認を得てアップグレードを続行できます。
- **アドバイザリ**: 管理者の承認を得てアップグレードを続行できます。

### NetScalerによって実行されるアップグレード前チェック

NetScalerによって実行されるアップグレード前チェックの詳細については、「NetScalerのアップグレード前検証チェック」を参照してください。

## NetScalerインスタンスのアップグレードをスケジュールする

1. **インフラストラクチャ > アップグレードジョブ**に移動します。**ジョブの作成**をクリックします。

   

2. **メンテナンスジョブの作成**で、**NetScalerのアップグレード (スタンドアロン/高可用性/クラスター)** を選択し、**続行**をクリックします。

   

3. **インスタンスの選択**で、**ジョブ名**に任意の名前を入力します。
4. アップグレードするNetScalerインスタンスを追加するには、**インスタンスの追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HAペアをアップグレードするには、プライマリまたはセカンダリノードのIPアドレスを指定します。ただし、HAペアのアップグレードにはプライマリインスタンスを使用することをお勧めします。
- クラスターをアップグレードするには、クラスターIPアドレスを指定します。



5. **次へ**をクリックしてイメージを選択します。**ソフトウェアイメージ**リストから次のいずれかのオプションを選択します。

   - **ローカル** - ローカルマシンからインスタンスアップグレードファイルを選択します。
   - **アプライアンス** - NetScaler Consoleファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler Console GUIには、`/var/mps/mps_images`にあるインスタンスファイルが表示されます。
     - **選択したイメージがすでに利用可能な場合は、NetScalerへのイメージアップロードをスキップする** - イメージがNetScalerインスタンスにすでに存在する場合は、このオプションを選択します。
     - **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップする** - インスタンスのアップグレード後、NetScalerインスタンス内のアップロードされたイメージをクリアするには、このオプションを選択します。

   **注:**

   - 選択したインスタンスがすでにターゲットビルドにある場合、警告が表示されます。この警告は、アップグレードジョブ中に誤ったインスタンスが選択されるのを防ぐのに役立ちます。インスタンスを再アップグレードする予定がある場合は、警告を無視してアップグレードを続行してください。

     

   - 選択したインスタンスに既存のアップグレードジョブがすでにスケジュールされている場合、NetScaler Consoleは警告メッセージを表示します。この警告メッセージは、同じNetScalerインスタンスで誤って重複するアップグレードジョブがスケジュールされるのを防ぐのに役立ちます。

6. 選択したインスタンスでアップグレード前の検証を開始するには、「**次へ**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「**アップグレード前の検証**」タブに失敗したインスタンスが表示されます。失敗したインスタンスを削除し、「**次へ**」をクリックします。

**重要**

クラスターIPアドレスを指定した場合、NetScaler Consoleは指定されたインスタンスに対してのみアップグレード前の検証を実行し、他のクラスターノードに対しては実行しません。

7. オプション: 「**カスタムスクリプト**」で、インスタンスのアップグレード前後に実行するスクリプトを指定します。コマンドを実行するには、次のいずれかの方法を使用します。

   - 「**ファイルからコマンドをインポート**」 - ローカルコンピューターからコマンド入力ファイルを選択します。
   - 「**コマンドを入力**」 - GUIに直接コマンドを入力します。

   カスタムスクリプトを使用して、インスタンスのアップグレード前後の変更を確認できます。例:

   - アップグレード前後のインスタンスバージョン。
   - アップグレード前後のインターフェース、高可用性ノード、仮想サーバー、およびサービスの状態。
   - 仮想サーバーとサービスの統計情報。
   - 動的ルート。

8. **次へ**をクリックします。**タスクのスケジュール**で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード** - アップグレードジョブがすぐに実行されます。
   - **後でスケジュール** - このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

     NetScaler HAペアを2段階でアップグレードする場合は、**HA内のノードに対して2段階アップグレードを実行**を選択します。

     HAペア内の別のインスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

9. **次へ**をクリックします。**ジョブの作成**で、次の詳細を指定します。

   a. イメージをインスタンスにアップロードするタイミングを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **今すぐアップロード** - イメージをすぐにアップロードするには、このオプションを選択します。ただし、アップグレードジョブはスケジュールされた時刻に実行されます。
- **実行時にアップロード** - アップグレードジョブの実行時にイメージをアップロードするには、このオプションを選択します。
- **アップグレードを開始する前にNetScalerインスタンスをバックアップします。** - 選択したNetScalerインスタンスのバックアップを作成します。
- **アップグレードを開始する前にNetScaler構成を保存します** - アップグレード前にインスタンスで構成されている構成ジョブを保存します。
- **NetScaler HAペアでのネットワーク停止を回避するためにISSUを有効にする** - インサービスソフトウェアアップグレード（ISSU）を有効にすると、ネットワークのダウンタイムなしでNetScaler高可用性（HA）ペアをアップグレードできます。ISSUは、アクティブなセッションをノード間でシームレスに移行することにより、アップグレード中に既存の接続が維持されるようにします。アップグレードワークフローでISSUを有効にすると、システムは顧客が定義した遅延時間の後にISSU移行完了をトリガーすることもできます。NetScaler Consoleが完全なISSU移行完了をトリガーすることで、接続が持続する場合でもアップグレードが完了します。NetScaler Consoleが移行を完了するまでの待機時間を設定するには、ISSU移行タイムアウトを分単位で指定します。

- **NetScaler Console Service Connect** - ビルド**13.0-64以降**および**12.1-58以降**にアップグレードする場合、NetScaler Console Service Connectは自動的に有効になります。詳細については、「NetScaler Console Service Connectを使用したNetScalerインスタンスのロータッチオンボーディング」を参照してください。
- **電子メールで実行レポートを受信する** - 実行レポートを電子メールで送信します。電子メール配信リストを追加するには、「電子メール配信リストの作成」(/ja-jp/netscaler-application-delivery-management-software/current-release/license-server/license-management.html)を参照してください。
- **Slackで実行レポートを受信する** - 実行レポートをSlackで送信します。Slackプロファイルを追加するには、「Slackプロファイルの作成」(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-notification-settings.html)を参照してください。



10. **ジョブの作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler SDXインスタンスのアップグレードをスケジュールする

1. **インフラストラクチャ > アップグレードジョブ**に移動します。**ジョブの作成**をクリックします。
2. **NetScaler SDXのアップグレード**を選択し、**続行**をクリックします。
3. **NetScaler SDXのアップグレード**ページで、**インスタンスの選択**タブに移動します。
   a. **タスク名**を追加します。
   b. **ソフトウェアイメージ**リストから、**ローカル** (ローカルマシン) または**アプライアンス** (ビルドファイルはNetScaler Console仮想アプライアンスに存在する必要があります) のいずれかを選択します。

      アップロードプロセスが開始されます。
   c. アップグレードプロセスを実行するNetScaler SDXインスタンスを追加します。
   d. **次へ**をクリックします。
4. **タスクのスケジュール**タブで、**実行モード**リストから**今すぐ**を選択してNetScaler SDXインスタンスを今すぐアップグレードし、**完了**をクリックします。
5. NetScaler SDXインスタンスを後でアップグレードするには、**実行モード**リストから**後で**を選択します。その後、NetScalerインスタンスをアップグレードするための実行日と開始時刻を選択し、**完了**をクリックします。
6. NetScaler SDXインスタンスのアップグレード実行レポートを受信するために、メールおよびSlack通知を有効にすることもできます。通知を有効にするには、**Receive Execution Report Through Email**チェックボックスと**Receive Execution Report through slack**チェックボックスをクリックします。

   メール配信リストとSlackチャネルの設定の詳細については、NetScalerインスタンスのアップグレードのスケジュールの**ステップ8**を参照してください。

## NetScaler BLXインスタンスのアップグレードをスケジュールする

1. **Infrastructure > Upgrade Jobs**に移動します。**Create Job**をクリックします。
2. **Create Maintenance Jobs**で、**Upgrade NetScaler BLX**を選択し、**Proceed**をクリックします。
3. **Select Instance**で、**Job Name**に任意の名前を入力します。
4. アップグレードするBLXインスタンスを追加するには、**Add Instances**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HAペアをアップグレードするには、プライマリまたはセカンダリノードのIPアドレスを指定します。ただし、HAペアをアップグレードするには、プライマリインスタンスを使用することをお勧めします。
- クラスターをアップグレードするには、クラスターIPアドレスを指定します。

5. **Next**をクリックしてイメージを選択します。**Software Image**リストから次のいずれかのオプションを選択します。

   - **Local** - ローカルマシンからインスタンスアップグレードファイルを選択します。
   - **Appliance** - NetScaler Consoleファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler Console GUIには、`/var/mps/mps_images`に存在するインスタンスファイルが表示されます。

     - **選択したイメージがすでに利用可能な場合は、NetScalerへのイメージアップロードをスキップする** - イメージがNetScalerインスタンスにすでに存在する場合に、このオプションを選択します。
     - **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップする** - インスタンスのアップグレード後、NetScalerインスタンスにアップロードされたイメージをクリアするには、このオプションを選択します。

6. **Next**をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

   「**アップグレード前検証**」タブに、失敗したインスタンスが表示されます。失敗したインスタンスを削除し、「**次へ**」をクリックします。

   **重要**

   クラスターIPアドレスを指定した場合、NetScaler Consoleは指定されたインスタンスに対してのみアップグレード前検証を実行し、他のクラスターノードに対しては実行しません。

7. オプションで、「**カスタムスクリプト**」で、インスタンスのアップグレード前後に実行するスクリプトを指定します。コマンドを実行するには、次のいずれかの方法を使用します。

   - **ファイルからコマンドをインポート** - ローカルコンピューターからコマンド入力ファイルを選択します。
   - **コマンドを入力** - GUIに直接コマンドを入力します。

   カスタムスクリプト(/en-us/netscaler-application-delivery-management-software/media/custom-scripts-upgrade-job.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタムスクリプトを使用して、インスタンスのアップグレード前後の変更を確認できます。例：

- アップグレード前後のインスタンスバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバー、およびサービスのステータス。
- 仮想サーバーとサービスの統計。
- 動的ルート。

8. 「**次へ**」をクリックします。「**タスクのスケジュール**」で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード** - アップグレードジョブがすぐに実行されます。
   - **後でスケジュール** - このオプションを選択すると、このアップグレードジョブを後で実行できます。インスタンスをアップグレードする「**実行日**」と「**開始時刻**」を指定します。

     HAペアを2段階でアップグレードする場合は、**HAのノードに対して2段階アップグレードを実行**を選択します。

     HAペア内の別のインスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

9. **次へ**をクリックします。**ジョブの作成**で、次の詳細を指定します。

   a. インスタンスにイメージをアップロードするタイミングを指定します。

      - **今すぐアップロード** - このオプションを選択すると、イメージがすぐにアップロードされます。ただし、アップグレードジョブはスケジュールされた時刻に実行されます。
      - **実行時にアップロード** - このオプションを選択すると、アップグレードジョブの実行時にイメージがアップロードされます。
      - **アップグレードを開始する前にNetScalerインスタンスをバックアップ** - 選択したNetScalerインスタンスのバックアップを作成します。
      - **アップグレードを開始する前にNetScaler構成を保存** - アップグレード前にインスタンスで構成されている構成ジョブを保存します。
      - **NetScaler HAペアでのネットワーク停止を回避するためにISSUを有効にする** - インサービスソフトウェアアップグレード (ISSU) を有効にすると、ネットワークのダウンタイムを発生させることなくNetScaler高可用性 (HA) ペアをアップグレードできます。ISSUは、アクティブなセッションをノード間でシームレスに移行することにより、アップグレード中に既存の接続が維持されるようにします。アップグレードワークフローでISSUを有効にした後、システムは顧客によって定義された遅延時間の後にISSU

© 1997–2026 Citrix Systems, Inc. All rights reserved.

移行完了をトリガーすることもできます。NetScaler Consoleが完全なISSU移行完了をトリガーすることで、接続が持続している場合でもアップグレードが完了します。NetScaler Consoleが移行を完了するまでの待機時間を設定するには、ISSU移行タイムアウトを分単位で指定します。

- **NetScaler Console Service Connect** - ビルド**13.0-64以降**および**12.1-58以降**にアップグレードする場合、NetScaler Console Service Connectは自動的に有効になります。詳細については、「NetScaler Console Service Connectを使用したNetScalerインスタンスのロータッチオンボーディング」を参照してください。
- **メールで実行レポートを受信する** - 実行レポートをメールで送信します。メール配布リストを追加するには、「メール配布リストの作成」を参照してください。
- **Slackで実行レポートを受信する** - 実行レポートをSlackで送信します。Slackプロファイルを追加するには、「Slackプロファイルの作成」を参照してください。

10. **ジョブの作成**をクリックします。

## Autoscale™グループのアップグレードをスケジュールする

Autoscaleグループに属するクラウドサービス内のすべてのインスタンスをアップグレードするには、次の手順を実行します。

1. **Infrastructure > Upgrade Jobs** に移動します。**Create Job** をクリックします。
2. **Upgrade Autoscale Group** を選択し、**Proceed** をクリックします。
3. **Upgrade Settings** タブで、:
   a. アップグレードする**Autoscale Group** を選択します。
   b. **Image** で、NetScalerのバージョンを選択します。このイメージは、Autoscaleグループ内のNetScalerインスタンスの既存のバージョンです。
   c. **NetScaler Image** で、アップグレードするNetScalerバージョンファイルを参照します。

      **Graceful Upgrade** をオンにすると、アップグレードタスクは指定されたドレイン接続期間が終了するまで待機します。
   d. **Next** をクリックします。
4. **Schedule Task** タブで、:
   a. Execution Modeリストから次のいずれかを選択します。
      - **Now:** NetScalerインスタンスのアップグレードをすぐに開始します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Later:** NetScalerインスタンスのアップグレードを後で開始します。

b. **Later** オプションを選択した場合は、アップグレードタスクを開始するExecution DateとStart Timeを選択します。

アップグレード中のAutoscaleグループの実行レポートを受信するために、メールとSlackの通知を有効にすることもできます。通知を有効にするには、**Receive Execution Report Through Email** チェックボックスと**Receive Execution Report through slack** チェックボックスをクリックします。

5. 「**完了**」をクリックします。

## NetScalerインスタンスのHAペア設定をスケジュールする

1. 「**インフラストラクチャ > アップグレードジョブ**」に移動します。「**ジョブの作成**」をクリックします。
2. 「**NetScalerインスタンスのHAペアを設定**」を選択し、「**続行**」をクリックします。
3. 「**NetScaler HAペア**」ページの「**インスタンスの選択**」タブで、次の操作を行います。

a. 「**タスク名**」を追加します。

b. プライマリIPアドレスを選択します。

c. プライマリRPCノードパスワードを入力します。

d. セカンダリIPアドレスを選択します。

> **注:**
>
> RPCノードパスワードフィールドは、NetScalerリリース14.1以降で利用可能です。

e. セカンダリRPCノードパスワードを入力します。

f. HAペアインスタンスが2つのサブネットにある場合は、「**INC (独立ネットワーク構成) モードをオンにする**」をクリックして有効にします。

4. 「**タスクのスケジュール**」タブで、次のいずれかのオプションを選択します。

- 「**今すぐアップグレード**」：このオプションを選択して、NetScalerインスタンスをすぐにアップグレードします。「**完了**」をクリックします。
- **後でスケジュール**：このオプションを選択すると、NetScaler HAペアを後でアップグレードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 「**後でスケジュール**」オプションを選択した場合は、NetScalerインスタンスをアップグレードするための「**実行日**」と「**開始時刻**」を選択します。

   a. 「**NetScaler HAノードのアップグレードを2段階で実行**」を選択します。このオプションを選択すると、両方のノードが正常にアップグレードされるまで、HA同期とHA伝播が無効になります。

   b. セカンダリノードのアップグレードをスケジュールするには、次のいずれかのオプションを選択します。このオプションを使用すると、ステージ1が正常に完了した後にのみステージ2のアップグレードが実行されます。

      - **設定された遅延の後**：最初のノードのアップグレードが完了してから、2番目のノードのアップグレードが開始されるまでの遅延（時間単位）を指定します。
      - **特定の時刻に**：セカンダリノードのアップグレードの日付と時刻を選択します。

6. 「**セカンダリノードのアップグレードが開始されるまでHAフェイルオーバーを遅延**」を選択します。「**次へ**」をクリックします。
7. 「**タスクのスケジュール**」タブで、「**実行モード**」リストから「**今すぐ**」を選択してNetScalerインスタンスを今すぐアップグレードし、「**完了**」をクリックします。

   HAペアを選択(/en-us/netscaler-application-delivery-management-software/media/ha-cluster-instance-select.png)

8. NetScaler HAペア作成の実行レポートを受信するために、メールとSlack通知を有効にすることもできます。「**メールで実行レポートを受信する**」チェックボックスと「**Slackで実行レポートを受信する**」チェックボックスをクリックして、通知を有効にします。

   メール配布リストとSlackチャネルの設定の詳細については、「NetScalerインスタンスのアップグレードをスケジュールする」の**ステップ8**を参照してください(#schedule-upgrading-of-pagecitrix-adc-generic-instances)

## HAペアインスタンスのクラスターへの変換をスケジュールする

1. 「**インフラストラクチャ > アップグレードジョブ**」に移動します。「**ジョブの作成**」をクリックします。
2. 「**HAペアインスタンスを2ノードクラスターに変換**」を選択し、「**続行**」をクリックします。
3. 「**NetScaler HAをクラスターに移行**」ページの「**インスタンス選択**」タブで、「**タスク名**」を追加します。プライマリIPアドレス、セカンダリIPアドレス、プライマリノードID、セカンダリノードID、クラスターIPアドレス、クラスターID、およびバックプレーンを指定し、「**次へ**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**スケジュールタスク**」タブで、「**実行モード**」リストから「**今すぐ**」を選択してNetScalerインスタンスを今すぐアップグレードし、「**完了**」をクリックします。
5. 後でアップグレードするには、「**実行モード**」リストから「**後で**」を選択します。その後、NetScaler HAペアインスタンスをアップグレードするための「**実行日**」と「**開始時刻**」を選択し、「**完了**」をクリックします。
6. NetScaler SDXインスタンスのアップグレード実行レポートを受信するために、メールとSlackの通知を有効にすることもできます。通知を有効にするには、「**メールで実行レポートを受信する**」チェックボックスと「**Slackで実行レポートを受信する**」チェックボックスをクリックします。

   メール配信リストとSlackチャネルの設定の詳細については、NetScalerインスタンスのアップグレードをスケジュールするの**ステップ8**を参照してください。

## ジョブを使用してNetScaler®インスタンスをアップグレードする

NetScaler Consoleを使用して、1つ以上のNetScalerインスタンスをアップグレードできます。インスタンスをアップグレードする前に、ライセンスフレームワークとライセンスの種類を理解しておく必要があります。

**注:** クラシックポリシーを持つインスタンスをアップグレードする場合は、NSPEPIツールを使用して、インスタンスをアップグレードする前にクラシックポリシーをアドバンストポリシーに変換することをお勧めします。これは、NSPEPIツールでサポートされている機能に適用されます。詳細については、「クラシックポリシーを持つ構成のアップグレードに関する考慮事項」を参照してください。

メンテナンスジョブを作成してNetScalerインスタンスをアップグレードする際は、アップグレードするインスタンスに対して事前検証チェックを実行してください。

### 事前検証チェック

1. **カスタマイズの確認** - カスタマイズをバックアップし、インスタンスから削除します。インスタンスのアップグレード後、バックアップしたカスタマイズを再適用できます。
2. **ディスク使用量の確認** - `/var`フォルダーの空き容量が6 GB未満で、`/flash`フォルダーの空き容量が200 MB未満の場合は、ディスクスペースをクリーンアップしてください。ディスクスペースをクリーンアップするには、次のフォルダーパスを確認してください。

   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `/var/tmp/support`
- `/var/core`
- `/var/crash`
- `/var/nsinstall`
- `/var/netscaler/nsbackup`

3. **ディスクハードウェアの問題を確認する** - ハードウェアの問題があれば解決してください。
4. **STAYPRIMARYおよびSTAYSECONDARYノードを確認する** - NetScaler HAの場合、STAYPRIMARYおよびSTAYSECONDARY状態のノードではアップグレードがブロックされます。これらのノードは事前検証チェックで特定され、「**アップグレードがブロックされたインスタンス**」の下にリストされます。



### NetScaler高可用性ペア

NetScaler HAペアをアップグレードする際は、次の点に注意してください。

- セカンダリノードが最初にアップグレードされます。
- 両方のノードが正常にアップグレードされるまで、ノードの同期と伝播は無効になります。
- HAペアのアップグレードが正常に完了すると、実行履歴にエラーメッセージが表示されます。このメッセージは、HAペア内のノードが異なるビルドまたはバージョンである場合に表示されます。このメッセージは、プライマリノードとセカンダリノード間の同期が無効になっていることを示します。

NetScaler HAペアは2つの段階でアップグレードできます。

1. アップグレードジョブを作成し、いずれかのノードで直ちに実行するか、後でスケジュールします。
2. 残りのノードで実行するアップグレードジョブを後でスケジュールします。このジョブは、最初のノードのアップグレード後にスケジュールするようにしてください。

### NetScalerクラスター

NetScalerクラスターをアップグレードする場合、NetScaler Consoleは指定されたインスタンスに対してのみアップグレード前の検証を実行します。アップグレードする前に、クラスターノードのカスタマイズ、ディスク使用量、およびハードウェアの問題を確認し、解決してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScalerインスタンスをアップグレードするためのアップグレードメンテナンスジョブを作成する

**注**

NetScalerのより高いバージョンからより低いバージョンへのアップグレードはサポートされていません。たとえば、NetScalerインスタンスが13.0 82.xの場合、NetScalerインスタンスを13.0 79.xまたはそれ以前のバージョンにダウングレードすることはできません。

1. NetScaler Consoleで、**Infrastructure > Upgrade Jobs**に移動します。**Create Job**ボタンをクリックします。
2. **メンテナンスジョブの作成**で、**NetScalerのアップグレード（スタンドアロン/高可用性/クラスター）**を選択し、**続行**をクリックします。



3. **Select Instance**で、**Job Name**に任意の名前を入力します。
4. アップグレードするNetScalerインスタンスを追加するには、**Add Instances**をクリックします。

   - NetScalerの高可用性ペアをアップグレードするには、高可用性ペアのIPアドレス（「S」と「P」の上付き文字で示されます）を選択します。
   - クラスターをアップグレードするには、クラスターIPアドレス（「C」の上付き文字で示されます）を選択します。



5. **Select Image**タブで、ローカルドライブまたはビルドイメージからNetScalerイメージを選択します。

   - **Local** - ローカルマシンからインスタンスアップグレードファイルを選択します。
   - **Appliance** - NetScaler Consoleのファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler Console GUIには、`/var/mps/ns_images`にあるインスタンスファイルが表示されます。



   - **選択したイメージがすでに利用可能な場合、NetScalerへのイメージアップロードをスキップする** - このオプションは、選択したイメージがNetScalerで利用可能かどうかを確認します。アップグレードジョブは新しいイメージのアップロードをスキップし、NetScalerで利用可能なイメージを使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップ** - このオプションは、インスタンスのアップグレード後、NetScalerインスタンス内のアップロードされたイメージをクリアします。

**次へ**をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

**注:**

- ダウンロードされたNetScalerイメージはNetScaler Consoleエージェントに保存され、`/var/mps/adcimages`に存在します。これらのキャッシュされたイメージは、複数のNetScalerアップグレードに使用できるため、アップグレードのたびにイメージをダウンロードする必要がなくなります。
- NetScaler Consoleは、イメージの最終変更時間に基づいて、キャッシュされたNetScalerイメージを3日ごとにクリアします。一度にNetScaler Consoleエージェントにキャッシュされるのは、最新の2つのイメージファイルのみです。

6. **アップグレード前の検証**タブには、次のセクションが表示されます。

- **アップグレード準備完了インスタンス**。これらのインスタンスのアップグレードを続行できます。
- **アップグレードがブロックされたインスタンス**。これらのNetScalerインスタンスは、アップグレード前の検証エラーのため、アップグレードがブロックされています。

  エラーを確認して修正し、**アップグレード準備完了に移動**をクリックしてアップグレードできます。インスタンスでディスク容量が不足している場合は、ディスク容量を確認してクリーンアップできます。「NetScalerディスク容量のクリーンアップ」を参照してください。(#clean-up-the-netscaler-disk-space).

- **ポリシーチェック**: NetScaler Consoleがサポートされていないクラシックポリシーを検出した場合、それらのポリシーを削除してアップグレードジョブを作成できます。

**重要:**

クラスターIPアドレスを指定した場合、NetScaler Consoleは、指定されたインスタンスに対してのみアップグレード前の検証を実行し、他のクラスターノードに対しては実行しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレード中にプライマリノードとセカンダリノード間の不一致を表示するには、高可用性ノードを選択し、**詳細**をクリックします。


アップグレード前検証レポート(/en-us/netscaler-application-delivery-management-software/media/upgrade-primary-secondary-diff.png)

- **HAのプライマリノードで見つかった構成の不一致** - NetScaler高可用性ペアのセカンダリノードで見つかったが、プライマリノードにはないすべての構成を表示します。
- **HAのセカンダリノードで見つかった構成の不一致** - NetScaler高可用性ペアのプライマリノードで見つかったが、セカンダリノードにはないすべての構成を表示します。

**注:**

構成の不一致セクションに表示される可能性のある以下の不一致は無視できます。

- IPアドレスなどのデバイス固有の構成。
- パスワードが同じであっても、ノード間で異なる可能性のある暗号化されたパスワードまたは証明書。

不一致を確認し、関連性がない場合は無視することを選択できます。

7. **検証スクリプト**で、インスタンスのアップグレード前後に実行するスクリプトを指定します。次のいずれかを実行できます。

   - **デフォルト検証スクリプト** - このオプションを選択して、事前定義された検証スクリプトを実行します。これらのスクリプトは、アップグレードジョブの前後両方で実行され、検証スクリプトの差分レポートを生成します。

     **注:**

     この事前定義されたコマンドセットを変更または編集することはできません。

   - **カスタム検証スクリプト** - このオプションを選択して、独自の検証スクリプトを実行します。スクリプトをアップグレード前またはアップグレード後に実行するかどうかを指定できます。差分レポートは、アップグレードの前後で同じスクリプトが選択されている場合にのみ生成されます。

   各構成のコマンドセットを確認するには、**詳細を表示**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

検証スクリプト(/en-us/netscaler-application-delivery-management-software/media/upgrade-validation-script-ns.png)

「**カスタム検証スクリプト**」で、インスタンスのアップグレード前後に実行するスクリプトを指定します。NetScaler CLIコマンドを実行するには、次のいずれかの方法を使用します。

カスタムスクリプトは、NetScalerインスタンスのアップグレード前後の変更を確認するために使用されます。例:

- アップグレード前後のインスタンスバージョン。
- アップグレード前後のインターフェイス、高可用性ノード、仮想サーバー、およびサービスの状態。
- 仮想サーバーとサービスの統計。
- 動的ルート。

インスタンスのアップグレードには複数の段階があります。これらのスクリプトは、次の段階で実行するように指定できます。

- **アップグレード前**: 指定されたスクリプトは、インスタンスをアップグレードする前に実行されます。
- **アップグレード後フェイルオーバー前 (HAに適用)**: この段階は、高可用性展開にのみ適用されます。指定されたスクリプトは、ノードのアップグレード後、フェイルオーバー前に実行されます。
- **アップグレード後 (スタンドアロンに適用) / アップグレード後フェイルオーバー後 (HAに適用)**: 指定されたスクリプトは、スタンドアロン展開でインスタンスをアップグレードした後に実行されます。高可用性展開では、スクリプトはノードとそのフェイルオーバーをアップグレードした後に実行されます。

**注:**

必要な段階でスクリプトの実行を有効にしてください。そうしないと、指定されたスクリプトは実行されません。

スクリプトファイルをインポートするか、NetScaler Console GUIでNetScaler CLIコマンドを直接入力できます。

- **アップグレード前と同じスクリプトを使用**: アップグレード前、フェイルオーバー前、アップグレード後に同じカスタムスクリプトを使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ファイルからコマンドをインポート**: ローカルコンピューターからNetScaler CLIコマンド入力ファイルを選択します。
- **コマンドの入力**: NetScaler CLIコマンドをGUIに直接入力します。

8. **タスクのスケジュール**で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード** - アップグレードジョブはすぐに実行されます。
   - **後でスケジュール** - このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

     NetScaler HAペアを2段階でアップグレードする場合は、**HA内のノードに対して2段階アップグレードを実行**を選択します。

     HAペア内の別のインスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

     

9. **ジョブの作成**で、次の詳細を指定します。

   a. **ソフトウェアイメージ**リストから次のいずれかのオプションを選択します。

      - **ローカル** - ローカルマシンからインスタンスアップグレードファイルを選択します。
      - **アプライアンス** - ファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler Console GUIには、`/var/mps/mps_images`にあるインスタンスファイルが表示されます。

   b. イメージをインスタンスにアップロードするタイミングを指定します。

      - **今すぐアップロード** - イメージをすぐにアップロードするには、このオプションを選択します。ただし、アップグレードジョブはスケジュールされた時刻に実行されます。
      - **実行時にアップロード** - アップグレードジョブの実行時にイメージをアップロードするには、このオプションを選択します。

      高可用性ペアの場合、イメージをアップロードするノードを指定できます。

      - **プライマリノードとセカンダリノードの両方にアップロード**: ビルドイメージファイルをプライマリノードとセカンダリノードの両方にアップロードします。
      - **セカンダリノードのみにアップロード**: ビルドイメージファイルをセカンダリノードのみにアップロードします。セカンダリノードがアップグレードされると、フェイルオーバーが発生し、ビルドイメージファイルは以前プライマリノードであった新しいセカンダリノードにアップロードされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性ペアで利用可能なスケジューリングシナリオの詳細については、「高可用性ペアのアップグレードジョブのスケジューリング」を参照してください。

- **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップ** - インスタンスのアップグレード後、NetScalerインスタンスにアップロードされたイメージをクリアするには、このオプションを選択します。
- **アップグレードを開始する前にNetScalerインスタンスをバックアップします。** - 選択したNetScalerインスタンスのバックアップを作成します。
- **アップグレード後にHAノードのプライマリおよびセカンダリステータスを維持**: 各ノードのアップグレード後にアップグレードジョブでフェイルオーバーを開始する場合は、このオプションを選択します。このようにして、アップグレードジョブはノードのプライマリおよびセカンダリステータスを維持します。
- **アップグレードを開始する前にNetScaler構成を保存** - NetScalerインスタンスをアップグレードする前に、実行中のNetScaler構成を保存します。
- **NetScaler HAペアでのネットワーク停止を回避するためにISSUを有効にする** - ISSUは、NetScaler高可用性ペアでのゼロダウンタイムアップグレードを保証します。このオプションは、アップグレード中に既存の接続を尊重する移行機能を提供します。そのため、ダウンタイムなしでNetScaler HAペアをアップグレードできます。ISSU移行タイムアウトを分単位で指定します。
- **メールで実行レポートを受信する** - 実行レポートをメールで送信します。メール配布リストを追加するには、「メール配布リストを作成する」を参照してください。
- **Slackで実行レポートを受信する** - 実行レポートをSlackで送信します。Slackプロファイルを追加するには、「Slackプロファイルを作成する」を参照してください。

**ジョブの作成**をクリックします。

アップグレードジョブは、**インフラストラクチャ > アップグレードジョブ**に表示されます。既存のジョブを編集する場合、必要なフィールドがすでに記入されていれば、任意のタブに切り替えることができます。たとえば、**構成の選択**タブにいる場合、**ジョブプレビュー**タブに切り替えることができます。

### スケジュールされたアップグレードジョブの一時停止または再開

スケジュールされたアップグレードジョブを一時停止することもできます。

この機能を使用するには、「**Infrastructure > Upgrade Jobs**」に移動し、既存のスケジュールされたアップグレードジョブを選択して、「**Stop**」をクリックしてジョブを一時停止します。スケジュールされたアップグレードジョブを再開するには、「**Resume**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スケジュールされたジョブを停止または再開する(/en-us/netscaler-application-delivery-management-software/media/upgrade-job-pause-resume.png)

**注：**

アップグレードジョブのスケジュールされた時間が、再開を決定した後で過ぎてしまった場合、アップグレードジョブを再度作成する必要があります。

### 失敗したアップグレードジョブを再試行する

1. 「**Infrastructure > Upgrade Jobs**」で、失敗したアップグレードジョブを選択し、「**Retry**」をクリックします。または、「**Select Action > Retry Upgrade Job**」に移動して、失敗したジョブを再試行することもできます。

   失敗したジョブを再試行する(/en-us/netscaler-application-delivery-management-software/media/retry-failed-job-main-page.png)

2. 「**Select Instance**」で、次の詳細を指定します。

   - **ジョブ名** - アップグレードの名前を入力します。
   - リストからアップグレードするNetScalerインスタンスを選択します。インスタンスを削除するには、「**Remove**」をクリックします。

   「**Next**」をクリックして検証プロセスを開始します。

   失敗したジョブを再試行する(/en-us/netscaler-application-delivery-management-software/media/retry-job-select-instance.png)

3. 「**Pre-upgrade validation**」タブには、次のセクションが表示されます。

   - **アップグレード準備完了インスタンス**。これらのインスタンスのアップグレードを続行できます。
   - **アップグレードがブロックされたインスタンス**。これらのNetScalerインスタンスは、アップグレード前の検証エラーのため、アップグレードがブロックされています。

     エラーを確認し、修正してから、**アップグレード準備完了に移動**をクリックしてアップグレードできます。インスタンスのディスク容量が不足している場合は、ディスク容量を確認してクリーンアップできます。参照: NetScalerディスク容量のクリーンアップ。
   - **ポリシーチェック**: NetScaler Consoleがサポートされていないクラシックポリシーを検出した場合、それらのポリシーを削除してアップグレードジョブを作成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

失敗したジョブを再試行(/en-us/netscaler-application-delivery-management-software/media/retry-job-pre-upgrade-validate.png)

**次へ**をクリックします。

4. **タスクのスケジュール**で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード**: アップグレードジョブはすぐに実行されます。
   - **後でスケジュール**: このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

   失敗したジョブを再試行(/en-us/netscaler-application-delivery-management-software/media/retry-job-schedule-task.png)

   **再試行**をクリックします。

### NetScalerディスク容量のクリーンアップ

NetScalerインスタンスのアップグレード中にディスク容量不足の問題が発生した場合は、NetScaler Console GUIからディスク容量をクリーンアップしてください。

1. **アップグレード前検証**タブの**アップグレードがブロックされたインスタンス**セクションには、ディスク容量不足のためにアップグレードに失敗したインスタンスが表示されます。ディスク容量の問題があるインスタンスを選択します。
2. **ディスク容量の確認**をクリックします。

   **ディスク容量の詳細**ページが表示されます。このページには、インスタンス、使用済みメモリ、および利用可能なメモリが表示されます。

   ディスク容量の詳細(/en-us/netscaler-application-delivery-management-software/media/upgrade-instance-disk-cleanup.png)
3. 「**ディスクスペースの詳細**」ペインで、クリーンアップが必要なインスタンスを選択し、次のいずれかを実行します。

   a. **ディスククリーンアップ** - 必要なフォルダーまたはディレクトリに移動し、それらを削除してディスクスペースを解放します。
   b. **クイッククリーンアップ** - 複数のフォルダーを削除して、ディスクスペースをすばやくクリアします。表示される「**確認**」ペインで、削除するフォルダーを選択し、「**はい**」をクリックします。

      クイッククリーンアップ(/en-us/netscaler-application-delivery-management-software/media/upgrade-quick-cleanup-confirm.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. ディスクスペースをクリアした後、インスタンスをアップグレードするのに十分なディスクスペースが利用可能になったかどうかを確認できます。「**アップグレードがブロックされているインスタンス**」セクションで、「**再検証**」をクリックします。

次の例では、ディスクスペースが利用可能です。これで、「**アップグレード準備完了に移動**」をクリックしてインスタンスをアップグレードするか、「**次へ**」をクリックして次のステップに進むことができます。

クリーンアップの検証(/en-us/netscaler-application-delivery-management-software/media/upgrade-cleanup-revalidate.png)

### NetScaler®高可用性ペアのアップグレードジョブのスケジュール設定

次の表に、「**タスクのスケジュール**」ページでのさまざまなスケジュール設定シナリオと、「**ジョブの作成**」ページで利用可能な対応するアップグレードオプションを示します。

| アップグレードジョブをいつ実行しますか？ | ソフトウェアイメージをNETSCALERにいつアップロードしますか？ | ビルドイメージをHAノードにどのようにアップロードしますか？ |
|---|---|---|
| **今すぐアップグレード** | 該当なし | **プライマリノードとセカンダリノードの両方にアップロード** (デフォルトオプション) |
| | **セカンダリノードにのみアップロード** | |
| **後でスケジュール** | **実行時にアップロード** (デフォルトオプション) | **プライマリノードとセカンダリノードの両方にアップロード** (デフォルトオプション) |
| | **セカンダリノードにのみアップロード** | |
| | **今すぐアップロード** | 該当なし |
| **後でスケジュール** (「**HAのノードに対して2段階アップグレードを実行**」が選択されている場合) | **実行時にアップロード** (デフォルトオプション) | **セカンダリノードにのみアップロード** (デフォルトかつ唯一のオプション) |
| | **今すぐアップロード** | 該当なし |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScalerアップグレードジョブの結合差分レポートをダウンロードする

カスタムスクリプトが指定されている場合、NetScalerアップグレードジョブの差分レポートをダウンロードできます。差分レポートには、アップグレード前スクリプトとアップグレード後スクリプトの出力間の差異が含まれています。このレポートを使用すると、アップグレード後にNetScalerインスタンスでどのような変更が発生したかを判断できます。

**注**

差分レポートは、アップグレード前とアップグレード後の段階で同じスクリプトを指定した場合にのみ生成されます。

アップグレードジョブの差分レポートをダウンロードするには、次の手順を実行します。

1. **インフラストラクチャ > アップグレードジョブ** に移動します。
2. 差分レポートをダウンロードするアップグレードジョブを選択します。
3. **差分レポート** をクリックします。
4. **差分レポート** で、選択したアップグレードジョブの統合差分レポートをダウンロードします。

   このページでは、次のいずれかの差分レポートをダウンロードできます。

   - **アップグレード前とアップグレード後（フェイルオーバー前）の差分レポート**
   - **アップグレード前とアップグレード後の差分レポート**

   NetScaler アップグレードジョブの差分レポートをダウンロードする(/en-us/netscaler-application-delivery-management-software/media/diff-reports-page.png)

# セキュリティアドバイザリ

安全でセキュア、かつ回復力のあるインフラストラクチャは、あらゆる組織にとって生命線です。組織は、新しい共通脆弱性識別子 (CVE) を追跡し、インフラストラクチャに対する CVE の影響を評価する必要があります。また、脆弱性を解決するための修復策を理解し、計画する必要もあります。

NetScaler Console のセキュリティアドバイザリ機能を使用すると、次のことができます。

- NetScaler の構成設定を分析して、システムを攻撃にさらす可能性のある誤った構成、弱点、またはベストプラクティスからの逸脱を特定します。
- 新しい共通脆弱性識別子 (CVE) を追跡し、CVE の影響を評価し、修復策を理解し、脆弱性を解決します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ビルドファイルの整合性を検査します。

## セキュリティアドバイザリのランディングページ

セキュリティアドバイザリのランディングページでは、NetScaler 展開のセキュリティ体制を包括的に俯瞰できます。このインターフェイスは、管理者とセキュリティ専門家が NetScaler インフラストラクチャ全体の健全性と脆弱性の状態を即座に把握できるように強化および設計されています。

NetScaler Console は、次の 3 種類のセキュリティアドバイザリを提供します。

- **セキュアな構成の推奨事項** - ベストプラクティスに従って NetScaler インスタンスを構成できます。
- **共通脆弱性識別子 (CVE) の検出** - NetScaler インスタンスを危険にさらしている CVE を特定し、修復策を推奨します。
- **ファイル整合性監視** - NetScaler ビルドファイルに変更や追加が行われたかどうかを特定できます。



NetScaler Console セキュリティアドバイザリダッシュボードには、次のものも含まれます。

- **全体的なセキュリティ体制の重大度** - セキュリティ体制のステータスを表し、3 種類のアドバイザリの最大重大度に基づいて計算されます。ステータスは次のいずれかになります。
  - **重大**: 複数の重大な観測事項が検出され、最優先で対処する必要があります。
  - **高**: 直ちに修正する必要がある重大な脆弱性または設定ミスが検出されました。重大な発見ほど緊急ではありませんが、これらの問題はセキュリティと安定性に重大なリスクをもたらします。
  - **中**: 適時に対応する必要がある重要なセキュリティ観測事項。これらの問題は差し迫った重大な脅威ではありませんが、対処しないまま放置すると、悪用されたり、より深刻な問題につながる可能性があります。
  - **低**: 重大なセキュリティリスクをもたらさない軽微なセキュリティ問題またはベストプラクティス違反。これらは差し迫った脅威ではありませんが、全体的なセキュリティ体制を改善するためにこれらの問題を修正することをお勧めします。
- **最終スキャン** - 最終スキャンの日付。ダッシュボードに表示されるデータは、最終スキャンの結果に基づいています。
- **次回のスケジュール済みスキャン** - 次回のスケジュール済みシステムスキャンの日付。
- **スケジュール済みスキャン頻度** - システムスキャンが実行される頻度。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **今すぐスキャン** - システムスキャンとは別に、必要に応じていつでもインスタンスをスキャンできるオンデマンドスキャンを許可します。
- **スキャン履歴** - NetScalerインスタンスで実行されたすべてのスキャンの履歴ビューを提供します。
- **影響を受けるNetScaler** - 影響を受けるNetScalerインスタンスを一覧表示します。
- **設定** - 必要に応じて、システムスキャン設定を構成し、イベントの通知を設定できます。

ダッシュボードで利用可能な情報により、重大な脆弱性、緩和策を含む安全な構成の推奨事項、および関連ドキュメントへのリンクを迅速に特定できます。

ランディングページでは、重要度とNetScaler IPアドレスで問題をフィルタリングできます。特定の重要度レベルが選択されている場合、その重要度レベルのNetScalerインスタンスのみが表示されます。

**重要:**

**セキュリティアドバイザリ**のGUIまたはレポートでは、すべてのCVEが表示されない場合があり、1つのCVEしか表示されない場合があります。回避策として、**今すぐスキャン**をクリックし、**CVE**を選択してオンデマンドスキャンを実行します。スキャンが完了すると、対象となるすべてのCVE（約15個）がUIまたはレポートに表示されます。-->

## セキュア構成の推奨事項

**セキュア構成の推奨事項**タブは、構成の観測結果について詳細なインスタンスレベルの分析を提供し、ユーザーが実用的な洞察を得られるように設計されています。詳細については、「セキュア構成の推奨事項」を参照してください。

## CVE検出

CVE検出は、主にセキュリティの脆弱性を特定し、軽減することに焦点を当てています。詳細については、「CVE検出」を参照してください。

## ファイル整合性監視

ファイル整合性監視は、NetScalerインスタンスのコアファイルに対する不正または悪意のある変更をチェックします。これはセキュリティアドバイザリの重要な部分です。詳細については、「ファイル整合性監視」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 今すぐスキャン

必要に応じていつでもインスタンスをスキャンでき、セキュリティ要件に基づいて実行するスキャンの種類を選択することもできます。

スキャンを実行するには、次の手順を実行します。

1. **今すぐスキャン**をクリックします。

   

2. 実行するスキャンの種類を選択します。

   - セキュリティ構成の推奨事項
   - CVE検出
   - ファイル整合性監視

   Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/scan-now-options.png)

3. **Scan Now**をクリックします。スキャンが完了すると、更新されたセキュリティの詳細がセキュリティアドバイザリダッシュボードに表示されます。

## スキャン履歴

**Scan History**をクリックすると、NetScalerインスタンスで実行されたすべての過去のスキャンを表示できます。

Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/scan-history.png)

スキャンタイプ（オンデマンドスキャンまたはシステムスキャン）、スキャンの開始時刻と終了時刻、全体的なスキャンステータスを表示でき、各スキャンの詳細をCSVまたはPDF形式でダウンロードすることもできます。

Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/scan-history-details.png)

## 影響を受けるNetScaler

**NetScalers Impacted**セクションには、セキュリティ構成、CVE、およびファイル整合性監視チェックによって影響を受けるすべてのNetScalerインスタンスが一覧表示されます。

Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/netscalers-impacted.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**SECURE RECOMMENDATION CONFIGURATION**、**CVE DETECTION**、または**FILE INTEGRITY MONITORING**の下の数字をクリックして、詳細を表示することもできます。以下は参考用のサンプル画像です。

Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/netscalers-impacted-details.png)

## 設定

管理者として、Citrix Cloud通知を受信できます。これにより、CVEによって脆弱なNetScalerインスタンスの数が通知されます。通知を受信するタイミングと方法を設定するには、セキュリティアドバイザリページの右上隅にある設定アイコンをクリックします。

Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/security-advisory-settings-icon.png)

次のアクションを実行できます。

- 通知を受け取る必要のあるイベントの種類を選択します。
- 通知の受け取り方法を選択します。たとえば、メール、Slack、PagerDuty などです。
- システムスキャンに含める必要のあるスキャンの種類を選択します。デフォルトでは、システムスキャンに対してCVEスキャンのみが有効になっています。
- セキュリティアドバイザリのカスタムスキャンをオプトアウトします。

システムスキャンに含める必要のあるスキャンの種類を設定することもできます。

Citrix Cloud通知(/en-us/netscaler-application-delivery-management-software/media/secuirty-advisory-settings.png)

**免責事項:**

NetScalerファイル整合性監視（「本機能」）は、脅威アクターが関連環境を標的とする際に使用する可能性のあるすべての手法、戦術、手順（TTP）を検出できるわけではないことにご注意ください。脅威アクターはTTPとインフラストラクチャを頻繁に変更するため、本機能は特定の脅威に関して法医学的価値が限定的であるか、まったくない場合があります。あらゆる可能性のある脅威に関連して環境を評価するために、経験豊富な法医学調査員のサービスを保持することを強くお勧めします。

本ドキュメントおよびその中に含まれる情報は現状有姿で提供されます。Cloud Software Group, Inc.は、本ドキュメントまたはその内容に関して、明示的か黙示的かを問わず、いかなる保証また

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

は表明も行いません。これには、本ドキュメントまたはその中に含まれる情報がエラーフリーであること、または商品性や特定の目的への適合性のいかなる条件も満たすことの保証は含まれませんが、これらに限定されません。

## セキュアな構成の推奨事項

NetScalerのセキュアな構成アドバイザリは、NetScaler構成のセキュリティ体制を強化するための専門的な推奨事項と具体的な指示を提供する包括的なガイドとして機能します。この機能により、潜在的な脆弱性や進化するサイバー脅威からアプリケーションデリバリーコントローラー (ADC) インフラストラクチャを保護できます。推奨されるガイドラインを綿密に遵守することで、リスクを積極的に軽減し、システムの回復力を高め、不正アクセスや悪意のある活動に対する堅牢な防御を維持できます。

この機能は、NetScaler構成の潜在的な脆弱性をスキャンするだけでなく、それらの構成を修正するための正確なコマンドを積極的に提案します。ネットワーク管理者は、セキュリティギャップを迅速に特定し、NetScalerの展開を強化するために必要な変更を実装できます。

**セキュアな構成の推奨事項**タブは、潜在的な構成の脆弱性に対処するための優先順位付けされたアプローチを可能にするため、重要度別に細心の注意を払って分類された包括的なビューを提供します。

### 重要度に基づく優先順位付け

重要度による分類により、ユーザーは効率的に作業を割り当てることができます。観測結果は通常、次のような階層に分類されます。

- **クリティカル**: NetScalerインスタンスのセキュリティと整合性に即座に重大なリスクをもたらす問題。これらの問題は、最優先で対処する必要があります。
- **高**: 悪用された場合、重大なセキュリティ侵害につながる可能性のある構成であり、迅速な対応が必要です。
- **中**: 潜在的な弱点や誤った構成を示す観測結果。これらの問題はクリティカルではありませんが、対処せずに放置すると、より大きなセキュリティインシデントにつながる可能性があります。
- **低**: 全体的なセキュリティ体制を向上させるための軽微な推奨事項またはベストプラクティス。これらの問題は、差し迫った脅威を表すものではありません。

### 詳細なインスタンスレベルビューの利点

- **ターゲットを絞った修復**: 一般的なアドバイスではなく、各NetScalerインスタンスに合わせた具体的な推奨事項がユーザーに提供され、正確で効果的な修復が保証されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **攻撃対象領域の削減**: 観測された誤った構成に体系的に対処することで、組織は攻撃対象領域を大幅に削減し、悪用が成功する可能性を最小限に抑えることができます。
- **コンプライアンス遵守**: 詳細な観測結果は、組織が規制コンプライアンス標準 (例: GDPR、HIPAA、PCI DSS) に違反する可能性のある構成を特定し、修正するのに役立ちます。
- **セキュリティ体制の向上**: 構成の弱点を積極的に特定して解決することで、全体的なセキュリティ体制が強化され、サイバー脅威に対する回復力が高まります。
- **運用効率**: 明確で実用的な洞察を提供することで、システムはセキュリティ修復プロセスを効率化し、時間とリソースを節約します。

優先順位、リスク許容度、利用可能なリソースに基づいて、どの観測結果に最初に対処するかを**選択**できます。この柔軟性により、最も差し迫ったセキュリティ上の懸念が遅滞なく対処されると同時に、時間の経過とともに包括的な構成強化を実現するために必要な情報が提供されます。このオプションにより、セキュリティ管理者は情報に基づいた意思決定を行い、NetScalerの展開を保護するための断固たる行動を取ることができます。

フリーテキスト検索機能を使用すると、さまざまな主要識別子に基づいて結果を絞り込むことができます。たとえば、一意のホスト名でインスタンスを効率的に検索でき、特定のデバイスを特定する直接的な方法を提供します。あるいは、IPアドレスで検索すると、インスタンスを特定する別の正確な方法が提供され、特にネットワーク中心の環境で役立ちます。

基本的な識別を超えて、検索はNetScalerモデルによるフィルタリングもサポートしています。これは、MPX、SDX、VPXなどのモデルを指定して、特定のハードウェアまたはソフトウェアカテゴリに属するインスタンスのみを表示できることを意味します。また、重要度レベルで検索を絞り込むこともでき、情報アラートから重大な警告まで、インスタンスの重要度に基づいて優先順位を付けることができます。

### 構成推奨事項の修復

構成の観測結果を評価し、どれがアクションを必要とするかを判断すると、推奨される構成の包括的なビューが表示されます。その後、システムは以下の画像に示すように、選択内容に合わせて調整された修復手順を表示する専用ページを表示します。たとえば、特定のNetScalerインスタンス（この特定のシナリオではIPアドレス10.102.56.45のインスタンス）の重大度が高い問題のみに対処することを選択した場合、ページには関連する優先度の高い推奨事項が動的に表示され、修復プロセスを効果的にガイドします。

構成の推奨事項は、次の2つのタイプに分類できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ユーザー入力が必要な推奨事項**: このカテゴリには、NetScaler管理者またはセキュリティチームからの特定の状況に応じた情報または決定を必要とする構成の提案が含まれます。これらは通常、一般的なデフォルト値が適切でない場合や、最適な設定が固有の運用環境、セキュリティポリシー、またはアプリケーション要件に依存する場合のシナリオです。以下にいくつかの推奨事項の例を示します。

  - **特定のIPアドレスまたはIP範囲の定義**: たとえば、信頼できる内部サブネットまたは特定のクライアントIPアドレスからのトラフィックのみを許可するようにファイアウォールルールを構成する場合などです。システムはこれらの固有のネットワーク詳細を推測できません。
  - **カスタムポート番号の設定**: 多くのサービスには標準ポートが存在しますが、アプリケーションはセキュリティまたは運用上の理由から非デフォルトポートを使用するように構成されている場合があります。ネットワーク管理者はポート番号を指定する必要があります。
  - **ホスト名またはドメイン名の指定**: SSL証明書、ロードバランシング仮想サーバー、またはコンテンツスイッチングポリシーを構成する場合、NetScalerインスタンスが提供または対話する正確なホスト名またはドメイン名をユーザーが指定する必要があります。
  - **認証サーバーの詳細の提供**: NetScalerをLDAP、RADIUS、SAML、OAuthなどの外部認証システムと統合するには、ユーザーがサーバーIPアドレス、共有シークレット、ディレクトリパス、およびその他のプロトコル固有の詳細を入力する必要があります。
  - **特定のURL書き換えまたはコンテンツスイッチングポリシーの設定**: これらの高度な機能の正確なURL、パターン、およびターゲットの宛先は、アプリケーションアーキテクチャに非常に固有のものであり、ユーザーが定義する必要があります。
  - **影響**: これらの推奨事項は、多くの場合、デプロイメントの特定のニーズ、セキュリティポリシー、およびネットワークトポロジに関するより深い理解を必要とします。ユーザー入力のエラーは、サービスの中断やセキュリティの脆弱性につながる可能性があり、慎重な計画と検証の必要性を強調しています。これらを実装する自動ツールまたはスクリプトは、通常、必要なパラメータを要求するか、構成ファイルから読み取ります。

- **ユーザー入力を必要としない推奨事項**: このカテゴリには、普遍的に適用できる構成の提案、または固有の環境変数に依存しない標準的なベストプラクティスが含まれます。これらは、多くの場合、ほとんどのNetScalerデプロイメントで有益な基本的なセキュリティ強化またはパフォーマンス最適化です。以下に、いくつかの推奨事項の例を示します。

  - **脆弱な暗号またはプロトコルの無効化**: SSLv3やTLS 1.0などのSSL/TLSバージョン、または特定の脆弱な暗号スイート（例：RC4、3DES）を無効にすることをお勧めします。これらは既知の脆弱性であり、それらを削除することは普遍的なセキュリティのベストプラク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ティスです。システムは、どの暗号が脆弱であるかを知るために特定の入力を必要としません。

- **HTTP Strict Transport Security (HSTS) の有効化**: これは、Webブラウザによって適用されるポリシーであり、安全なHTTPS接続を使用してサーバーと対話することのみを許可します。これを有効にすることは、標準的なセキュリティ強化手順です。
- **セキュアなCookieフラグの設定（例：`Secure`、`HttpOnly`）**: これらのフラグはセッションCookieのセキュリティを強化し、暗号化されていないチャネルを介して送信されたり、クライアントサイドスクリプトを介してアクセスされたりするのを防ぎます。その適用は一般的な推奨事項です。
- **一般的なセキュリティヘッダーの有効化**: X-Frame-Options、X-Content-Type-Options、Content-Security-Policy（デフォルトの安全なポリシーを使用）などのヘッダーは、クライアントサイドのセキュリティを普遍的に向上させるため、特定のユーザー入力なしで推奨できます。
- **一般的な攻撃に対するデフォルトのレート制限の実装**: カスタムレート制限には入力が必要な場合がありますが、一般的な攻撃ベクトル（例：過剰なログイン失敗試行）に一般的なレート制限を適用するという推奨事項は、ベースラインとして適用できる場合があります。
- **最適なバッファサイズまたはタイムアウトの構成**: 特定のアプリケーションロジックではなく、システムアーキテクチャによって決定される内部バッファサイズまたは接続タイムアウトに関連する一般的なパフォーマンス推奨事項。
- **セキュリティイベントの適切なログレベルの確保**: セキュリティ関連イベントの特定のログレベルを確保するという推奨事項は、監査およびインシデント対応のための一般的なベストプラクティスです。

- **影響**: これらの推奨事項は、多くの場合、自動化またはベースライン構成スクリプトの優れた候補となります。特定の詳細について手動での介入を必要とせずに、複数のNetScalerインスタンスに均一に適用できるためです。これらは、一般的な脆弱性に対処し、広く受け入れられている標準を適用することで、強力なセキュリティ体制に貢献します。

要約すると、ユーザー入力要件に基づいて構成推奨事項を分類することで、実装プロセスが合理化されます。入力を必要とする推奨事項は、ユーザーからの慎重なデータ収集と検証を必要とし、入力を必要としない推奨事項は、標準的なセキュリティベースラインとして、または自動デプロイメカニズムを通じて適用できることがよくあります。

ユーザーが対処する構成を決定すると、既存の構成ジョブワークフローが引き継ぎ、構成変更をプッシュします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例えば、ユーザー入力を必要とする構成推奨事項の例を次に示します。構成値を1つずつ入力することも、次の画像に示すように、構成値を含むファイルをアップロードすることもできます。

構成ジョブの作成(/en-us/netscaler-application-delivery-management-software/media/create-config-job.png)

## CVE検出

NetScalerは、インスタンスのバージョン、構成、システムファイルをスキャンして脆弱性を特定することにより、CVEを検出します。更新されたCVEリポジトリを使用し、詳細な影響分析と修復の提案を提供します。

**Security Advisory**ダッシュボードの**CVE検出**セクションには、次の項目が一覧表示されます。

- 検出されたCVEの数
- 影響を受けるNetScalerインスタンスの数
- 最終スキャン実行日
- 重大度別に、緊急、高、中、低に分類された影響を受けるNetScalerインスタンス

管理者として、NetScalerに定期的にスケジュールされたシステムスキャンを実行させることも、必要に応じてオンデマンドスキャンを実行することもできます。

- **システムスキャン** - デフォルトですべての管理対象インスタンスをスキャンします。NetScaler Consoleがシステムスキャンの日時を決定するため、変更することはできません。
- **オンデマンドスキャン** - 必要に応じてインスタンスを手動でスキャンできます。前回のシステムスキャンからかなりの時間が経過している場合は、オンデマンドスキャンを実行して現在のセキュリティ体制を評価できます。または、修正が適用された後にスキャンを実行して、改訂された体制を評価することもできます。オンデマンドスキャンを実行するには、セキュリティアドバイザリで**今すぐスキャン**をクリックします。

**CVE検出**セクションをクリックすると、詳細情報を表示できます。

**CVE検出**セクションには、次の2つのビューがあります。

- インスタンスビュー
- CVE ビュー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### インスタンスビュー

インスタンスビューには、**影響を受けるインスタンス**タブと**CVE リポジトリ**タブがあります。

**影響を受けるインスタンス**タブには、影響を受けるNetScalerインスタンスのリストが表示されます。



影響を受けるインスタンスは、次のフォームファクターに基づいて分類されます。

- MPX および VPX
- SDX
- CPX
- BLX

次の条件に基づいてインスタンスを検索することもできます。

- CVE 検出済み
- ホスト名
- モデル
- NetScalerインスタンス
- 状態

表には次の詳細が表示されます。

- NetScaler IPアドレス
- ホスト名
- NetScalerのモデル番号
- NetScalerの状態
- ソフトウェアのバージョンとビルド
- NetScalerに影響を与えるCVEのリスト。

ほとんどのCVEは修正としてアップグレードが必要ですが、アップグレードと追加の手順が必要なものもあります。

- CVE-2020-8300の修正については、「CVE-2020-8300の脆弱性を修正する」を参照してください。
- CVE-2021-22927およびCVE-2021-22920については、「CVE-2021-22927およびCVE-2021-22920の脆弱性を修正する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CVE-2021-22956については、「CVE-2021-22956の脆弱性を特定して修正する」を参照してください。
- CVE-2022-27509については、「CVE-2022-27509の脆弱性を修正する」を参照してください。

> **注**
>
> NetScalerインスタンスにカスタマイズがある場合は、NetScalerのアップグレードを計画する前に、「カスタマイズされたNetScaler構成のアップグレードに関する考慮事項」を参照してください。

脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードできます。アップグレードするには、次のいずれかを実行します。

- **アップグレードワークフロー** - インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。
- **構成ジョブワークフロー** - インスタンスを選択し、**構成ジョブワークフロー**をクリックします。

アップグレードワークフローが開始され、脆弱なNetScalerがターゲットNetScalerとして自動入力されます。NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。

> **注:**
>
> - リリース13.0、12.1、12.0、11.0、10.5、およびそれ以前のバージョンは、すでにサポート終了（EOL）となっています。NetScalerインスタンスがこれらのリリースのいずれかで実行されている場合は、サポートされているリリースにアップグレードしてください。
> - アップグレードしたいリリースとビルドは、お客様の判断に委ねられます。どのリリースとビルドにセキュリティ修正が含まれているかについては、修復列のアドバイスを参照してください。そして、まだサポート終了に達していない、サポートされているリリースとビルドを適切に選択してください。

CVEビューに切り替えるには、**CVEビューに切り替える**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CVEビュー

CVEビューには、インフラストラクチャに影響を与えるすべてのCVEと、影響を受けるすべてのNetScalerインスタンスの結果が表示され、修復が提案されます。この情報を使用して、セキュリティリスクを修正するための修復を適用できます。



NetScalerインスタンスに影響を与えるCVEの数を示す表には、次の詳細が含まれています。

- **CVE ID**: インスタンスに影響を与えるCVEのID。
- **公開日**: そのCVEのセキュリティ速報がリリースされた日付。
- **深刻度スコア**: 深刻度の種類（高/中/重大）とスコア。スコアを表示するには、深刻度の種類にカーソルを合わせます。
- **脆弱性の種類**: このCVEの脆弱性の種類。
- **影響を受けるNetScalerインスタンス**: CVE IDが影響を与えているインスタンスの数。ホバーすると、NetScalerインスタンスのリストが表示されます。
- **修正**: 利用可能な修正策。通常はインスタンスのアップグレード、または構成パックの適用です。

同じインスタンスが複数のCVEの影響を受ける可能性があります。この表は、特定の1つのCVEまたは選択された複数のCVEがいくつのインスタンスに影響を与えているかを確認するのに役立ちます。影響を受けるインスタンスのIPアドレスを確認するには、**影響を受けるNetScalerインスタンス**の下にあるNetScalerの詳細にカーソルを合わせます。影響を受けるインスタンスの詳細を確認するには、表の下部にある**影響を受けるインスタンスを表示**をクリックします。 プラス記号をクリックして、表の列を追加または削除することもできます。

### CVEリポジトリ

インスタンスビューとCVEビューの両方に**CVEリポジトリ**タブがあります。このタブには、2019年12月以降にCitrixが発表した、NetScalerインフラストラクチャに影響を与える可能性のあるすべてのNetScaler関連CVEの詳細が表示されます。

- CVE ID
- 脆弱性の種類
- 公開日
- 重大度レベル
- 修正
- セキュリティ速報へのリンク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このビューを使用して、セキュリティアドバイザリの範囲内のCVEを理解し、CVEについて詳しく知ることができます。サポートされていないCVEについては、「セキュリティアドバイザリでサポートされていないCVE」を参照してください。

### 注意事項

- セキュリティアドバイザリは、ライフサイクル終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。
- CVE検出でサポートされるインスタンス: すべてのNetScaler (SDX、MPX、VPX) およびGateway。
- ファイル整合性監視でサポートされるインスタンス: MPX、VPXインスタンス、およびGateway。
- サポートされるCVE: 2019年12月以降のすべてのCVE。

  **注:**

  Windows用NetScaler Gatewayプラグインに影響を与える脆弱性の検出と修復は、NetScaler Consoleセキュリティアドバイザリではサポートされていません。サポートされていないCVEの詳細については、セキュリティアドバイザリでサポートされていないCVEを参照してください。

- NetScaler Consoleセキュリティアドバイザリは、脆弱性を特定する際に、いかなる種類の機能の誤設定も考慮しません。
- NetScaler Consoleセキュリティアドバイザリは、CVEの特定と修復のみをサポートします。セキュリティ記事で強調されているセキュリティ上の懸念の特定と修復はサポートしていません。
- NetScaler、Gatewayリリースの範囲: この機能はメインビルドに限定されています。セキュリティアドバイザリには、特別なビルドは含まれません。
  - セキュリティアドバイザリは、管理パーティションではサポートされていません。
- CVEで利用可能なスキャンタイプは次のとおりです。
  - **バージョンスキャン**: このスキャンでは、NetScaler ConsoleがNetScalerインスタンスのバージョンと、修正が利用可能なバージョンおよびビルドを比較する必要があります。このバージョン比較により、NetScaler Consoleセキュリティアドバイザリは、NetScalerがCVEに対して脆弱であるかどうかを特定できます。たとえば、CVEがNetScalerリリースお

© 1997–2026 Citrix Systems, Inc. All rights reserved.

よびビルドxx.yyで修正されている場合、セキュリティアドバイザリは、xx.yyより低いビルドのすべてのNetScalerインスタンスを脆弱であると見なします。バージョンスキャンは現在、セキュリティアドバイザリでサポートされています。

- **設定スキャン**: このスキャンでは、NetScaler ConsoleがCVEスキャンに固有のパターンをNetScaler設定ファイル (`nsconf`) と照合する必要があります。特定の構成パターンがNetScaler ns.confファイルに存在する場合、そのインスタンスはそのCVEに対して脆弱であると見なされます。このスキャンは通常、バージョンスキャンと組み合わせて使用されます。 設定スキャンは現在、セキュリティアドバイザリでサポートされています。
- **カスタムスキャン**: このスキャンでは、NetScaler Consoleが管理対象のNetScalerインスタンスに接続し、スクリプトをプッシュして実行する必要があります。スクリプトの出力は、NetScaler ConsoleがNetScalerがCVEに対して脆弱であるかどうかを特定するのに役立ちます。例としては、特定のシェルコマンド出力、特定のCLIコマンド出力、特定のログ、特定のディレクトリまたはファイルの存在または内容などがあります。カスタムスキャンを必要とするCVEの場合、スケジュールされたスキャンまたはオンデマンドスキャンが実行されるたびにスクリプトが実行されます。収集されたデータと特定のカスタムスキャンのオプションについては、そのCVEのセキュリティアドバイザリドキュメントを参照してください。

- スキャンはNetScaler上の本番トラフィックに影響を与えず、NetScaler上のNetScaler設定を変更することもありません。
- NetScaler Console Security Advisory は CVE 軽減をサポートしていません。NetScaler インスタンスに軽減策（一時的な回避策）を適用した場合でも、修正が完了するまで、NetScaler Console はその NetScaler を脆弱な NetScaler として識別し続けます。
- FIPS インスタンスの場合、CVE スキャンはサポートされていません。

## ファイル整合性監視

ファイル整合性監視により、NetScalerファイルシステムに変更や追加が行われたかどうかを特定できます。この機能は、現在のNetScalerビルドのバイナリハッシュ値を、同じNetScalerビルドにリンクされている元のバイナリハッシュと比較することで、NetScalerファイルの整合性を評価します。

**セキュリティアドバイザリ**ダッシュボードの**ファイル整合性監視**セクションには、次の情報が一覧表示されます。

- 検出された問題の数
- 影響を受けるNetScalerインスタンスの数
- 最終スキャン実行日

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 重大度（緊急、高、中、低）別に分類された、影響を受けるNetScalerインスタンス
- バイナリ署名と検証を使用して問題を報告した、影響を受けるNetScalerインスタンス



管理者として、定期的にスケジュールされたシステムスキャンをNetScalerに実行させることができます。また、必要に応じてオンデマンドスキャンを実行することもできます。

- **システムスキャン** - デフォルトですべての管理対象インスタンスをスキャンします。NetScaler Consoleがシステムスキャンの日時を決定し、デフォルトでは無効になっています。
- **オンデマンドスキャン** - 必要に応じて手動でスキャンをトリガーできます。オンデマンドスキャンを実行するには、セキュリティアドバイザリダッシュボードで**今すぐスキャン**をクリックします。

**ファイル整合性監視**セクションをクリックすると、詳細情報を表示できます。

### コンソール検出

**Console-Detected**タブには、現在のビルドのバイナリハッシュを元のビルドハッシュと比較して、変更または新規追加されたファイルを検出することで、影響を受けるNetScalerインスタンスが一覧表示されます。この表には、次の詳細が表示されます。

- IPアドレス - 影響を受けるインスタンスのIPアドレスです。
- スキャンステータス - スキャンエラーの結果を表示します。
- 既存ファイルの変更 - 変更された既存ファイルのリストです。
- 新規ファイルの追加 - 追加された新規ファイルのリストです。
- スキャン時間 - 最終スキャンの時刻です。
- ホスト名 - 影響を受けるNetScalerのホスト名です。
- モーダル - 影響を受けるNetScalerのモーダル名です。

スキャンエラーの結果はメインダッシュボードビュー内に表示されるため、エラーの詳細にアクセスするために個々のスキャン結果や項目をクリックする必要はありません。ハッシュの不一致やスキャンエラーなどの整合性に関する問題は、ダッシュボード上で明確でアクセスしやすい形式で表示され、問題を迅速に特定し理解するのに役立ちます。

**既存ファイルの変更**および**新規ファイルの追加**の下の数字をクリックして、詳細を表示します。



カスタム許可リストを作成し、特定のファイルをファイル整合性監視スキャンから除外できます。スキャンから除外するファイルを定義することで、監視を効率化し、信頼できるファイルに対する不要なアラートを減らすことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ファイル整合性監視スキャンから特定のファイルを除外するには、次の手順を実行します。

1. **ファイル/ディレクトリの除外**をクリックします。
2. 必要なファイルまたはディレクトリを選択します。

   または

   新しいファイルを追加するには、「**ファイル/ディレクトリの追加**」をクリックします。標準のシェルグロブパターンを追加し、定義された条件に一致するパスを除外できます。ディレクトリが追加されると、そのすべてのファイルはスキャンから除外されます。「**追加**」をクリックします。

   特定のファイルやフォルダーを見つけるために検索を実行することもできます。`path` オプションの下にある検索バーにファイルまたはフォルダーの一部を入力して、除外リストのパスを見つけることもできます。検索機能により、除外されたパスの管理と確認が容易になります。

ファイルをスキャンから除外したくない場合は、必要なファイルまたはディレクトリを選択し、「**ファイル/ディレクトリの削除**」をクリックします。指定されたファイルまたはディレクトリは、次回のスケジュールされたスキャンに含まれます。

**注意点**

- ファイル整合性監視でサポートされているインスタンス: MPX、VPXインスタンス、およびGateway。
- ファイル整合性監視で利用可能なスキャンは次のとおりです。
  - **ファイル整合性監視スキャン**: このスキャンでは、NetScaler Consoleが管理対象のNetScalerインスタンスに接続する必要があります。NetScaler Consoleは、NetScalerでスクリプトを実行し、NetScalerシステムファイルの現在のバイナリハッシュ値を収集することで、ハッシュ値の比較を行います。比較後、NetScaler Consoleは、変更された既存ファイルの総数と新しく追加されたファイルの総数を含む結果を提供します。管理者は、スキャン結果に関するさらなる調査のために、組織のデジタルフォレンジックに連絡できます。
- サポートされていないプラットフォームのリストは次のとおりです: BLX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### デバイスレポート

「**デバイスレポート**」タブには、バイナリ署名と検証を使用して問題を報告したNetScalerインスタンスが一覧表示されます。この検証により、各ファイルのデジタル署名が検証され、信頼性が確認され、改ざんが検出されます。影響を受けるインスタンスが見つかった場合は、組織のデジタルフォレンジック活動を進めることができます。この表には、影響を受けるNetScalerインスタンスと、ホスト名、追加されたバイナリ、変更されたバイナリなどのその他の詳細が一覧表示されます。必要なインスタンスに対応する「**詳細**」をクリックすると、詳細情報を表示できます。



## NetScaler Consoleにおける侵害の痕跡の検出

NetScaler Consoleの侵害の痕跡 (IoC) 検出機能は、NetScalerアプライアンスが脆弱性によって潜在的に影響を受けているかどうかを検出するように設計されています。

CVEイベントが発生した場合、最初の懸念事項の1つは、悪意のあるアクターがその脆弱性を悪用できたかどうかです。エクスプロイトは顧客のビジネスに壊滅的な損害をもたらすため、そのようなインシデントを直ちに検出することが重要です。侵害の痕跡は、これまでサポートチャネルを通じてNetScaler向けに配布されてきました。これは顧客のニーズを満たしますが、チケットの発行、サポート担当者との会話といったサポートプロセスを経る追加の労力が必要となり、場合によっては理想的ではないことがあります。NetScaler Consoleの侵害の痕跡検出機能は、現在のサポート中心のプロセスを短絡させ、顧客がNetScalerインフラストラクチャを迅速に評価するのに役立つように設計されています。

### 前提条件

この機能を使用するには、製品使用状況テレメトリを送信する必要があります。NetScalerテレメトリの詳細については、`<https://docs.netscaler.com/ja-jp/netscaler-application-delivery-management-software/current-release/ns-telemetry.html>`を参照してください。

### 利点

- NetScaler Consoleの**セキュリティアドバイザリ**ページから侵害検出スキャンを実行できます。

  

- スキャンは以下のいずれかの結果を提供します。
  - **侵害の可能性あり** – 検出ロジックがCVEに対する潜在的な侵害を検出した場合。
  - **侵害は検出されませんでした** – 検出ロジックが侵害を検出していない場合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **スキップ済み** – 特定のNetScalerインスタンスに対してスキャンが手動でスキップされた場合。
- **実行に失敗しました** – スキャンが正常に実行されなかった場合。
- **実行中** – スキャンが進行中の場合。

- より多くのIoCが発見されるにつれて、IoCロジックは常に更新されます。そのような場合、ホームページには更新が利用可能であることが表示されます。
- IoC検出ロジックのアップデートが利用可能になると、ランディングページで確認できます。



- 以前のスキャンの結果は保存され、いつでも表示できます。



- このソリューションは、ハブアンドスポークアーキテクチャを使用しており、中央のクラウドサービスが安全なクラウドロケーションからアセットを取り込み、それらをターゲットデバイスにインストールします。

**注:**

IoC情報には、脅威アクターが関連環境を標的とする際に使用する可能性のあるすべての手法、戦術、または手順（「TTP」）が含まれているわけではありません。また、脅威アクターはTTPやインフラストラクチャを頻繁に変更します。これらの理由やその他の理由により、IoC情報は法医学的価値が限られている可能性があり、実際の侵害を特定できない場合があります。環境を評価するために、経験豊富な法医学調査員のサービスを利用することをお勧めします。

## セキュリティアドバイザリを介してサポートされるCVE

NetScaler Consoleオンプレミスでは、Cloud Connectまたは自動有効化チャネルを介してセキュリティアドバイザリを有効にしている場合、セキュリティアドバイザリのフルバージョンがサポートされます。詳細については、セキュリティアドバイザリを参照してください。

### 最新のサポートされているCVE

次の表に、セキュリティアドバイザリで特定および修復できる最新のサポートされているCVEの詳細を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| リリース日 | CVE ID | 特定 | 修復 | リソースリンク |
|---|---|---|---|---|
| 27 Sep 2026 | CVE-2026-88771 | バージョンスキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |
| 27 Sep 2026 | CVE-2026-88772 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |
| 27 Sep 2026 | CVE-2026-88773 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |
| 27 Sep 2026 | CVE-2026-88774 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |
| 27 Sep 2026 | CVE-2026-88775 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |
| 27 Sep 2026 | CVE-2026-88776 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| リリース日 | CVE ID | 特定 | 修復 | リソースリンク |
|---|---|---|---|---|
| 27 Sep 2026 | CVE-2026-88777 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードしてください。 | セキュリティ速報 |
| 27 Sep 2026 | CVE-2026-88778 | バージョン スキャンが必要です。 | セキュリティ速報に記載されている推奨ビルドにアップグレードし、構成ジョブを適用します。 | セキュリティ速報 |

**注:**

セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュール内のCVEの影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、 をクリックしてオンデマンドスキャンを開始できます。

### サポートされているCVE

以下は、セキュリティアドバイザリでサポートされている既存のCVEです。

| リリース日 | CVE ID | リソースリンク |
|---|---|---|
| 19 Aug 2026 | CVE-2026-19490 | セキュリティ速報 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| リリース日 | CVE ID | リソースリンク |
|---|---|---|
| 19 Aug 2026 | CVE-2026-19489 | セキュリティ速報 |
| 30 Jun 2026 | CVE-2026-13474 | セキュリティ速報 |
| 30 Jun 2026 | CVE-2026-10817 | セキュリティ速報 |
| 30 Jun 2026 | CVE-2026-10816 | セキュリティ速報 |
| 30 Jun 2026 | CVE-2026-8655 | セキュリティ速報 |
| 30 Jun 2026 | CVE-2026-8452 | セキュリティ速報 |
| 30 Jun 2026 | CVE-2026-8451 | セキュリティ速報 |
| Mar 23, 2026 | CVE-2026-4368 | セキュリティ速報 |
| Mar 23, 2026 | CVE-2026-3055 | セキュリティ速報 |
| Nov 11, 2025 | CVE-2025-12101 | セキュリティ情報 |
| Aug 26, 2025 | CVE-2025-8424 | セキュリティ情報 |
| Aug 26, 2025 | CVE-2025-7776 | セキュリティ情報 |
| Aug 26, 2025 | CVE-2025-7775 | セキュリティ情報 |
| Jun 25, 2025 | CVE-2025-6543 | セキュリティ情報 |
| Jun 17, 2025 | CVE-2025-5349 | セキュリティ情報 |
| Jun 17, 2025 | CVE-2025-5777 | セキュリティ情報 |
| Nov 12, 2024 | CVE-2024-8535 | セキュリティ情報 |
| Jul 09, 2024 | CVE-2024-5491 | セキュリティ情報 |
| Jul 09, 2024 | CVE-2024-5492 | セキュリティ情報 |
| Jan 16, 2024 | CVE-2023-6549 | セキュリティ速報 |
| Jan 16, 2024 | CVE-2023-6548 | セキュリティ速報 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| リリース日 | CVE ID | リソースリンク |
|---|---|---|
| Oct 10, 2023 | CVE-2023-4967 | セキュリティ速報 |
| Oct 10, 2023 | CVE-2023-4966 | セキュリティ速報 |
| Jul 18, 2023 | CVE-2023-3519 | セキュリティ速報 |
| Jul 18, 2023 | CVE-2023-3467 | セキュリティ速報 |
| Jul 18, 2023 | CVE-2023-3466 | セキュリティ速報 |
| May 09, 2023 | CVE-2023-24488 | セキュリティ速報 |
| May 09, 2023 | CVE-2023-24487 | セキュリティ速報 |
| Dec 13, 2022 | CVE-2022-27518 | セキュリティ速報 |
| Nov 08, 2022 | CVE-2022-27516 | セキュリティ速報 |
| Nov 08, 2022 | CVE-2022-27513 | セキュリティ速報 |
| Nov 08, 2022 | CVE-2022-27510 | セキュリティ速報 |
| Jul 26, 2022 | CVE-2022-27509 | セキュリティ速報 |
| May 25, 2022 | CVE-2022-27508 | セキュリティ速報 |
| May 25, 2022 | CVE-2022-27507 | セキュリティ速報 |
| Nov 09, 2021 | CVE-2021-22956 | セキュリティ速報 |
| Nov 09, 2021 | CVE-2021-22955 | セキュリティ速報 |
| Jul 19, 2021 | CVE-2021-22927 | セキュリティ速報 |
| Jul 19, 2021 | CVE-2021-22920 | セキュリティ速報 |
| Jul 19, 2021 | CVE-2021-22919 | セキュリティ速報 |
| Jun 08, 2021 | CVE-2020-8300 | セキュリティ速報 |
| Jun 08, 2021 | CVE-2020-8299 | セキュリティ速報 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| リリース日 | CVE ID | リソースリンク |
|---|---|---|
| Sep 17, 2020 | CVE-2020-8247 | セキュリティ速報 |
| Sep 17, 2020 | CVE-2020-8246 | セキュリティ速報 |
| Sep 17, 2020 | CVE-2020-8245 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8197 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8199 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8195 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8196 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8193 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8187 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8191 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8190 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2019-18177 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8194 | セキュリティ速報 |
| Jul 07, 2020 | CVE-2020-8198 | セキュリティ速報 |
| Dec 17, 2019 | CVE-2019-19781 | セキュリティ速報 |

## CVE-2026-88771の脆弱性を特定して修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88771を検索します。CVE-2026-88771の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88771の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-88771を修正する

CVE-2026-88771の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

## CVE-2026-88772の脆弱性を特定して修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88772を検索します。CVE-2026-88772の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88772の影響が反映されるまで、数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-88772を修正する

CVE-2026-88772の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定された状態で表示されます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブを作成するを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

## CVE-2026-88773の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、「**CVE検出**」をクリックします。「**影響を受けるインスタンス**」タブで、CVE-2026-88773を検索します。CVE-2026-88773の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88773の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**今すぐスキャン**」をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-88773を修正する

CVE-2026-88773の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、「**CVE検出 > 影響を受けるインスタンス**」の下で、インスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、「CVE検出」を参照してください。

## CVE-2026-88774の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88774を検索します。CVE-2026-88774の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88774の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CVE-2026-88774を修正する

CVE-2026-88774の影響を受けるNetScalerインスタンスの場合、修正は1ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態でアップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

## CVE-2026-88775 の脆弱性を特定し、修正する

NetScaler Console® のセキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2026-88775 を検索します。CVE-2026-88775 の影響を受ける NetScaler インスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2026-88775 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-88775 を修正する

CVE-2026-88775 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUI で、**CVE Detection > Impacted Instances** の下でインスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade job を参照してください。

このステップは、すべての脆弱な NetScaler インスタンスに対して一度に実行できます。詳細については、CVE Detection を参照してください。

## CVE-2026-88776の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88776を検索します。CVE-2026-88776の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88776の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-88776を修正する

CVE-2026-88776の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## CVE-2026-88777の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88777を検索します。CVE-2026-88777の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88777の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-88777を修正する

CVE-2026-88777の影響を受けるNetScalerインスタンスの場合、修正は1ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

## CVE-2026-88778 の脆弱性を修正する

NetScaler Console のセキュリティアドバイザリダッシュボードの **現在の CVE** `<number of>` **NetScaler インスタンスが CVE の影響を受けています** の下で、CVE-2026-88778 により脆弱なすべてのインスタンスを確認できます。CVE の影響を受けるインスタンスの詳細を確認するには、CVE-2026-88778 を選択し、**影響を受けるインスタンスを表示** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CVE-2026-88778 を修正する

CVE-2026-88778 の影響を受ける NetScaler インスタンスの場合、修正は 2 段階のプロセスです。GUI の **現在の CVE > NetScaler インスタンスが CVE の影響を受けています** の下で、ステップ 1 と 2 を確認できます。

2 つのステップは次のとおりです。

1. 脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする。
2. 設定ジョブでカスタマイズ可能な組み込み設定テンプレートを使用して、必要な設定コマンドを適用する。

**現在の CVE > NetScaler インスタンスが CVE の影響を受けています** の下には、この 2 段階の修正プロセスに対して、**アップグレードワークフローに進む** と **設定ジョブワークフローに進む** という 2 つの異なるワークフローが表示されます。

#### ステップ 1: 影響を受ける NetScaler インスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

#### ステップ 2: 設定コマンドを適用する

影響を受けるインスタンスをアップグレードした後、`<number of` **> NetScaler インスタンスが CVE の影響を受けています** ウィンドウで、CVE-2026-88778 の影響を受けるインスタンスを選択し、**設定ジョブワークフローに進む** をクリックします。ワークフローには次のステップが含まれます。

1. 設定のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が設定された最終設定の確認。
5. ジョブの実行。

インスタンスを選択して をクリックする前に、次の点に留意してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CVE-2026-88778 のみに影響を受ける複数の NetScaler インスタンスの場合: すべてのインスタンスで一度に構成ジョブを実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3 があり、それらすべてが CVE-2026-88778 のみに影響を受けているとします。これらのインスタンスをすべて選択し、 をクリックすると、組み込みの構成テンプレートが の下に自動入力されます。

ステップ 1: 構成の選択

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが の下に自動入力されます。

構成の選択(/en-us/netscaler-application-delivery-management-software/media/sep-cve-config-job.png)

**ステップ 2: インスタンスの選択**

影響を受けるインスタンスは の下に自動入力されます。インスタンスを選択します。 をクリックします。次のステップで構成をプレビューします。 をクリックします。

> **注:**
>
> クラスターモードの NetScaler インスタンスの場合、セキュリティアドバイザリを使用して、NetScaler Console はクラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートします。CCO 以外のノードでは、コマンドを個別に実行してください。

ステップ 3: 構成の実行

設定ジョブを実行するには、**完了**をクリックします。

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、修正されたセキュリティ体制を確認できます。

## CVE-2026-19490の脆弱性を特定して修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-19490を検索します。CVE-2026-19490の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-19490のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-19490.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-19490の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-19490を修正する

CVE-2026-19490の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定された状態で表示されます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

## CVE-2026-19489の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-19489を検索します。CVE-2026-19489の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-19489のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-19489.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-19489の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CVE-2026-19489を修正する

CVE-2026-19489の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下で、インスタンスを選択し、**Proceed to upgrade workflow**をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態でアップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

## CVE-2026-13474の脆弱性を修正する

NetScaler Consoleセキュリティアドバイザリダッシュボードの「**現在のCVE > `<number of>` NetScalerインスタンスは共通脆弱性識別子 (CVE) の影響を受けています**」の下で、この特定のCVEによって脆弱なすべてのインスタンスを確認できます。CVE-2026-13474の影響を受けるインスタンスの詳細を確認するには、「**CVE-2026-13474**」を選択し、「**影響を受けるインスタンスを表示**」をクリックします。

「`<number of>` **CVEの影響を受けるNetScalerインスタンス**」ウィンドウが表示されます。ここには、CVE-2026-13474の影響を受けるNetScalerインスタンスの数と詳細が表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

### CVE-2026-13474を修正する

CVE-2026-13474の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの「**現在のCVE > CVEの影響を受けるNetScalerインスタンス**」の下で、ステップ1と2を確認できます。

2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードする。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。

「**現在のCVE > CVEの影響を受けるNetScalerインスタンス**」の下には、この2段階の修正プロセスに対して2つの異なるワークフローが表示されます。それらは「**アップグレードワークフローに進む**」と「**構成ジョブワークフローに進む**」です。

**ステップ1：影響を受けるNetScalerインスタンスをアップグレードする**

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「NetScaler アップグレードジョブの作成」を参照してください。

**ステップ2：構成コマンドを適用する**

影響を受けるインスタンスをアップグレードした後、`<number of>` **CVE の影響を受ける NetScaler インスタンス**ウィンドウで、CVE-2026-13474 の影響を受けるインスタンスを選択し、**構成ジョブワークフローに進む**をクリックします。ワークフローには次の手順が含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が入力された最終構成の確認。
5. ジョブの実行。

インスタンスを選択して**構成ジョブワークフローに進む**をクリックする前に、次の点に注意してください。

- CVE-2026-13474 のみに影響を受ける複数の NetScaler インスタンスの場合：すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3 があり、それらすべてが CVE-2026-13474 のみに影響を受けているとします。これらのインスタンスをすべて選択し、**構成ジョブワークフローに進む**をクリックすると、組み込みの構成テンプレートが**構成の選択**の下に自動入力されます。

#### ステップ1：構成の選択

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが**構成の選択**の下に自動入力されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステップ2：インスタンスの選択

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択し、**次へ**をクリックします。次のステップで、構成をプレビューし、**次へ**をクリックします。

**注:**

セキュリティアドバイザリを使用するクラスターモードのNetScalerインスタンスの場合、NetScaler Consoleは、クラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートしています。CCO以外のノードでは、コマンドを個別に実行してください。

CVE-2026-13474の修復手順(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-2.png)

ステップ3：構成を実行する

**完了**をクリックして、構成ジョブを実行します。

CVE-2026-13474の修復手順(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-3.png)

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

## CVE-2026-10817の脆弱性を特定して修復する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-10817を検索します。CVE-2026-10817の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記：**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-10817の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始してください。

### CVE-2026-10817を修復する

CVE-2026-10817の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、「CVE Detection」を参照してください。

## CVE-2026-10816の脆弱性を特定し、修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-10816を検索します。CVE-2026-10816の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-10816のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-10816.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-10816の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CVE-2026-10816を修正する

CVE-2026-10816の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

## CVE-2026-8655 の脆弱性を特定して修復する

NetScaler Console® セキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2026-8655 を検索します。CVE-2026-8655 の影響を受ける NetScaler インスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

**注記：**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2026-8655 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-8655 を修復する

CVE-2026-8655 の影響を受ける NetScaler インスタンスの場合、修復は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUI の **CVE Detection > Impacted Instances** で、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

このステップは、すべての脆弱な NetScaler インスタンスに対して一度に実行できます。詳細については、「CVE Detection」を参照してください。

## CVE-2026-8452 の脆弱性を特定し、修正する

NetScaler Console® セキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2026-8452 を検索します。CVE-2026-8452 の影響を受ける NetScaler インスタンスのリストが表示されます。

CVE-2026-8452 のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-8452.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2026-8452 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-8452 を修正する

CVE-2026-8452 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUI で、**CVE Detection > Impacted Instances** の下で、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade job を参照してください。

このステップは、すべての脆弱な NetScaler インスタンスに対して一度に実行できます。詳細については、CVE Detection を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## CVE-2026-8451の脆弱性を特定して修正する

NetScaler Console® セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-8451を検索します。CVE-2026-8451の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注：**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-8451の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-8451を修正する

CVE-2026-8451の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態でアップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

## CVE-2026-4368 の脆弱性を特定し、修正する

NetScaler Console® のセキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2026-4368 を検索します。CVE-2026-4368 の影響を受ける NetScaler インスタンスのリストが表示されます。

CVE-2026-4368 のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-4368.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2026-4368 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-4368 を修正する

CVE-2026-4368 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUI で、**CVE Detection > Impacted Instances** の下でインスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

**重要**

脆弱な NetScaler インスタンスに /etc/httpd.conf ファイルが /nsconfig ディレクトリにコピーされている場合は、NetScaler のアップグレードを計画する前に、「Upgrade considerations for customized NetScaler configurations」を参照してください。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

修正ワークフロー(/en-us/netscaler-application-delivery-management-software/media/remediation-workflow-cve-2026-4368.png)

## CVE-2026-3055 の脆弱性を特定して修正する

NetScaler Console® セキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2026-3055 を検索します。CVE-2026-3055 の影響を受ける NetScaler インスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2026-3055 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

### CVE-2026-3055 を修正する

CVE-2026-3055 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUI で、**CVE Detection > Impacted Instances** の下でインスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

**重要**

脆弱な NetScaler インスタンスに /etc/httpd.conf ファイルが /nsconfig ディレクトリにコピーされている場合は、NetScaler のアップグレードを計画する前に、「カスタマイズされた NetScaler 構成のアップグレードに関する考慮事項」を参照してください。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「NetScaler アップグレードジョブの作成」を参照してください。

## CVE-2025-12101 の脆弱性を特定し、修復する

NetScaler Console® のセキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2025-12101 を検索します。CVE-2025-12101 の影響を受ける NetScaler インスタンスのリストが表示されます。

CVE-2025-12101 のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2025-12101.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2025-12101 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

### CVE-2025-12101 を修復する

CVE-2025-12101 の影響を受ける NetScaler インスタンスの場合、修復は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUI で、**CVE Detection > Impacted Instances** の下でインスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

**重要**

脆弱な NetScaler インスタンスに /etc/httpd.conf ファイルが /nsconfig ディレクトリにコピーされている場合は、NetScaler のアップグレードを計画する前に、カスタマイズされた NetScaler 構成のアップグレードに関する考慮事項 を参照してください。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、NetScaler アップグレードジョブの作成 を参照してください。

修復ワークフロー(/en-us/netscaler-application-delivery-management-software/media/remediation-workflow-cve-2025-12101.png)

## CVE-2025-8424 の脆弱性を特定して修正する

NetScaler Console のセキュリティアドバイザリダッシュボードの **Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs** の下で、CVE-2025-8424 によって脆弱になっているすべてのインスタンスを確認できます。CVE の影響を受けるインスタンスの詳細を確認するには、CVE-2025-8424 を選択し、**View Affected Instances** をクリックします。

CVE-2025-8424 のセキュリティアドバイザリダッシュボードのスクリーンショット(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2025-8424.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記:**

NetScaler の脆弱性の理由を理解するには、セキュリティアドバイザリの **Scan logs** タブで CSV レポートをダウンロードしてください。

`<number of>` **NetScaler instances impacted by CVEs** ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2025-8424 の影響を受ける NetScaler インスタンスの数と詳細を確認できます。

CVE-2025-8424 の影響を受けるインスタンスのスクリーンショット(/en-us/netscaler-application-delivery-management-software/media/cve-2025-8424-impacted-instance.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

**注記:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2025-8424 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始してください。

### CVE-2025-8424 を修正する

CVE-2025-8424 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUI の **Current CVEs > NetScaler instances are impacted by CVEs** の下で、修正手順を確認できます。

**Current CVEs > NetScaler instances impacted by CVEs** の下には、この単一ステップの修正プロセスとして、**Proceed to upgrade workflow** が表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要**

脆弱性のあるNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、「カスタマイズされたNetScaler構成のアップグレードに関する考慮事項」(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html#upgrade-considerations-for-customized-adc-configurations)を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html)を参照してください。

## CVE-2025-7776 の脆弱性を特定し、修正する

NetScaler Console のセキュリティアドバイザリダッシュボードの「**Current CVEs `<number of>` NetScaler instances are impacted by CVEs**」で、CVE-2025-7776 によって脆弱になっているすべてのインスタンスを確認できます。CVE の影響を受けるインスタンスの詳細を確認するには、CVE-2025-7776 を選択し、「**View Affected Instances**」をクリックします。

**注：**

NetScaler の脆弱性の理由を理解するには、セキュリティアドバイザリの「**Scan logs**」タブで CSV レポートをダウンロードしてください。

「`<number of>` **NetScaler instances impacted by CVEs**」ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2025-7776 の影響を受ける NetScaler インスタンスの数と詳細を確認できます。

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注：**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2025-7776 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**Scan-Now**」をクリックしてオンデマンドスキャンを開始してください。

### CVE-2025-7776 を修正する

CVE-2025-7776 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUI の「**Current CVEs > NetScaler instances are impacted by CVEs**」で、修正手順を確認できます。

「**Current CVEs > NetScaler instances impacted by CVEs**」の下に、この単一ステップの修正プロセスとして「**Proceed to upgrade workflow**」というワークフローが表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、「**Proceed to upgrade workflow**」をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

**重要**

脆弱なNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

## CVE-2025-7775の脆弱性を特定し、修復する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、「**現在のCVE** `<number of>` **CVEの影響を受けるNetScalerインスタンス**」の下に、CVE-2025-7775によって脆弱なすべてのインスタンスが表示されます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2025-7775を選択し、「**影響を受けるインスタンスを表示**」をクリックします。

「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

」.

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリの「**スキャンログ**」タブでCSVレポートをダウンロードしてください。

「`<number of>` **CVEの影響を受けるNetScalerインスタンス**」ウィンドウが表示されます。次のスクリーンショットでは、CVE-2025-7775の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

「

**注:**

」.

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-7775の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**今すぐスキャン**」をクリックしてオンデマンドスキャンを開始してください。

### CVE-2025-7775を修復する

CVE-2025-7775の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUIの「**現在のCVE > CVEの影響を受けるNetScalerインスタンス**」の下に、修復手順が表示されます。

「**現在のCVE > CVEの影響を受けるNetScalerインスタンス**」の下に、この単一ステップの修復プロセスである「**アップグレードワークフローに進む**」という次のワークフローが表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要**

」

脆弱性のあるNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

## CVE-2025-6543の脆弱性を特定し、修復する

NetScaler Consoleセキュリティアドバイザリダッシュボードの**現在のCVE** `<number of>` **CVEの影響を受けるNetScalerインスタンス**で、CVE-2025-6543によって脆弱なすべてのインスタンスを確認できます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2025-6543を選択し、**影響を受けるインスタンスを表示**をクリックします。

CVE-2025-6543のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2025-6543.png)

**注:**

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリの**スキャンログ**タブでCSVレポートをダウンロードしてください。

`<number of>` **CVEの影響を受けるNetScalerインスタンス**ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2025-6543の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

CVE-2025-6543の影響を受けるインスタンス(/en-us/netscaler-application-delivery-management-software/media/cve-2025-6543-impacted-instance.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-6543の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始してください。

### CVE-2025-6543を修復する

CVE-2025-6543の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUIの**現在のCVE > CVEの影響を受けるNetScalerインスタンス**で、修復手順を確認できます。

**現在のCVE > CVEの影響を受けるNetScalerインスタンス**の下に、この単一ステップの修復プロセスである**アップグレードワークフローに進む**というワークフローが表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

**重要**

脆弱なNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

## CVE-2025-5349の脆弱性を特定し、修復する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**現在のCVE** `<number of>` **CVEの影響を受けるNetScalerインスタンス**の下に、CVE-2025-5349によって脆弱なすべてのインスタンスが表示されます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2025-5349を選択し、**影響を受けるインスタンスを表示**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリの**スキャンログ**タブでCSVレポートをダウンロードしてください。

`<number of>` **CVEの影響を受けるNetScalerインスタンス**ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2025-5349の影響を受けるNetScalerインスタンスの数と詳細を確認できます。



セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-5349の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始してください。

### CVE-2025-5349を修復する

CVE-2025-5349の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUIの**現在のCVE > CVEの影響を受けるNetScalerインスタンス**の下に、修復手順が表示されます。

**現在のCVE > CVEの影響を受けるNetScalerインスタンス**の下に、この単一ステップの修復プロセスである**アップグレードワークフローに進む**というワークフローが表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

**重要**

脆弱なNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

## CVE-2025-5777の脆弱性を修復する

NetScaler Consoleのセキュリティアドバイザリダッシュボードの**Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**の下で、CVE-2025-5777によって脆弱なすべてのインスタンスを確認できます。CVEによって影響を受けるインスタンスの詳細を確認するには、CVE-2025-5777を選択し、**View Affected Instances**をクリックします。

**注:**

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリの**Scan logs**タブでCSVレポートをダウンロードします。

`<number of>` **NetScaler instances impacted by CVEs**ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2025-5777によって影響を受けるNetScalerインスタンスの数と詳細を確認できます。

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

**注:**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-5777の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

### CVE-2025-5777を修復する

CVE-2025-5777の影響を受けるNetScalerインスタンスの場合、修復は2段階のプロセスです。GUIの**Current CVEs > NetScaler instances are impacted by CVEs**の下で、ステップ1と2を確認できます。

2つのステップは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 脆弱なNetScalerインスタンスを、修正を含むリリースとビルドにアップグレードします。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用します。

**現在のCVE > CVEの影響を受けるNetScalerインスタンス**の下に、この2段階の修復プロセスに対応する2つの別々のワークフローが表示されます。これらは、**アップグレードワークフローに進む**と**構成ジョブワークフローに進む**です。

**ステップ1：脆弱なNetScalerインスタンスをアップグレードする**

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

**注：**

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

**ステップ2：構成コマンドを適用する**

影響を受けるインスタンスをアップグレードした後、`<number of>` **CVEの影響を受けるNetScalerインスタンス**ウィンドウで、CVE-2025-5777の影響を受けるインスタンスを選択し、**構成ジョブワークフローに進む**をクリックします。ワークフローには次の手順が含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの実行。

インスタンスを選択して**構成ジョブワークフローに進む**をクリックする前に、次の点に注意してください。

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956、CVE-2025-5777など）の影響を受けるNetScalerインスタンスの場合：インスタンスを選択して**構成ジョブワークフローに進む**をクリックしても、**構成の選択**の下に組み込み構成テンプレートが自動入力されません。**セキュリティアドバイザリテンプレート**の下にある適切な構成ジョブテンプレートを、右側の構成ジョブペインに手動でドラッグアンドドロップする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CVE-2025-5777のみの影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2025-5777のみの影響を受けているとします。これらのインスタンスをすべて選択し、**構成ジョブワークフローに進む**をクリックすると、**構成の選択**の下に組み込み構成テンプレートが自動入力されます。
- CVE-2025-5777およびその他の1つ以上のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスに対して、一度に1つのNetScalerに修正を適用する必要がある場合：これらのインスタンスを選択して**Proceed to configuration job workflow**をクリックすると、一度に1つのNetScalerで構成ジョブを実行するように指示するエラーメッセージが表示されます。

#### ステップ1：構成を選択する

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが**Select configuration**の下に自動入力されます。

構成を選択(/en-us/netscaler-application-delivery-management-software/media/select-config-step-cve-2025-5777.png)

#### ステップ2：インスタンスを選択する

影響を受けるインスタンスは**Select Instances**の下に自動入力されます。インスタンスを選択します。このインスタンスがHAペアの一部である場合は、**Execute on Secondary Nodes**を選択します。**Next**をクリックします。

インスタンスを選択(/en-us/netscaler-application-delivery-management-software/media/select-instance-cve-2025-5777.png)

**注：**

クラスターモードのNetScalerインスタンスの場合、セキュリティアドバイザリを使用すると、NetScaler Consoleはクラスター構成コーディネーター（CCO）ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

#### ステップ3：ジョブを実行する

**Finish**をクリックして構成ジョブを実行します。

構成ジョブを実行(/en-us/netscaler-application-delivery-management-software/media/run-job-cve-2021-22956.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ジョブが実行されると、**Infrastructure > Configuration > Configuration Jobs**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修正ステップを完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

## CVE-2024-8535の脆弱性を修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**現在のCVE > `<number of>`** NetScalerインスタンスが共通脆弱性識別子 (CVE) の影響を受けている場合、この特定のCVEによって脆弱なすべてのインスタンスを確認できます。CVE-2024-8535の影響を受けるインスタンスの詳細を確認するには、CVE-2024-8535を選択し、**影響を受けるインスタンスを表示**をクリックします。

CVE-2024-8535のセキュリティアドバイザリダッシュボード(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2024-8435.png)

`<number of>` CVEの影響を受けるNetScalerインスタンスウィンドウが表示されます。ここでは、CVE-2024-8535の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

CVE-2020-8300の影響を受けるインスタンス(/en-us/netscaler-application-delivery-management-software/media/cve-2024-8535-impacted-instance.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2024-8535の影響が反映されるまでに時間がかかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

### CVE-2024-8535を修正する

CVE-2024-8535の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの**現在のCVE > CVEの影響を受けるNetScalerインスタンス**で、ステップ1と2を確認できます。

CVE-2024-8535の修正手順(/en-us/netscaler-application-delivery-management-software/media/remediate-steps-CVE-2024-8535.png)

2つの手順は次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 脆弱なNetScalerインスタンスを、修正を含むリリースとビルドにアップグレードします。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用します。

**現在のCVE > CVEの影響を受けるNetScalerインスタンス**で、この2段階の修正プロセスには2つの異なるワークフローが表示されます。それらは**アップグレードワークフローに進む**と**構成ジョブワークフローに進む**です。



**ステップ 1: 脆弱なNetScalerインスタンスをアップグレードする**

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態で、アップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

**注:**

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

**ステップ 2: 構成コマンドを適用する**

影響を受けるインスタンスをアップグレードした後、`<number of` **> CVEの影響を受けるNetScalerインスタンス**ウィンドウで、CVE-2024-8535の影響を受けるインスタンスを選択し、**構成ジョブワークフローに進む**をクリックします。

インスタンスを選択して**構成ジョブワークフローに進む**をクリックする前に、以下の点に留意してください。

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956など）の影響を受けるNetScalerインスタンスの場合: インスタンスを選択して**構成ジョブワークフローに進む**をクリックしても、**構成の選択**の下に組み込みの構成テンプレートが自動入力されません。**セキュリティアドバイザリテンプレート**の下にある適切な構成ジョブテンプレートを、手動で右側の構成ジョブペインにドラッグアンドドロップしてください。
- CVE-2024-8535のみの影響を受ける複数のNetScalerインスタンスの場合、すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2024-8535のみの影響を受けているとします。これらすべてのイ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンスタンスを選択して**構成ジョブワークフローに進む**をクリックすると、**構成の選択**の下に組み込みの構成テンプレートが自動入力されます。

- CVE-2024-8535および1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスで、各NetScalerに一度に1つずつ修復を適用する必要がある場合: これらのインスタンスを選択して**構成ジョブワークフローに進む**をクリックすると、各NetScalerで構成ジョブを一度に1つずつ実行するように促すエラーメッセージが表示されます。

#### ステップ 1: 構成を選択する

構成ジョブワークフローでは、**構成の選択**の下に組み込みの構成ベーステンプレートが自動入力されます。



#### ステップ2：インスタンスを選択する

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択します。このインスタンスがHAペアの一部である場合は、**セカンダリノードで実行**を選択します。**次へ**をクリックします。



**注：**

クラスターモードのNetScalerインスタンスの場合、セキュリティアドバイザリを使用して、NetScaler Consoleはクラスター構成コーディネーター（CCO）ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

#### ステップ3：変数値を指定する

このステップでは、変数を指定する必要はありません。**すべてのインスタンスの共通変数値**を選択し、**次へ**をクリックします。

#### ステップ4：構成をプレビューする

構成に挿入された変数値をプレビューし、**次へ**をクリックします。



#### ステップ5：ジョブを実行する

構成ジョブを実行するには、**完了**をクリックします。



ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

## CVE-2020-8300の脆弱性に対処する

NetScaler Consoleのセキュリティアドバイザリダッシュボードの**Current CVEs > `<number of>` NetScaler instances are impacted by CVEs**の下で、この特定のCVEによって脆弱なすべてのインスタンスを確認できます。CVE-2020-8300の影響を受けるインスタンスの詳細を確認するには、**CVE-2020-8300**を選択し、**View Affected Instances**をクリックします。



**注**

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

**`<number of>` NetScaler instances impacted by CVEs**ウィンドウが表示されます。ここでは、CVE-2020-8300の影響を受けるNetScalerインスタンスの数と詳細が表示されます。



### CVE-2020-8300に対処する

CVE-2020-8300の影響を受けるNetScalerインスタンスの場合、対処は2段階のプロセスです。GUIの**Current CVEs > NetScaler instances are impacted by CVEs**の下で、ステップ1と2を確認できます。



2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。このステップは、脆弱なNetScalerごとに1つずつ実行し、そのNetScalerのすべてのSAMLアクションとSAMLプロファイルを含めます。

**Current CVEs> NetScaler instances impacted by CVEs**の下で、この2段階の対処プロセスには、**Proceed to upgrade workflow**と**Proceed to configuration job workflow**という2つの異なるワークフローが表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、 をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「NetScaler アップグレードジョブの作成」を参照してください。

**注**

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

### ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、**`<number of>` CVE の影響を受ける NetScaler インスタンス** ウィンドウで、CVE-2020-8300 の影響を受けるインスタンスを 1 つ選択し、 をクリックします。ワークフローには、次の手順が含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が設定された最終構成の確認。
5. ジョブの実行。

インスタンスを選択して をクリックする前に、次の点に注意してください。

- 複数の CVE (CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 など) の影響を受ける NetScaler インスタンスの場合：インスタンスを選択して をクリックしても、組み込みの構成テンプレートは の下に自動入力されません。適切な構成ジョブテンプレートをの下から右側の構成ジョブペインに手動でドラッグアンドドロップしてください。
- CVE-2021-22956のみの影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで一度に構成ジョブを実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2021-22956のみの影響を受けているとします。これらのインスタンスをすべて選択し、**Proceed to configuration job workflow**をクリックすると、**Select configuration**の下に組み込みの構成テンプレートが自動入力されます。
- CVE-2021-22956と1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスの場合、各NetScalerに一度に修復を適用する必要があります。これらのインスタンスを選択して**Proceed to**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**configuration job workflow**をクリックすると、各NetScalerで一度に構成ジョブを実行するように指示するエラーメッセージが表示されます。

#### ステップ1：構成の選択

構成ジョブワークフローでは、**Select configuration**の下に組み込みの構成テンプレートが自動入力されます。

構成の選択(/en-us/netscaler-application-delivery-management-software/media/select-config-step.png)

影響を受けるNetScalerインスタンスごとに、一度に1つずつ個別の構成ジョブを実行し、そのNetScalerのすべてのSAMLアクションとSAMLプロファイルを含めます。たとえば、それぞれ2つのSAMLアクションと2つのSAMLプロファイルを持つ脆弱なNetScalerインスタンスが2つある場合、この構成ジョブを2回実行する必要があります。各NetScalerにつき1回、そのすべてのSAMLアクションとSAMLプロファイルをカバーするように実行します。

| NETSCALER 1 | NETSCALER 2 |
| --- | --- |
| ジョブ1：2つのSAMLアクション +2つのSAMLプロファイル | ジョブ2：2つのSAMLアクション +2つのSAMLプロファイル |

ジョブに名前を付け、以下の仕様に合わせてテンプレートをカスタマイズします。組み込みの構成テンプレートは、単なる概要または基本テンプレートです。以下の要件に合わせて、デプロイメントに基づいてテンプレートをカスタマイズしてください。

a. **SAMLアクションとその関連ドメイン**

デプロイメント内のSAMLアクションの数に応じて、1～3行目を複製し、各SAMLアクションのドメインをカスタマイズする必要があります。

SAMLアクションのカスタマイズ(/en-us/netscaler-application-delivery-management-software/media/saml-action.png)

たとえば、2つのSAMLアクションがある場合、1～3行目を2回繰り返し、それに応じて各SAMLアクションの変数定義をカスタマイズします。

また、SAMLアクションにN個のドメインがある場合、そのSAMLアクションに対して行がN回表示されるように、`bind patset $saml_action_patset$ “$saml_action_domain1$”`の行を手動で複数回入力する必要があります。そして、以下の変数定義名を変更します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `saml_action_patset`: は設定テンプレート変数であり、SAMLアクションのパターンセット (patset) の名前の値を表します。設定ジョブワークフローのステップ3で実際の値を指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。
- `saml_action_domain1`: は設定テンプレート変数であり、特定のSAMLアクションのドメイン名を表します。設定ジョブワークフローのステップ3で実際の値を指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。

デバイスのすべてのSAMLアクションを見つけるには、コマンド `show samlaction` を実行します。

b. **SAMLプロファイルとそれに関連付けられたURL**

展開内のSAMLプロファイルの数に応じて、4〜6行目を複製します。各SAMLプロファイルのURLをカスタマイズします。

たとえば、SAMLプロファイルが2つある場合、4〜6行目を2回手動で入力し、それに応じて各SAMLアクションの変数定義をカスタマイズします。

また、SAMLアクションにN個のドメインがある場合、そのSAMLプロファイルに対して行がN回表示されるように、`bind patset $saml_profile_patset$ “$saml_profile_url1$”`の行を手動で複数回入力する必要があります。そして、以下の変数定義名を変更します。

- `saml_profile_patset`: は設定テンプレート変数であり、SAMLプロファイルのパターンセット (patset) の名前の値を表します。設定ジョブワークフローのステップ3で実際の値を指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。
- `saml_profile_url1`: は設定テンプレート変数であり、特定のSAMLプロファイルのドメイン名を表します。設定ジョブワークフローのステップ3で実際の値を指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。

デバイスのすべてのSAMLプロファイルを見つけるには、コマンド `show samlidpProfile` を実行します。

**ステップ2: インスタンスを選択する**

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択し、**次へ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスの選択(/en-us/netscaler-application-delivery-management-software/media/select-instance.png)

#### ステップ 3: 変数値を指定する

変数値を入力します。

- `saml_action_patset`: SAMLアクションの名前を追加します
- `saml_action_domain1`: `https://<example1.com>/`の形式でドメインを入力します
- `saml_action_name`: ジョブを構成しているSAMLアクションの同じものを入力します
- `saml_profile_patset`: SAMLプロファイルの名前を追加します
- `saml_profile_url1`: URLをこの形式で入力します `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: ジョブを構成しているSAMLプロファイルの同じものを入力します

**注**

URLの場合、拡張子は常に`cgi/samlauth`ではありません。使用しているサードパーティ認証によって異なり、それに応じて拡張子を設定する必要があります。

変数を指定(/en-us/netscaler-application-delivery-management-software/media/specify-variables.png)

#### ステップ 4: 構成をプレビューする

設定に挿入された変数値をプレビューし、**次へ**をクリックします。

#### ステップ 5: ジョブを実行する

**完了**をクリックして、構成ジョブを実行します。

構成ジョブを実行(/en-us/netscaler-application-delivery-management-software/media/run-job.png)

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

### NetScaler Console Expressアカウントに関する注意点

NetScaler Console Expressアカウントには機能制限があり、構成ジョブは2つまでという制限が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2020-8300の修復には、脆弱なNetScalerインスタンスの数と同じ数の構成ジョブを実行する必要があります。したがって、Expressアカウントをお持ちで、2つを超える構成ジョブを実行する必要がある場合は、この回避策に従ってください。

**回避策**: 2つの脆弱なNetScalerインスタンスに対して2つの構成ジョブを実行し、その後、両方のジョブを削除して、次の2つの脆弱なNetScalerインスタンスに対して次の2つのジョブを実行し続けます。すべての脆弱なインスタンスをカバーするまでこれを続けます。ジョブを削除する前に、今後の参照のためにレポートをダウンロードできます。レポートをダウンロードするには、**ネットワーク > ジョブ**でジョブを選択し、**アクション**の下にある**ダウンロード**をクリックします。

**例**: 6つの脆弱なNetScalerインスタンスがある場合、それぞれ2つの脆弱なインスタンスで2つの構成ジョブを実行し、その後、両方の構成ジョブを削除します。この手順をさらに2回繰り返します。最終的に、それぞれ6つのNetScalerインスタンスに対して6つの構成ジョブを実行したことになります。NetScaler Console UIの**インフラストラクチャ > ジョブ**では、最後の2つの構成ジョブのみが表示されます。

### シナリオ

このシナリオでは、3つのNetScalerインスタンスがCVE-2020-8300に対して脆弱であり、すべてのインスタンスを修復する必要があります。次の手順に従ってください:

1. このドキュメントの「**インスタンスのアップグレード**」セクションに記載されている手順に従って、3つのNetScalerインスタンスすべてをアップグレードします。
2. 構成ジョブワークフローを使用して、一度に1つのNetScalerに構成パッチを適用します。このドキュメントの「**構成コマンドの適用**」セクションに記載されている手順を参照してください。

脆弱なNetScaler 1には次の構成があります:

| 2つのSAMLアクション | 2つのSAMLプロファイル |
| --- | --- |
| | |

NetScaler 1を選択し、**構成ジョブワークフローに進む**をクリックします。組み込みテンプレートが自動入力されます。次に、ジョブ名を入力し、指定された構成に従ってテンプレートをカスタマイズします。

次の表に、カスタマイズされたパラメータの変数定義を一覧表示します。

表1. SAMLアクションの変数定義

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| NETSCALER構成 | PATSETの変数定義 | SAMLアクション名の変数定義 | ドメインの変数定義 |
|---|---|---|---|
| SAMLアクション1には1つのドメインがあります | saml_action_patset1 | saml_action_name1 | saml_action_domain1 |
| SAMLアクション2には2つのドメインがあります | saml_action_patset2 | saml_action_name2 | saml_action_domain2, saml_action_domain3 |

表2. SAMLプロファイルの変数定義

| NETSCALER構成 | PATSETの変数定義 | SAMLプロファイル名の変数定義 | URLの変数定義 |
|---|---|---|---|
| SAMLプロファイル1には1つのURLがあります | saml_profile_patset1 | saml_profile_name1 | saml_profile_url1 |
| SAMLプロファイル2には2つのURLがあります | saml_profile_patset2 | saml_profile_name2 | saml_profile_url2, saml_profile_url3 |

「**インスタンスの選択**」でNetScaler 1を選択し、「**次へ**」をクリックします。「**変数値を指定**」ウィンドウが表示されます。このステップでは、前のステップで定義されたすべての変数に値を指定する必要があります。

次に、変数をレビューします。

「**次へ**」をクリックし、次に「**完了**」をクリックしてジョブを実行します。

ジョブが実行されると、「**インフラストラクチャ > 構成 > 構成ジョブ**」の下に表示されます。

NetScaler1の2つの修復手順を完了したら、NetScaler 2とNetScaler 3を修復するために同じ手順に従います。修復が完了したら、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# CVE-2021-22927およびCVE-2021-22920の脆弱性に対処する

NetScaler Consoleのセキュリティアドバイザリダッシュボードの**Current CVEs > `<number of>` NetScaler instances are impacted by CVEs**の下で、CVE-2021-22927およびCVE-2021-22920によって脆弱なすべてのインスタンスを確認できます。これら2つのCVEの影響を受けるインスタンスの詳細を確認するには、1つ以上のCVEを選択し、**View Affected Instances**をクリックします。



**注**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2021-22927およびCVE-2021-22920の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

`<number of>` **NetScaler instances impacted by CVEs**ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2021-22927およびCVE-2021-22920の影響を受けるNetScalerインスタンスの数と詳細を確認できます。



## CVE-2021-22927およびCVE-2021-22920に対処する

CVE-2021-22927およびCVE-2021-22920の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの**Current CVEs > NetScaler instances are impacted by CVEs**の下で、ステップ1と2を確認できます。



2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードします。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用します。このステップを脆弱なNetScalerごとに1つずつ実行し、そのNetScalerのすべてのSAMLアクションを含めます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

NetScalerインスタンスでCVE-2020-8300の構成ジョブをすでに実行している場合は、ステップ2をスキップしてください。

**Current CVEs> NetScaler instances impacted by CVEs**の下に、この2段階の修復プロセスに2つの別々のワークフローが表示されます。これらは、**Proceed to upgrade workflow**と**Proceed to configuration job workflow**です。

**ステップ1：脆弱なNetScalerインスタンスをアップグレードする**

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

**注**

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。 **注**

CVE-2021-22920およびCVE-2021-22927に対して脆弱なすべてのNetScalerインスタンスについてステップ1を完了したら、オンデマンドスキャンを実行します。**Current CVEs**の下の更新されたセキュリティ態勢は、NetScalerインスタンスがこれらのCVEのいずれかに対してまだ脆弱であるかどうかを理解するのに役立ちます。新しい態勢から、構成ジョブを実行する必要があるかどうかも確認できます。 CVE-2020-8300に対して適切な構成ジョブをNetScalerインスタンスにすでに適用しており、NetScalerインスタンスをアップグレードした場合は、オンデマンドスキャンを実行した後、インスタンスはCVE-2020-8300、CVE-2021-22920、およびCVE-2021-22927に対して脆弱であるとは表示されなくなります。

**ステップ2：構成コマンドを適用する**

影響を受けるインスタンスをアップグレードした後、`<number of` **> NetScaler instances impacted by CVEs**ウィンドウで、CVE-2021-22927およびCVE-2021-22920の影響を受けるインスタンスを1つ選択し、**Proceed to configuration job workflow**をクリックします。ワークフローには次のステップが含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が設定された最終設定を確認する。
5. ジョブを実行する。

インスタンスを選択し、**Proceed to configuration job workflow** をクリックする前に、以下の点に留意してください。

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956など）の影響を受けるNetScalerインスタンスの場合：インスタンスを選択して**Proceed to configuration job workflow**をクリックしても、組み込みの構成テンプレートは「Select configuration」の下に自動入力されません。適切な構成ジョブテンプレートを**Security Advisory Template**の下から手動で右側の構成ジョブペインにドラッグアンドドロップしてください。
- CVE-2021-22956のみの影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで一度に構成ジョブを実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2021-22956のみの影響を受けているとします。これらのインスタンスをすべて選択し、**Proceed to configuration job workflow**をクリックすると、組み込みの構成テンプレートが**Select configuration**の下に自動入力されます。
- CVE-2021-22956と1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスの場合、各NetScalerに一度に1つずつ修正を適用する必要があります。これらのインスタンスを選択して**Proceed to configuration job workflow**をクリックすると、各NetScalerで一度に1つずつ構成ジョブを実行するように指示するエラーメッセージが表示されます。

#### ステップ1：構成を選択する

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが**Select configuration**の下に自動入力されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

構成コマンドを適用するためにステップ2で選択されたNetScalerインスタンスが、CVE-2021-22927、CVE-2021-22920、およびCVE-2020-8300にも脆弱である場合、CVE-2020-8300のベーステンプレートが自動入力されます。CVE-2020-8300テンプレートは、これら3つのCVEすべてに必要な構成コマンドのスーパーセットです。このベーステンプレートをNetScalerインスタンスの展開と要件に合わせてカスタマイズしてください。

影響を受けるNetScalerインスタンスごとに、一度に1つずつ個別の構成ジョブを実行し、そのNetScalerのすべてのSAMLアクションを含める必要があります。たとえば、それぞれ2つのSAMLアクションを持つ脆弱なNetScalerインスタンスが2つある場合、この構成ジョブを2回実行する必要があります。各NetScalerにつき1回、そのすべてのSAMLアクションをカバーするように実行します。

| NETSCALER 1 | NETSCALER 2 |
| --- | --- |
| ジョブ1：2つのSAMLアクション | ジョブ2：2つのSAMLアクション |

ジョブに名前を付け、以下の仕様に合わせてテンプレートをカスタマイズします。組み込みの構成テンプレートは、単なる概要またはベーステンプレートです。以下の要件に基づいて、展開に合わせてテンプレートをカスタマイズしてください。

a. **SAMLアクションとその関連ドメイン**

展開にあるSAMLアクションの数に応じて、1〜3行目を複製し、各SAMLアクションのドメインをカスタマイズする必要があります。

たとえば、2つのSAMLアクションがある場合、1〜3行目を2回繰り返し、それに応じて各SAMLアクションの変数定義をカスタマイズします。

また、SAMLアクションにN個のドメインがある場合、そのSAMLアクションに対して行がN回表示されるように、`bind patset $saml_action_patset$ “$saml_action_domain1$”`の行を手動で複数回入力する必要があります。そして、以下の変数定義名を変更します。

- `saml_action_patset`: は構成テンプレート変数であり、SAMLアクションのパターンセット（patset）の名前の値を表します。実際の値は、構成ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3：変数値を指定する」セクションを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `saml_action_domain1`: は構成テンプレート変数であり、その特定のSAMLアクションのドメイン名を表します。実際の値は、構成ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3：変数値を指定する」セクションを参照してください。

デバイスのすべてのSAMLアクションを見つけるには、コマンド`show samlaction`を実行します。

**ステップ2：インスタンスを選択する**

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択し、**次へ**をクリックします。

#### ステップ3：変数値を指定する

変数値を入力します。

- `saml_action_patset`: SAMLアクションの名前を追加します
- `saml_action_domain1`: `https://<example1.com>/`の形式でドメインを入力します
- `saml_action_name`: ジョブを設定しているSAMLアクションと同じものを入力します

変数を指定します(/en-us/netscaler-application-delivery-management-software/media/specify-variables-cve-2021-22927-2021-22920.png)

#### ステップ4：構成をプレビューする

構成に挿入された変数値をプレビューし、**次へ**をクリックします。

ジョブをプレビューします(/en-us/netscaler-application-delivery-management-software/media/preview-job-cve-2021-22927-2021-22920.png)

#### ステップ5：ジョブを実行する

構成ジョブを実行するには、**完了**をクリックします。

構成ジョブを実行します(/en-us/netscaler-application-delivery-management-software/media/run-job-cve-2021-22927-2021-22920.png)

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

脆弱なすべてのNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### シナリオ

このシナリオでは、2つのNetScalerインスタンスがCVE-2021-22920に対して脆弱であり、すべてのインスタンスを修復する必要があります。以下の手順に従ってください。

1. このドキュメントの「インスタンスのアップグレード」セクションに記載されている手順に従って、3つのNetScalerインスタンスすべてをアップグレードします。
2. 構成ジョブワークフローを使用して、一度に1つのNetScalerに構成パッチを適用します。このドキュメントの「構成コマンドの適用」セクションに記載されている手順を参照してください。

脆弱なNetScaler 1には、2つのSAMLアクションがあります。

- SAMLアクション1には1つのドメインがあります
- SAMLアクション2には2つのドメインがあります

構成ジョブワークフローを開始する(/en-us/netscaler-application-delivery-management-software/media/scenario-config-job-workflow-cve-2021-22927-2021-22920.png)

NetScaler 1を選択し、**構成ジョブワークフローに進む**をクリックします。組み込みのベーステンプレートが自動的に入力されます。次に、ジョブ名を入力し、指定された構成に従ってテンプレートをカスタマイズします。

指定されたシナリオのテンプレートをカスタマイズする(/en-us/netscaler-application-delivery-management-software/media/scenario-customize-template-cve-2021-22927-2021-22920.png)

次の表に、カスタマイズされたパラメーターの変数定義を示します。

表。SAMLアクションの変数定義

| NETSCALER構成 | PATSETの変数定義 | SAMLアクション名の変数定義 | ドメインの変数定義 |
|---|---|---|---|
| SAMLアクション1には1つのドメインがあります | saml_action_patset1 | saml_action_name1 | saml_action_domain1 |
| SAMLアクション2には2つのドメインがあります | saml_action_patset2 | saml_action_name2 | saml_action_domain2, saml_action_domain3 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**インスタンスの選択**で、NetScaler 1を選択し、**次へ**をクリックします。**変数値の指定**ウィンドウが表示されます。このステップでは、前のステップで定義されたすべての変数に値を提供する必要があります。

変数のシナリオを指定する(/en-us/netscaler-application-delivery-management-software/media/specify-variables-scenario-cve-2021-22927-2021-22920.png)

次に、変数をレビューします。

変数のシナリオをレビューする(/en-us/netscaler-application-delivery-management-software/media/review-variables-scenario-cve-2021-22927-2021-22920.png)

**次へ**をクリックし、**完了**をクリックしてジョブを実行します。

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

NetScaler1の2つの修復手順を完了したら、NetScaler 2とNetScaler 3を修復するために同じ手順に従います。修復が完了したら、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

## CVE-2021-22956の脆弱性を特定して修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**Current CVEs > `<number of>`** の「NetScalerインスタンスが共通脆弱性識別子 (CVE) の影響を受けています」の下に、この特定のCVEによって脆弱なすべてのインスタンスが表示されます。CVE-2021-22956の影響を受けるインスタンスの詳細を確認するには、CVE-2021-22956を選択し、**影響を受けるインスタンスを表示** をクリックします。

- `<number of>` 「CVEの影響を受けるNetScalerインスタンス」ウィンドウが表示されます。ここには、CVE-2021-22956の影響を受けるNetScalerインスタンスの数と詳細が表示されます。

- セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2021-22956の影響が反映されるまでに時間がかかる場合があります。影響をより早く確認するには、**今すぐスキャン** をクリックしてオンデマンドスキャンを開始します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CVE-2021-22956の影響を受けるインスタンスを特定する

CVE-2021-22956にはカスタムスキャンが必要です。このスキャンでは、NetScaler Consoleサービスが管理対象のNetScalerインスタンスに接続し、スクリプトをインスタンスにプッシュします。スクリプトはNetScalerインスタンス上で実行され、Apache設定ファイル ( `httpd.conf file` ) と最大クライアント接続数 ( `maxclient` ) のパラメータをチェックして、インスタンスが脆弱であるかどうかを判断します。スクリプトがNetScaler Consoleサービスと共有する情報は、脆弱性ステータスをブール値 (trueまたはfalse) で示したものです。スクリプトはまた、NetScaler Consoleサービスに、ローカルホスト、NSIP、管理アクセスを持つSNIPなど、異なるネットワークインターフェースのmax_clientsのカウントリストを返します。

このスクリプトは、スケジュールされたスキャンまたはオンデマンドスキャンが実行されるたびに実行されます。スキャンが完了すると、スクリプトはNetScalerインスタンスから削除されます。

### CVE-2021-22956を修正する

CVE-2021-22956の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの **Current CVEs > NetScalerインスタンスがCVEの影響を受けています** の下に、ステップ1と2が表示されます。

2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。

Current CVEs > NetScaler instances impacted by CVEs の下には、この2段階の修復プロセスに対応する2つの異なるワークフローが表示されます。これらは「Proceed to upgrade workflow」と「Proceed to configuration job workflow」です。

#### ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「NetScaler アップグレードジョブの作成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

### ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、`<number of>` **NetScaler instances impacted by CVEs** ウィンドウで、CVE-2021-2295 の影響を受けるインスタンスを選択し、**Proceed to configuration job workflow** をクリックします。ワークフローには次の手順が含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が設定された最終構成の確認。
5. ジョブの実行。

インスタンスを選択し、**Proceed to configuration job workflow** をクリックする前に、次の点に注意してください。

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956など）の影響を受けるNetScalerインスタンスの場合：インスタンスを選択して **Proceed to configuration job workflow** をクリックしても、組み込みの構成テンプレートは の下に自動入力されません。適切な構成ジョブテンプレートを **Security Advisory Template** の下から手動で右側の構成ジョブペインにドラッグアンドドロップしてください。
- CVE-2021-22956のみの影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2021-22956のみの影響を受けているとします。これらのインスタンスをすべて選択し、**Proceed to configuration job workflow** をクリックすると、組み込みの構成テンプレートが **Select configuration** の下に自動入力されます。
- CVE-2021-22956と1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスで、各NetScalerに一度に修正を適用する必要がある場合：これらのインスタンスを選択して **Proceed to configuration job workflow** をクリックすると、各NetScalerで一度に構成ジョブを実行するように指示するエラーメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

#### ステップ1：構成の選択

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが **Select configuration** の下に自動入力されます。



#### ステップ2：インスタンスの選択

影響を受けるインスタンスは **Select Instances** の下に自動入力されます。インスタンスを選択します。このインスタンスがHAペアの一部である場合は、**Execute on Secondary Nodes** を選択します。**Next** をクリックします。



**注**

クラスターモードのNetScalerインスタンスの場合、NetScaler Consoleセキュリティアドバイザリを使用すると、NetScaler Consoleはクラスター構成コーディネーター（CCO）ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

`rc.netscaler` はすべてのHAノードとクラスターノード間で同期され、再起動後も修正が永続的になります。

#### ステップ3：変数値を指定する

変数値を入力します。

変数を指定する(/en-us/netscaler-application-delivery-management-software/media/specify-variables-cve-2021-22956.png)

インスタンスの変数を指定するには、次のいずれかのオプションを選択します。

**すべてのインスタンスに共通の変数**: 変数`max_client`に共通の値を入力します。

**変数値を入力ファイルでアップロード**: **入力キーファイルのダウンロード**をクリックして、入力ファイルをダウンロードします。入力ファイルで、変数`max_client`の値を入力し、ファイルをNetScaler Consoleサーバーにアップロードします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

上記の両方のオプションで、推奨される`max_client`値は30です。現在の値に応じて値を設定できます。ただし、ゼロであってはならず、`/etc/httpd.conf`ファイルで設定されているmax_client以下である必要があります。NetScalerインスタンスで文字列`MaxClients`を検索することで、Apache HTTP Server構成ファイル`/etc/httpd.conf`に設定されている現在の値を確認できます。

#### ステップ4：構成をプレビューする

構成に挿入された変数値をプレビューし、**次へ**をクリックします。

ジョブをプレビューする(/en-us/netscaler-application-delivery-management-software/media/preview-job-cve-2021-22956.png)

#### ステップ5：ジョブを実行する

**完了**をクリックして、構成ジョブを実行します。

構成ジョブを実行する(/en-us/netscaler-application-delivery-management-software/media/run-job-cve-2021-22956.png)

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

## CVE-2022-27509の脆弱性を特定し、修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**現在のCVE `<number of>` CVEの影響を受けるNetScalerインスタンス**の下に、CVE-2022-27509によって脆弱なすべてのインスタンスが表示されます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2022-27509を選択し、**影響を受けるインスタンスを表示**をクリックします。

**注**

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリのタブでCSVレポートをダウンロードしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**<number of> CVEの影響を受けるNetScalerインスタンス**ウィンドウが表示されます。次のスクリーンショットでは、CVE-2022-27509の影響を受けるNetScalerインスタンスの数と詳細を確認できます。



セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

**注**

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2022-27509の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始してください。

### CVE-2022-27509の影響を受けるインスタンスを特定する

CVE-2022-27509には、カスタムスキャンとバージョンスキャンの組み合わせが必要です。カスタムスキャンの一環として、NetScaler Consoleサービスは管理対象のNetScalerインスタンスに接続し、スクリプトをインスタンスにプッシュします。スクリプトはNetScalerインスタンス上で実行され、インスタンスが脆弱であるかどうかを判断します。このスクリプトは、スケジュールされたスキャンまたはオンデマンドスキャンが実行されるたびに実行されます。

スキャンが完了すると、スクリプトはNetScalerインスタンスから削除されます。

これらのセキュリティアドバイザリカスタムスキャンをオプトアウトすることもできます。カスタムスキャン設定とカスタムスキャンのオプトアウトの詳細については、**セキュリティアドバイザリ**ページの**カスタムスキャン設定の構成**セクションを参照してください。

### CVE-2022-27509を修正する

CVE-2022-27509の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUIの**Current CVEs > NetScaler instances are impacted by CVEs**で、修正手順を確認できます。

**Current CVEs> NetScaler instances impacted by CVEs**の下に、この単一ステップの修正プロセスとして、**Proceed to upgrade workflow**という以下のワークフローが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

**重要**

脆弱なNetScalerインスタンスが/etc/httpd.confファイルを/nsconfigディレクトリにコピーしている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。



## セキュリティアドバイザリにおけるサポートされていないCVE

NetScaler Consoleセキュリティアドバイザリは、すべての新しい共通脆弱性識別子 (CVE) を追跡し、インフラストラクチャに対するCVEの影響を評価します。推奨事項を確認し、適切な措置を講じることができます。しかし、サポートされていないCVEがいくつかあり、脆弱性の検出と修復はNetScaler Consoleセキュリティアドバイザリの範囲外です。

- **CVE-2022-21827**:

  CVE-2022-21827は、Windows用NetScaler Gatewayプラグインのバージョン21.9.1.2より前のサポートされているバージョンに影響を与えます。

  Windows用NetScaler Gatewayプラグインに影響を与える脆弱性の検出と修復は、NetScaler Consoleではサポートされていません。また、NetScaler Gatewayプラグインの脆弱性は、NetScaler側でチェックを実行したり、NetScalerのバージョンを確認したり、NetScalerの設定をチェックしたりすることでは評価できません。このCVEの検出と修復は、クライアントに展開されているWindows用NetScaler Gatewayプラグインのバージョンに基づいてのみ評価できます。

  その結果、この脆弱性の検出と修復はNetScaler Consoleセキュリティアドバイザリの範囲外です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# アップグレードアドバイザリ

NetScaler Console リリース 14.1 ビルド 66.x 以降、アップグレードアドバイザリ機能は完全にサポートされています。Cloud Connect を有効にすることで、この機能にアクセスして使用できます。Cloud Connect が正常に確立されると、アップグレードアドバイザリは自動的に有効になります。

**重要**

Cloud Connect が完全に有効になっており、すべての前提条件が完了していることを確認してください。Cloud Connect 接続に問題があると、アップグレードアドバイザリが利用できなくなります。



ネットワーク管理者として、NetScaler Console で異なる NetScaler リリースで実行されている多くの NetScaler インスタンスを管理しているかもしれません。各 NetScaler インスタンスのライフサイクルを監視することは、面倒な作業になる可能性があります。NetScaler 製品マトリックスにアクセスし、End of Life (EOL) または End of Maintenance (EOM) に達している、または達した NetScaler インスタンスを特定し、その後、アップグレードを計画する必要があります。

このプロセスを容易にするために、NetScaler Console のアップグレードアドバイザリは、次の方法で NetScaler インスタンスのライフサイクルを監視するのに役立ちます。

- EOL または EOM に達している、または達したインスタンスを特定します。これにより、EOL または EOM 日付より前に NetScaler のアップグレードを計画できます。
- 最新のリリースまたはビルドではないインスタンスを強調表示します。これらのインスタンスを最新のリリースまたはビルドにアップグレードできます。このアップグレードにより、新機能や修正された問題に関する更新を受け取ることができます。
- 推奨される NetScaler ビルドではないインスタンスを強調表示します。一部の組織では、インスタンスに対して推奨される NetScaler ビルドがある場合があります。NetScaler Console では、ビルドの安定性、機能、その他の考慮事項に応じて、組織の推奨ビルドを設定できます。その後、推奨ビルドではないインスタンスを確認し、アップグレードします。推奨ビルドを実行しているインスタンスは、星のアイコンで示されます。
- 最も人気のあるリリースまたはビルドで実行されているインスタンスを強調表示します。人気のあるビルドを実行しているインスタンスは、リボンアイコンで示されます。

アップグレードアドバイザリは、対応するリリースノートへのリンクを提供します。この情報により、アップグレードする NetScaler ビルドを確認し、決定できます。アップグレードアドバイザ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リページから NetScaler インスタンスをアップグレードするためのメンテナンスジョブの作成に進むことができます。

**重要:**

アップグレードアドバイザリは、NetScaler ソフトウェアリリースの EOL のみを監視します。NetScaler アプライアンスの EOL は確認しません。

## アップグレードアドバイザリを表示

**Infrastructure > Instance Advisory > Upgrade Advisory** に移動し、次の情報を表示します。

- NetScaler インスタンスの総数。
- サポート終了に達するインスタンス。
- メンテナンス終了に達するインスタンス。
- 古いビルドのインスタンス。
- 推奨ビルドではないインスタンス。
- さまざまな NetScaler リリースのサポート終了日とメンテナンス終了日。

アップグレードアドバイザリページ(/en-us/netscaler-application-delivery-management-software/media/upgrade-advisory-adm.png)

**Upgrade Advisory** ページには、NetScaler インスタンスがリリースごとにグループ化されています。**Release Notes** リンクをクリックすると、特定の NetScaler リリースノートが表示されます。アップグレードを決定する前に、新機能、修正された問題、既知の問題を確認してください。異なるリリースにわたる複数の NetScaler インスタンスを一度に選択してアップグレードできます。アップグレードを進めると、アップグレードジョブが作成されます。「NetScaler インスタンスのアップグレード」を参照してください。

## 推奨ビルドを設定する

管理者として、組織の推奨 NetScaler ビルドを定義できます。推奨ビルドを設定するには、次の手順を実行します。

1. 「**インフラストラクチャ > インスタンスアドバイザリ > アップグレードアドバイザリ**」で、「**設定**」をクリックします。
2. 推奨リリースとビルドを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

推奨ビルドを設定する(/en-us/netscaler-application-delivery-management-software/media/set-preferred-build.png)

この例では、推奨ビルドは `13.0-58.30` と `13.0-67.39` です。

3. 「**保存**」をクリックします。

## NetScalerインスタンスをアップグレードする

**アップグレードアドバイザリ**ページで、確認後、必要なNetScalerインスタンスをアップグレードするには、次の手順を実行します。

1. アップグレードするインスタンスビルドを選択し、「**アップグレードするインスタンスを選択**」をクリックします。
2. アップグレードするNetScalerインスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。

   アップグレードワークフロー(/en-us/netscaler-application-delivery-management-software/media/upgrade-workflow.png)

   このワークフローはアップグレードジョブを作成します。
3. **インスタンスの選択**タブで、,

   a. アップグレードジョブに名前を指定します。
   b. (オプション) 他のインスタンスを追加する場合は、「**インスタンスの追加**」をクリックします。
   c. 「**次へ**」をクリックします。

4. **イメージの選択**タブで、イメージライブラリ、ローカル、またはアプライアンスからNetScalerイメージを選択します。

   - **イメージライブラリから選択**: リストからNetScalerイメージを選択します。このオプションには、NetScalerダウンロードWebサイトで利用可能なすべてのNetScalerイメージが一覧表示されます。

     NetScalerイメージ(/en-us/netscaler-application-delivery-management-software/media/adc-images.png)

     NetScalerソフトウェアイメージには、星のアイコンが付いた推奨ビルドと、ブックマークアイコンが付いた最もダウンロードされたビルドが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ローカルまたはアプライアンスから選択**: イメージをローカルコンピューターまたはNetScalerアプライアンスからアップロードできます。NetScalerアプライアンスを選択すると、NetScaler Console GUIに`/var/mps/mps_images`にあるインスタンスファイルが表示されます。NetScaler Console GUIからイメージを選択します。
- **選択したイメージがすでに利用可能な場合は、NetScalerへのイメージのアップロードをスキップする** - このオプションは、選択したイメージがNetScalerで利用可能かどうかを確認します。アップグレードジョブは新しいイメージのアップロードをスキップし、NetScalerで利用可能なイメージを使用します。
- **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップする** - このオプションは、インスタンスのアップグレード後、NetScalerインスタンス内のアップロードされたイメージをクリアします。

**次へ**をクリックして、選択したインスタンスでアップグレード前の検証を開始します。

5. **アップグレード前の検証**タブに、失敗したインスタンスが表示されます。失敗したインスタンスを削除して、**次へ**をクリックできます。

   - **ディスク容量の確認**: インスタンスでディスク容量が不足している場合は、ディスク容量を確認してクリーンアップできます。参照: NetScalerのディスク容量をクリーンアップする。
   - **ポリシーの確認**: NetScaler Consoleがサポートされていないクラシックポリシーを検出した場合、アップグレードジョブを作成するためにそれらのポリシーを削除できます。

   **注:**

   クラスターIPアドレスを指定した場合、NetScaler Consoleは指定されたインスタンスに対してのみアップグレード前の検証を実行し、他のクラスターノードに対しては実行しません。

6. オプションで、**カスタムスクリプト**タブで、インスタンスのアップグレード前後に実行するスクリプトを指定します。

   詳細については、「カスタムスクリプトの使用」を参照してください。

7. **タスクのスケジュール**で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード** - アップグレードジョブはすぐに実行されます。
   - **後でスケジュール** - このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerの高可用性ペアを2段階でアップグレードする場合は、「HAノードの2段階アップグレードを実行」を選択します。

2段階アップグレードを実行(/en-us/netscaler-application-delivery-management-software/media/upgrade-two-stage-on-adc-ha.png)

詳細については、NetScaler高可用性ペアのアップグレードを参照してください。

8. 「**ジョブの作成**」タブで、次の詳細を指定します。

   アップグレードジョブをスケジュールする場合、インスタンスにイメージをアップロードするタイミングを指定できます。

   - 「**今すぐアップロード**」: このオプションを選択すると、イメージがすぐにアップロードされます。ただし、アップグレードジョブはスケジュールされた時間に実行されます。
   - 「**実行時にアップロード**」: このオプションを選択すると、アップグレードジョブの実行時にイメージがアップロードされます。

その他のオプションの詳細については、NetScalerアップグレードオプションを参照してください。

# オーケストレーション

SDN（Software Defined Networking）では、ネットワークをサポートするハードウェアの代わりに、ソフトウェアアプリケーションコントローラがネットワークとそのアクティビティを管理します。つまり、SDNを使用すると、ネットワーク管理者は物理ネットワーク接続を論理ネットワーク接続に仮想化し、ソフトウェアベースの一元管理ツールを使用してネットワークサービスを管理できます。SDNにより、ネットワークエンジニアと管理者は、急速に変化するビジネス要件に対応できます。

SDNのよりよく知られている利点は、トラフィックのプログラマビリティ、より高い俊敏性、ポリシー駆動型ネットワーク監視の作成能力、およびネットワーク自動化の実装ですが、SDNの具体的な利点のいくつかを以下に示します。

- 一元化されたネットワークプロビジョニング
- 詳細なレベルでのネットワークセキュリティの向上
- 運用コストの削減
- クラウド抽象化レベルの向上
- 保証されたコンテンツ配信
- ネットワークダウンタイムの削減

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleは、さまざまなベンダーのSDNコントローラと統合することで、エンタープライズネットワークにおけるSDNをサポートします。NetScaler Consoleは、VMware NSX ManagerとCisco Application Policy Infrastructure Controller（APIC）の両方をサポートしています。

## VMware NSX マネージャー

NetScaler Consoleは、VMwareネットワーク仮想化プラットフォームと統合し、NetScalerサービスの展開、構成、および管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが抽象化され、vSphere/vCenter管理者はNetScalerサービスをより迅速にプログラムで展開できるようになります。

VMware NSX Managerは、論理ファイアウォール、スイッチ、ルーター、ポート、およびその他のネットワーク要素を公開し、多様なハイパーバイザー、クラウド管理システム、および関連するネットワークハードウェア間での仮想ネットワークを可能にします。また、外部ネットワークおよびセキュリティサービスもサポートしています。

NetScaler Consoleのクラウドオーケストレーション機能は、NetScaler製品とVMware NSXの統合を可能にし、以下の機能を提供します。

- サービス挿入の一部として、特定のEdgeゲートウェイに事前プロビジョニングされたVPXをオンデマンドで割り当てる機能。
- NSX環境内で実行されているインスタンス上で、アプリケーションテンプレートを介して、基本的なロードバランシングに加えて、SSLやCSなどのNetScalerの高度な機能を構成する機能。
- サービス削除の一環として、特定のEdgeゲートウェイからVPXの割り当てを解除し、同じVPXを別のEdgeゲートウェイに再割り当てする機能。
- アプリケーションに必要なすべてのインフラストラクチャの展開ワークフローの一環として、vCenterコンソールからNetScaler機能を迅速に展開する機能。

利点:

- アプリケーション展開ワークフローの一環としての、新しいNetScalerサービスの自動オンデマンド割り当て
- アプリケーションテンプレートを介した、アプリケーション固有の高度なNetScaler機能の簡素化された構成
- マルチテナントの職務分離とセルフサービス消費モデルにより、クラウド管理者に単一の制御ポイントを提供
- 予期せぬ将来の用途をサポートするのに役立つNetScaler Console APIとのより簡単な統合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ConsoleでVMware NSX Managerを構成する方法の詳細については、「VMware NSX ManagerとのNetScalerアプライアンスの統合」を参照してください。

## OpenStack: NetScalerインスタンスの統合

NetScaler Consoleのクラウドオーケストレーション機能により、NetScaler製品とOpenStackプラットフォームの統合が可能になります。この機能をOpenStackプラットフォームで使用することで、OpenStackユーザーはNetScalerのロードバランシング機能（LBaaS）を利用できます。これにより、OpenStackユーザーはOpenStackからNetScalerインスタンスにロードバランサー構成を展開できます。

以下のセクションでは、NetScaler Consoleの機能とOpenStack統合ワークフローについて簡単に説明します。

### OpenStack Neutron LBaaS用NetScalerドライバー

OpenStack Neutron LBaaSプラグインには、OpenStackがNetScaler Consoleと通信できるようにするNetScalerドライバーが含まれています。OpenStackはこのドライバーを使用して、LBaaS APIを介して行われたロードバランシング構成をNetScaler Consoleに転送し、NetScaler Consoleは目的のNetScalerインスタンスにロードバランサー構成を作成します。OpenStackはまた、このドライバーを使用して、定期的にNetScaler Consoleを呼び出し、NetScalerからすべてのロードバランシング構成のさまざまなエンティティ（VIPやプールなど）のステータスを取得します。OpenStackプラットフォーム用のNetScalerドライバーソフトウェアは、NetScaler Consoleにバンドルされています。ドライバーをダウンロードしてインストールするには、まずNetScaler Consoleをインストールしてアプリケーションを起動する必要があります。

### NetScaler ConsoleとOpenStackの相互登録

まず、NetScaler ConsoleにOpenStack情報を登録する必要があります。OpenStackコントローラーのIPアドレスとクラウド管理ユーザーの資格情報、およびOpenStack NetScalerドライバーのユーザー資格情報を指定します。後で、Neutron構成ファイル（neutron.conf）のNetScaler_driverセクションに同じログイン資格情報を指定することで、OpenStackのNetScalerドライバーがLB構成中にNetScaler Consoleに接続できるようになります。

OpenStackとNetScaler Consoleが相互に登録されると、両者は通信できるようになります。また、OpenStackユーザーは、OpenStackの既存の資格情報を使用してNetScaler Consoleユーザーインターフェイスにログオンし、NetScalerでのLB構成のパフォーマンスを確認できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### OpenStackのテナント

OpenStackでは、テナントはプロジェクトとも呼ばれます。テナントはユーザーのグループであり、テナントまたはプロジェクトは、分離されたユーザーグループに割り当てられたリソース（コンピューティング、ネットワーク、ストレージなど）のセットとしても定義できます。

### 配置ポリシー

配置ポリシーは、ユーザーが作成する各ロードバランサー構成で使用されるNetScalerインスタンスを決定する柔軟性を提供します。あるいは、NetScaler Consoleは、OpenStackテナントに基づいてNetScalerインスタンスを割り当てるオプションも提供します。

### サービスパッケージ

サービスパッケージは、ポリシー/SLA、デバイスまたは自動プロビジョニング構成仕様、およびテナント/配置ポリシーをまとめたバンドルです。サービスパッケージは通常、テナントに提供される分離ポリシーの観点から定義されます。

サービスパッケージに関するいくつかのポイントを以下に示します。

- テナントは複数のサービスパッケージに属することはできません。
- 複数のテナントを同じサービスパッケージに関連付けることができます。
- 自動プロビジョニングが設定されているサービスパッケージでは、仮想NetScalerインスタンスは1つのプラットフォームタイプ（SDXプラットフォームまたはOpenStack Computeプラットフォーム上）からのみ作成できます。

### LBaaS V1およびLBaaS V2でサポートされる機能

OpenStackのLBaaS V1ドライバーはOpenStack Horizonユーザーインターフェイスからの操作をサポートしますが、LBaaS V2ドライバーはコマンドライン操作のみをサポートします。

以下に、OpenStackのLBaaS V1とLBaaS V2の両方でサポートされる機能を示します。

- LBaaS V1
  - ロードバランシング
- LBaaS V2
  - ロードバランシング
  - OpenStackのキーマネージャーである**Barbican**によって管理される証明書によるSSLオフロード
  - 証明書バンドル（中間認証局を含む）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SNIサポート

このドキュメントでは、以下の情報を提供します。

- ユースケースシナリオ
- NetScaler ConsoleとOpenStackワークフローの統合
- 前提条件
- NetScaler ConsoleとOpenStackでの事前構成タスク
- Horizonを使用したLBaaS V1の構成手順
- コマンドラインを使用したLBaaS V2の構成手順
- OpenStackでのNetScaler VPXインスタンスの手動プロビジョニング
- NetScaler ConsoleとOpenStack Heatサービスとの統合
- NetScaler ConsoleでのOpenStackアプリケーションの監視

## ユースケースシナリオ

以下のユースケースシナリオでは、NetScaler ConsoleとOpenStackプラットフォームを統合するワークフローについて説明します。

Example-Cloud-Providerという企業は、OpenStackコンポーネントを使用して、テナントにインフラストラクチャを提供するクラウドをセットアップしました。Steveはこのクラウドプロバイダーの管理者であり、TomはExample-Cloud-Providerのクラウドインフラストラクチャのテナントです。Tomの組織であるExample-SportsOnline.comは、2台のサーバーS1とS1を必要としており、TomはOpenStackプラットフォーム上のサーバーS1とS2間のトラフィックをロードバランスするために専用のNetScalerデバイスも必要としています。

この要件を満たすために、SteveはOpenStackとNetScaler Consoleの両方をインストールして構成し、互換性があるように準備する必要があります。SteveはOpenStackにExample-SportsOnlineというテナントアカウントを作成し、そのテナントアカウントにリソースを割り当てる必要があります。また、SteveはExample-SportsOnlineがそのリソースと構成を管理するための異なるログオン資格情報（ユーザー）を作成する必要があります。TomはこれでOpenStack上に2台のサーバーS1とS2を作成し、組織内のトラフィックを管理できます。

SteveはOpenStackの詳細をNetScaler Consoleに登録し、OpenStackのネットワークコンポーネントであるNeutronでNetScaler LBaaSドライバーを構成する必要があります。登録が完了すると、NetScaler ConsoleはOpenStackからのすべてのテナントの詳細を表示します。Steveは、NetScaler LBaaS機能を必要とするリストからExample-SportsOnlineを選択し、TomがNetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consoleでロードバランサー構成のために専用のNetScalerを割り当てられるように構成できます。

このため、SteveはNetScaler Consoleユーザーインターフェイスを使用してOpenStackのコンピューティング層（Nova）にNetScaler VPXインスタンスをプロビジョニングするか、TomがOpenStackでLB構成を行う際に、MASを有効にしてNetScaler VPXインスタンスをオンデマンドで自動プロビジョニングすることができます。どちらの場合でも、NetScaler ConsoleがVPXインスタンスを管理します。これを実現するために、SteveはNetScaler Consoleでサービスパッケージを作成し、TomとのSLAで合意された条件をサービスパッケージで定義します。たとえば、SteveはTomにロードバランサー構成を提供するための専用インスタンスを提供するために、「専用」分離ポリシーを選択します。つまり、Steveはサービスパッケージでtomのために非共有インスタンスを選択します。その後、彼は多くのNetScaler VPXインスタンスをサービスパッケージに割り当て、専用のNetScalerを必要とするExample-SportsOnlineと他のテナントをサービスパッケージに関連付けます。その結果、Tomが最初のロードバランサー構成を実行すると、NetScaler Consoleはサービスパッケージ内のNetScaler VPXインスタンスの1つをExample-SportsOnlineに割り当て、そのNetScalerに構成を展開します。

Tomは、OpenStack LBaaS/UIを使用して、プール、仮想IP（VIP）、およびヘルスモニターを作成することで、ロードバランシング構成を作成できるようになりました。OpenStackのプールとVIPは、NetScalerインスタンス上でサービスグループおよび仮想サーバーとして展開されます。Tomはまた、サーバーを監視するためのヘルスモニターを作成し、任意の時点で稼働しており、NetScalerから到達可能なサーバーにのみアプリケーショントラフィックを送信することができます。

OpenStackで作成されたロードバランシング設定が、NetScalerインスタンスに実装されました。完全に設定されると、NetScaler VPXインスタンスはロードバランシング機能を引き継ぎ、アプリケーションのトラフィックを受け入れ始め、Tomが作成したサーバーS1とS2間のトラフィックをロードバランスします。

### NetScaler ConsoleとOpenStackワークフローの統合

以下のフローチャートは、LBaaS V1およびLBaaS V2を設定する際に従うべきワークフローを示しています。

LBaaS V1およびV2設定ワークフロー(/en-us/netscaler-application-delivery-management-software/media/openstack-orchestartion-workflow-console.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## OpenStack: NetScalerインスタンスの統合

NetScaler Consoleのクラウドオーケストレーション機能により、NetScaler製品とOpenStackプラットフォームの統合が可能になります。この機能をOpenStackプラットフォームで使用することで、OpenStackユーザーはNetScalerのロードバランシング機能（LBaaS）を利用できます。これにより、OpenStackユーザーはOpenStackからNetScalerインスタンスにロードバランサー構成を展開できます。

以下のセクションでは、NetScaler Consoleの機能とOpenStack統合ワークフローについて簡単に説明します。

### OpenStack Neutron LBaaS用NetScalerドライバー

OpenStack Neutron LBaaSプラグインには、OpenStackがNetScaler Consoleと通信できるようにするNetScalerドライバーが含まれています。OpenStackはこのドライバーを使用して、LBaaS APIを介して行われたロードバランシング構成をNetScaler Consoleに転送し、NetScaler Consoleは目的のNetScalerインスタンスにロードバランサー構成を作成します。OpenStackはまた、このドライバーを使用して、定期的にNetScaler Consoleを呼び出し、NetScalerからすべてのロードバランシング構成のさまざまなエンティティ（VIPやプールなど）のステータスを取得します。OpenStackプラットフォーム用のNetScalerドライバーソフトウェアは、NetScaler Consoleにバンドルされています。ドライバーをダウンロードしてインストールするには、まずNetScaler Consoleをインストールしてアプリケーションを起動する必要があります。

### NetScaler ConsoleとOpenStackの相互登録

まず、NetScaler ConsoleにOpenStack情報を登録する必要があります。OpenStackコントローラーのIPアドレスとクラウド管理ユーザーの資格情報、およびOpenStack NetScalerドライバーのユーザー資格情報を指定します。後で、Neutron構成ファイル（neutron.conf）のNetScaler_driverセクションに同じログイン資格情報を指定することで、OpenStackのNetScalerドライバーがLB構成中にNetScaler Consoleに接続できるようになります。

OpenStackとNetScaler Consoleが相互に登録されると、両者は通信できるようになります。また、OpenStackユーザーは、OpenStackの既存の資格情報を使用してNetScaler Consoleユーザーインターフェイスにログオンし、NetScalerでのLB構成のパフォーマンスを確認できます。

### OpenStackのテナント

OpenStackでは、テナントはプロジェクトとも呼ばれます。テナントはユーザーのグループであり、テナントまたはプロジェクトは、分離されたユーザーグループに割り当てられたリソース（コンピューティング、ネットワーク、ストレージなど）のセットとしても定義できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 配置ポリシー

配置ポリシーは、ユーザーが作成する各ロードバランサー構成で使用されるNetScalerインスタンスを決定する柔軟性を提供します。あるいは、NetScaler Consoleは、OpenStackテナントに基づいてNetScalerインスタンスを割り当てるオプションも提供します。

### サービスパッケージ

サービスパッケージは、ポリシー/SLA、デバイスまたは自動プロビジョニング構成仕様、およびテナント/配置ポリシーをまとめたバンドルです。サービスパッケージは通常、テナントに提供される分離ポリシーの観点から定義されます。

サービスパッケージに関するいくつかのポイントを以下に示します。

- テナントは複数のサービスパッケージに属することはできません。
- 複数のテナントを同じサービスパッケージに関連付けることができます。
- 自動プロビジョニングが設定されているサービスパッケージでは、仮想NetScalerインスタンスは1つのプラットフォームタイプ（SDXプラットフォームまたはOpenStack Computeプラットフォーム上）からのみ作成できます。

### LBaaS V1およびLBaaS V2でサポートされる機能

OpenStackのLBaaS V1ドライバーはOpenStack Horizonユーザーインターフェイスからの操作をサポートしますが、LBaaS V2ドライバーはコマンドライン操作のみをサポートします。

以下に、OpenStackのLBaaS V1とLBaaS V2の両方でサポートされる機能を示します。

- LBaaS V1
  - ロードバランシング
- LBaaS V2
  - ロードバランシング
  - OpenStackのキーマネージャーである**Barbican**によって管理される証明書によるSSLオフロード
  - 証明書バンドル（中間認証局を含む）
  - SNIサポート

このドキュメントでは、以下の情報を提供します。

- ユースケースシナリオ
- NetScaler ConsoleとOpenStackワークフローの統合

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 前提条件
- NetScaler ConsoleとOpenStackでの事前構成タスク
- Horizonを使用したLBaaS V1の構成手順
- コマンドラインを使用したLBaaS V2の構成手順
- OpenStackでのNetScaler VPXインスタンスの手動プロビジョニング
- NetScaler ConsoleとOpenStack Heatサービスとの統合
- NetScaler ConsoleでのOpenStackアプリケーションの監視

### ユースケースシナリオ

以下のユースケースシナリオでは、NetScaler ConsoleとOpenStackプラットフォームを統合するワークフローについて説明します。

Example-Cloud-Providerという企業は、OpenStackコンポーネントを使用して、テナントにインフラストラクチャを提供するクラウドをセットアップしました。Steveはこのクラウドプロバイダーの管理者であり、TomはExample-Cloud-Providerのクラウドインフラストラクチャのテナントです。Tomの組織であるExample-SportsOnline.comは、2台のサーバーS1とS1を必要としており、TomはOpenStackプラットフォーム上のサーバーS1とS2間のトラフィックをロードバランスするために専用のNetScalerデバイスも必要としています。

この要件を満たすために、SteveはOpenStackとNetScaler Consoleの両方をインストールして構成し、互換性があるように準備する必要があります。SteveはOpenStackにExample-SportsOnlineというテナントアカウントを作成し、そのテナントアカウントにリソースを割り当てる必要があります。また、SteveはExample-SportsOnlineがそのリソースと構成を管理するための異なるログオン資格情報（ユーザー）を作成する必要があります。TomはこれでOpenStack上に2台のサーバーS1とS2を作成し、組織内のトラフィックを管理できます。

SteveはOpenStackの詳細をNetScaler Consoleに登録し、OpenStackのネットワークコンポーネントであるNeutronでNetScaler LBaaSドライバーを構成する必要があります。登録が完了すると、NetScaler ConsoleはOpenStackからのすべてのテナントの詳細を表示します。Steveは、NetScaler LBaaS機能を必要とするリストからExample-SportsOnlineを選択し、TomがNetScaler Consoleでロードバランサー構成のために専用のNetScalerを割り当てられるように構成できます。

このため、SteveはNetScaler Consoleユーザーインターフェイスを使用してOpenStackのコンピューティング層（Nova）にNetScaler VPXインスタンスをプロビジョニングするか、TomがOpenStackでLB構成を行う際に、MASを有効にしてNetScaler VPXインスタンスをオンデマンドで自動プロビジョニングすることができます。どちらの場合でも、NetScaler ConsoleがVPXインスタンスを管理します。これを実現するために、SteveはNetScaler Consoleでサービスパッケージ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を作成し、TomとのSLAで合意された条件をサービスパッケージで定義します。たとえば、SteveはTomにロードバランサー構成を提供するための専用インスタンスを提供するために、「専用」分離ポリシーを選択します。つまり、Steveはサービスパッケージで Tomのために非共有インスタンスを選択します。その後、彼は多くのNetScaler VPXインスタンスをサービスパッケージに割り当て、専用のNetScalerを必要とするExample-SportsOnlineと他のテナントをサービスパッケージに関連付けます。その結果、Tomが最初のロードバランサー構成を実行すると、NetScaler Consoleはサービスパッケージ内のNetScaler VPXインスタンスの1つをExample-SportsOnlineに割り当て、そのNetScalerに構成を展開します。

Tomは、OpenStack LBaaS/UIを使用して、プール、仮想IP（VIP）、およびヘルスモニターを作成することで、ロードバランシング構成を作成できるようになりました。OpenStackのプールとVIPは、NetScalerインスタンス上でサービスグループおよび仮想サーバーとして展開されます。Tomはまた、サーバーを監視するためのヘルスモニターを作成し、任意の時点で稼働しており、NetScalerから到達可能なサーバーにのみアプリケーショントラフィックを送信することができます。

OpenStackで作成されたロードバランシング設定が、NetScalerインスタンスに実装されました。完全に設定されると、NetScaler VPXインスタンスはロードバランシング機能を引き継ぎ、アプリケーションのトラフィックを受け入れ始め、Tomが作成したサーバーS1とS2間のトラフィックをロードバランスします。

### NetScaler ConsoleとOpenStackワークフローの統合

以下のフローチャートは、LBaaS V1およびLBaaS V2を設定する際に従うべきワークフローを示しています。

LBaaS V1およびV2設定ワークフロー(/en-us/netscaler-application-delivery-management-software/media/openstack-orchestartion-workflow-console.png)

## 前提条件

NetScaler仮想インスタンスをOpenStackプラットフォームと統合する前に、以下の要件が満たされていることを確認してください。

### NetScaler ConsoleおよびOpenStackのソフトウェア要件

- NetScaler Console 13.1が、最小ハードウェア要件システムを満たすサポート対象のハイパーバイザーワークステーションにインストールされていること。
- OpenStackコンポーネントがインストールされ、稼働していること。
- NetScaler Console 13.1は、以下のOpenStackバージョンをサポートしています - **Newton**、**Ocata**、**Pike**、**Queens**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Consoleのハードウェア要件

NetScaler仮想インスタンスをインストールするために、OpenStackサーバーに以下の仮想コンピューティングリソースがあることを確認してください。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 8 GB |
| 仮想CPU | 8 |
| ストレージ容量 | 500 GB |
| 仮想ネットワークインターフェース | 1 |
| スループット | 1 Gbps または 100 Mbps |

**注**

指定されたメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮した上で、OpenStackプラットフォームにNetScaler Consoleを展開するためのものです。OpenStackのハードウェア要件は、その上で実行される仮想マシンの数によって異なります。

## NetScaler ConsoleとOpenStackでの事前構成タスク

このセクションでは、NetScaler ConsoleとOpenStackを構成する前に、事前構成タスクを実行するのに役立ちます。

### NetScaler Consoleのインストール

サポートされているハイパーバイザーにNetScaler Consoleをインストールします。NetScaler Consoleのダウンロードとインストール方法の詳細については、「NetScaler Consoleの展開」を参照してください。

### NetScalerドライバーソフトウェアのインストールとOpenStackへのNetScaler Consoleの登録

NetScaler Consoleのダウンロードページから、OpenStack用NetScalerバンドルをダウンロードします。

### NetScaler Console GUIを使用してOpenStackプラットフォームにNetScalerドライバーをインストールするには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、 をクリックします。NetScaler Consoleの**** ページには、**Newton**、**Ocata**、**Pike**のOpenStackバージョンに必要な**OpenStack用NetScalerバンドル**ソフトウェアをダウンロードするためのリンクが用意されています。
2. 最新のNetScalerバンドルtarファイルをOpenStack Controllerの一時ディレクトリ（例: /tmp）にダウンロードします。このバンドルには、すべてのOpenStackリリース用のLBaaS V2ドライバーとHeatプラグインが含まれています。

   
3. NetScalerドライバーtarファイルからファイルを抽出するには、次のコマンドを実行します。

   `tar -xvzf <name_of_tar_file>`
4. OpenStack \<リリース名\> のセットアップがある場合は、プロンプトで次のコマンドを入力します。

   `cd <Release Name>`

   **例**:

   `cd Newton`
5. ドライバーをインストールし、NetScaler ConsoleのIPアドレス、OpenStackをNetScaler Consoleに登録したときに設定したNetScalerドライバーのパスワード、およびプロトコルを指定するには、次のコマンドを実行します。

   `./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>`

   **シングルノードOpenStackセットアップの例**:

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas`

   **マルチノードOpenStackセットアップの例**:

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages`

   **注**

   システムの`neutron-lbaas`ディレクトリのパスを指定することはオプションです。パスを指定すると、スクリプトがドライバーを見つけるのに役立つ場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ConsoleがOpenStackに正常に登録された後、OpenStackのユーザー資格情報を使用してNetScaler Consoleにログオンすることもできます。
NetScaler ConsoleがOpenStackに正常に登録されたら、OpenStack Neutronサービスを再起動します。

### OpenStackをNetScaler Consoleに登録する

**NetScaler Console GUIを使用してOpenStackをNetScaler Consoleに登録するには:**

1. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** の順に移動します。
2. **Configure OpenStack Settings** をクリックします。
3. **Configure OpenStack Settings** ページで、NetScaler ConsoleでOpenStackを設定するためのパラメータを設定できます。ここでは、DefaultとCustomizedの2つのオプションがあります。

   NewtonおよびOcataリリースのOpenStackでは、デフォルトまたはカスタマイズされた展開タイプのいずれかを使用できます。ただし、Pikeリリースでは、NetScaler ConsoleにOpenStackを登録するために、カスタマイズされた展開タイプを使用する必要があります。

- **デフォルトの展開タイプ**

  OpenStackサービスがデフォルトポートで実行されている場合は、**デフォルト**を選択します。たとえば、Neutronサービスのデフォルトポータルは9696、Keystoneサービスのデフォルトポータルは5000です。

1. OpenStackコントローラーのIPアドレス - OpenStackコントローラーのIPアドレス（**KeyStone**サービスと**Neutron**サービスの両方がこのIPアドレスで到達可能である必要があります）。たとえば、IPアドレス10.102.205.23を入力します。
2. OpenStack管理者ユーザー名 - OpenStackコントローラーの管理者ユーザー名。たとえば、admin1と入力します。
3. パスワード - OpenStackコントローラーの管理者ユーザーのパスワード。
4. OpenStack管理者テナント - OpenStack上の管理者テナントの名前。たとえば、adminと入力します。



- **カスタマイズされた展開タイプ**

  OpenStackサービスがデフォルトポートとは異なるポートで実行されている場合は、展開タイプとして**カスタマイズ**を選択します。これらのサービスが異なるポートで実行されている場合

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、ここで指定します。NetScaler ConsoleへのOpenStack Newtonおよび**Ocata**リリースの登録は、OpenStack Pikeリリースの登録とは異なります。

**OpenStackのNewtonおよびOcataリリース:**

a. OpenStackのNewtonリリースを登録する場合は、さまざまなOpenStackサービスのポート番号を指定します。
b. **デフォルト**設定で以前に指定したOpenStack管理者ユーザー名、パスワード、およびOpenStack管理者テナントユーザー名を指定します。

**OpenStackのPikeリリース:**

OpenStackのPikeリリースを登録する場合は、以下の画像に示すようにOpenStackサービスの詳細を入力します。また、デフォルト設定と同様に、OpenStack管理者ユーザー名、パスワード、およびOpenStack管理者テナントユーザー名を指定する必要があります。

1. **OpenStack Neutron LBaaS - NetScalerドライバーが使用する資格情報**セクションで、OpenStack NetScalerドライバーユーザーアカウントのNetScalerドライバーパスワードを設定します。NetScaler Consoleは、これらの資格情報を使用して、OpenStack NetScalerドライバーからの呼び出しを認証します。OpenStackコントローラーでNetScalerドライバーインストールスクリプトを実行するときは、同じパスワードを指定する必要があります。
2. **OK**をクリックします。

### OpenStackでのテナントの作成

OpenStackでプロジェクトまたはテナントを作成し、プロジェクトまたはテナントにユーザーを追加し、すべてのユーザーにロールを割り当てます。OpenStackのIDサービスである**KeyStone**は、各OpenStackサービスに認証サービスを提供します。認証サービスは、ドメイン、プロジェクト（テナント）、ユーザー、およびロールの組み合わせを使用します。

プロジェクトの作成方法やOpenStackでのその他のタスクの実行方法の詳細については、`<http://docs.openstack.org/>`のOpenStackドキュメントを参照してください。

### OpenStackテナントの追加

1. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **OpenStack Tenants**に移動し、**Add**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **OpenStackテナントの追加**ページで、**+Add**をクリックし、OpenStackテナントを選択します。
3. **OK**をクリックします。

OpenStackを統合する際に、事前プロビジョニングされたインスタンスを使用するか、インスタンスを自動プロビジョニングするかに応じて、次の2つのタスクのいずれかを実行します。

- NetScalerデバイスを事前プロビジョニングする
- OpenStackでNetScaler VPXデバイスを自動プロビジョニングする

### NetScalerデバイスのプロビジョニング

OpenStackを統合する際に、事前にプロビジョニングされたインスタンスを使用するか、インスタンスを自動プロビジョニングするかに応じて、以下の2つのタスクのいずれかを実行してください。

- NetScalerデバイスを事前にプロビジョニングする
- OpenStackでNetScaler VPXデバイスを自動プロビジョニングする

#### NETSCALERデバイスの事前プロビジョニング

Citrix Hypervisor、KVM、ESXなどのハイパーバイザープラットフォームにNetScalerデバイスをインストールし、そのインスタンスをNetScaler Consoleに追加します。NetScaler Consoleは、サーバー内のトラフィックをロードバランシングするこのデバイスを管理します。

**NetScaler Consoleに既存のNetScaler VPXインスタンスを追加するには：**

1. NetScaler Consoleで、**インフラストラクチャ** \> **インスタンス** \> **NetScaler VPX** に移動し、**追加** をクリックします。
2. **NetScaler VPXの追加** ページで、NetScaler VPXインスタンスのIPアドレスを指定し、**プロファイル名** リストからインスタンスプロファイルを選択します。インスタンスプロファイルには、NetScaler VPXにログオンするために使用される資格情報が含まれています。+アイコンをクリックして新しいインスタンスプロファイルを作成することもできます。**OK** をクリックします。

#### NETSCALERデバイスの自動プロビジョニング

必要なNetScalerインスタンスイメージをNetScalerダウンロードページからダウンロードし、OpenStackイメージングサービスであるGlanceにアップロードします。Glanceでイメージが利用可能になると、テナントにインスタンスを割り当てる際に、オンデマンドでNetScalerインスタンスを構成できます。

**OpenStackでNetScaler VPXデバイスを自動プロビジョニングするには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**オーケストレーション** \> **クラウドオーケストレーション** \> **OpenStack** に移動します。
2. **展開設定** をクリックします。
3. 次のパラメータを設定します。

    a. 管理ネットワーク - 自動プロビジョニングされたNetScaler VPXが接続されるOpenStack上の管理ネットワークを選択します。

    b. プロファイル名 - ドロップダウンリストからプロファイルを選択します。NetScaler Consoleは、このプロファイルに含まれるパスワードを使用して、新しく自動プロビジョニングされたNetScaler VPXインスタンスを設定します。

    c. ライセンス - 新しく自動プロビジョニングされたNetScalerインスタンスのライセンスに使用されるNetScaler Consoleライセンスアクセスコードを提供します。NetScaler Consoleは、管理ネットワーク内のOpenStackコンピュート上にNetScalerインスタンスをプロビジョニングし、指定されたライセンスコードを使用してそれらにライセンスのインストールをトリガーします。その後、NetScalerインスタンスは、ここで指定されたライセンスアクセスコードを使用して、Citrixウェブサイトからライセンスファイルをダウンロードします。

    d. Glance内のNetScaler VPXイメージ - NetScaler VPXインスタンスの作成に使用される、OpenStack Glanceで利用可能なNetScaler VPXイメージを選択します。

    e. プロキシ設定 - ライセンスをインストールするためのNetScalerプロキシサーバーの詳細を提供します。これは、NetScalerが管理ネットワークを介してインターネットに直接アクセスできない場合に必要となることがあります。

4. **OK**をクリックします。

**NetScaler Consoleでのサービスパッケージの作成**

**NetScaler Consoleでテナントのサービスパッケージを作成するには：**

1. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Service Packages**に移動し、**Add**をクリックします。
2. **Service Package**ページで、次のパラメーターを指定します。

    a. 名前 - サービスパッケージの名前。例：SVC-PKG-GOLDと入力します。

    b. NetScalerインスタンスの割り当て - サービスパッケージで定義されているインスタンス割り当てのタイプで、これに基づいてNetScalerインスタンスリソースがテナントに割り当て

© 1997–2026 Citrix Systems, Inc. All rights reserved.

られます。**Dedicated**を選択します。ポリシーの詳細については、「Service Package Isolation Policies」を参照してください。

c. NetScalerインスタンスのプロビジョニング - 既存のNetScalerインスタンスをテナントに割り当てるには、**Existing Instance**を選択します。設定中にNetScalerインスタンスを作成する場合は、**Create Instance OnDemand**を選択します。

d. NetScalerインスタンスタイプ - **NetScaler VPX**を選択します。

**注**

SDXプラットフォームでホストされている事前プロビジョニングされたNetScalerインスタンスを割り当てるには、NetScaler VPXを選択します。

3. テナントをサービスパッケージに関連付けるには、**続行**をクリックします。

**注**

高可用性モードでNetScalerインスタンスを展開している場合は、**高可用性用にNetScalerインスタンスのペアをプロビジョニング**を有効にします。

4. **インスタンスの割り当て**セクションで、**追加**をクリックし、テナントに割り当てるNetScalerインスタンスを選択して、**続行**をクリックします。
5. **OpenStackテナント/配置ポリシーの割り当て**セクションの**OpenStackテナント**の下にある**追加**をクリックしてテナントを選択します。
6. **続行**をクリックし、次に**完了**をクリックします。

**注**

ポリシーが見つからない場合、フォールバックメカニズムが再開され、NetScaler Consoleはテナントに基づいてNetScalerインスタンスを割り当てます。テナントがいずれのサービスパッケージにも属していない場合、NetScaler Consoleは「テナント\<admin\>はいずれのサービスパッケージにも属しておらず、デフォルトのサービスパッケージもありません。」というエラーメッセージを表示します。

### 配置ポリシーの作成 (オプション)

分離ポリシーはテナントベースだけではありません。ポリシーはテナント名やIDだけでなく、他のカスタム属性にも基づく、柔軟な配置ポリシーを作成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NetScaler Consoleでテナントの配置ポリシーを作成するには:**

1. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Placement Policy**に移動し、次に**追加**をクリックします。
2. **配置ポリシーの追加**ページで、次のパラメーターを設定します。
    a. 名前 - 配置ポリシーの名前を入力します
    b. サンプル式 - リストからサンプル式を選択します。これらの例は、配置ポリシーを構築するのに役立ちます。
    c. 式 - 以前のフィールドで選択したサンプル式に基づいて、このフィールドにブール式が入力されます。必要に応じてフィールド名を編集します。
3. **OK**をクリックします。

### クライアントネットワークを介したNetScalerインスタンスからバックエンドサーバーへのトラフィックの有効化

デフォルトでは、OpenStackオーケストレーションワークフローでは、NetScalerインスタンスはロードバランサーまたはクライアントネットワークと、メンバーまたはサーバーネットワークに動的にバインドされます。

特定の展開では、サーバーはクライアントネットワークを介しても到達可能であり、クライアントゲートウェイを介してルーティングできます。このような場合、NetScalerインスタンスはサーバーネットワークにバインドする必要はなく、クライアントネットワークにのみバインドする必要があります。

クライアントゲートウェイを介したトラフィックを構成するには、次の設定を実行します。

「**オーケストレーション** > **クラウドオーケストレーション** > **OpenStack** > **デプロイ設定**」に移動し、「**VIPネットワークのみをプロビジョニングし、VIPネットワーク経由でプールトラフィックをルーティングする**」オプションを選択します。

NetScaler Consoleは、そのネットワークにSNIPを追加することでNetScalerインスタンスをクライアントネットワークに構成し、さらにクライアントネットワークゲートウェイへのデフォルトルートを追加します。これにより、インスタンスはクライアントゲートウェイを介してサーバーに到達できるようになります。

### NetScaler SDXプラットフォームに展開されたNetScaler VPXデバイスの自動プロビジョニング

NetScaler ConsoleにNetScaler SDXプラットフォームを追加して、NetScaler Consoleがこのプラットフォーム上のインスタンスをオンデマンドでプロビジョニングできるようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NetScaler SDXプラットフォームに展開されたNetScalerインスタンスを自動プロビジョニングするには：**

1. NetScaler Console GUIで、**Infrastructure > Instances** \> **NetScaler SDX** に移動し、**Add** をクリックしてNetScaler SDXプラットフォームを追加します。
2. 「**オーケストレーション** \> **クラウドオーケストレーション** \> **OpenStack** \> **デプロイ設定**」に移動します。
3. 「**Management Network**」セクションで、自動プロビジョニングされたNetScaler SDXが接続されているOpenStack上の管理ネットワークを選択します。
   a. 「**Profile Name**」で、ドロップダウンリストからプロファイルを選択します。NetScaler Consoleは、このプロファイルに含まれるパスワードを使用して、新しく自動プロビジョニングされたNetScaler VPXインスタンスを構成します。
   b. 「**OK**」をクリックします。
4. OpenStackでNetScaler SDXプラットフォームをプロビジョニングするには、**Orchestration** \> **Cloud Orchestration** \> **OpenStack**\> **Service Package** に移動します。
   a. 「**Add**」をクリックして、新しいサービスパッケージを作成します。
   b. サービスパッケージの名前を入力します。
   c. 「**NetScaler Instance Allocation**」フィールドで、「**Dedicated**」を選択します。
   d. 「**NetScaler Instance Provisioning**」フィールドで「**Create Instance OnDemand**」を選択し、「**Auto Provision Platform**」フィールドで「**NetScaler SDX**」を選択します。
   e. デフォルトでは、NetScaler SDXプラットフォームにはNetScaler VPXインスタンスのみがプロビジョニングされます。
   f. 「**Continue**」をクリックします。
   g. 「**Auto Provision Settings**」セクションで、「**Resources**」プロパティを設定します。
      i. 「**Throughput**」フィールド。1000 Mbpsと入力します。
      ii. 「**NetScaler Version**」フィールド。リストから、NetScaler SDX platformに存在するNetScaler VPXイメージの適切なバージョンを選択します。
   h. 「**NetScaler SDX Platforms**」セクションで、「**Add**」をクリックしてSDXプラットフォームをサービスパッケージに追加します。
   i. 「**Continue**」をクリックします。
   j. 「**Configure OpenStack Tenants**」セクションで、「**Add**」をクリックしてテナントを追加します。「**New**」をクリックして新しいテナントを追加することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

k. 「**Done**」をクリックします。

5. LBaaS V2 API の実装は、Neutron LBaaS コマンドを介して実行されます。任意の Neutron クライアントに接続し、構成タスクを実行します。構成コマンドの実行方法の詳細については、「Configuring LBaaS V2 using Command Line」(/ja-jp/netscaler-application-delivery-management-software/current-release/orchestration/integrate-with-openstack-platform/openstack-configuring-lbaasv2-using-command-line.html)を参照してください。

### Horizon を使用して LBaaS V1 を構成する

OpenStack Horizon ポータルにログオンして、LBaaS プールを作成し、サブネットを選択できます。このプールのすべてのメンバーはサブネット内にあります。構成するには：

- 仮想 IP (VIP) アドレスを追加し、この VIP を作成したプールに割り当てます。
- このアクションは、コマンドラインまたは API を介して実行することもできます。
- サーバーの外部クライアントは、割り当てられた NetScaler でホストされているこの VIP アドレスに接続できます。
- NetScaler は、構成されたポート上のプールメンバーにすべてのリクエストを分散します。
- LBaaS プールメンバーは、選択したプールに追加されるロードバランスされたサーバーです。
- これらの各メンバーに重みとポートを割り当てます。

ヘルスモニターは、プールのすべてのメンバーのヘルスと良好な機能を監視するために使用されます。OpenStack で、遅延、タイムアウト、再試行制限、メソッド、URL パス、予期される HTTP 成功コードなどのパラメーターを定義して、ヘルス監視テンプレートを作成できます。モニターを作成した後、以前に作成したプールにモニターを関連付ける必要があります。

プールの作成方法、および OpenStack でのその他の LBaaS 構成タスクの詳細については、OpenStack ドキュメント を参照してください。

**重要**

LBaaS V1 は、OpenStack の Liberty リリースではサポートされていません。詳細については、OpenStack リリースノート を参照してください。

### コマンドラインを使用してLBaaS V2を構成する

LBaaS V2は、**Barbican**で管理される証明書、証明書バンドル（中間認証局を含む）、SNIサポート、および通常のロードバランシング機能によるSSLオフロードをサポートします。LBaaS V2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、構成タスクを実行するためのコマンドラインインターフェイスのみをサポートします。LBaaS V2 APIの実装は、Neutron LBaaSコマンドを通じて実行されます。

**注**

SSLオフロード機能が必要な場合は、証明書とキーを**Barbican**サービスにアップロードします。SSLオフロードがサポートされている場合は、ステップ1、2、3を実行します。そうでない場合は、ロードバランサー、リスナー、プール、およびメンバーを作成するために[ステップ4]から続行します。

1. 以下のコマンドを使用して、証明書を**Barbican**サービスにアップロードします。

```
barbican secret store --payload-content-type <content_type> --name
<certificate_name> --payload<certificate_location>
```

**例**:

```
barbican secret store --payload-content-type='text/plain' --
name='hp_server_certificate' --payload=" hp_server/tmp/
server_certificate"
```

2. 以下のコマンドを使用して、キーを**Barbican**サービスにアップロードします。

```
barbican secret store --payload-content-type <content_type> --name
<key_name> --payload<key_location>
```

**例**:

```
barbican secret store -- payload-content-type='text/plain' --
name='shp_server_key' --payload="hp-server/tmp/server_key"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

これら2つの**Barbican**コマンドを実行して証明書とキーをロードすると、Secret hrefフィールドに場所またはURLが提供されます。これは、OpenStackがインストールされているシステムに証明書とキーが保存されている場所です。これらのリンクをコピーし、ステップ3で**Barbican**サービスにコンテナを作成するときに、これらのリンクをパラメーターとして提供します。

3. 以下のコマンドを使用して、証明書とキーを保存するためのコンテナを**Barbican**サービスに作成します。

   コマンドでは、<certificate_url>を証明書をアップロードしたときにSecret hrefフィールドから取得したURLに置き換えます。同様に、<key_url>をキーをアップロードしたときにSecret hrefフィールドから取得したURLに置き換えます。

   ```
   barbican secret container create --name<container_name> --
   type<container_type> --secret<certificate_url> --secret<key_url>
   ```

   **例**:

   ```
   barbican secret container create --name='hp_container' --
   type='certificate' --secret="`certificate=http://localhost:9311/v1/
   secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --
   secret="private_key=http://localhost:9311/v1/secrets/
   1b9e1a93-2aeb-4101-8002-e52acab987b0`"
   ```

   ☐ コンテナのhref値をコピーします。ステップ6でリスナーを作成する際に、コンテナへのリンクを提供する必要があります。

4. OpenStackで環境変数を設定します。これらの変数は、OpenStackクライアントコマンドがOpenStackサービスと通信できるようにします。

   **例**:

   OS_PASSWORD-hp をエクスポート

   OS_AUTH_URL=`http://10.106.43.15:35357/v2.0/` をエクスポート

   OS_USERNAME=hp_user をエクスポートします

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OS_TENANT_NAME=hp をエクスポートします

OS_IDENTITY_API_VERSION=2.0 をエクスポートします。

BARBICAN_ENDPOINT="`http://10.106.43.15:9311/`" をエクスポートします。

**注**

他のコマンドを実行する前に、SSHセッションごとにこれらの変数を設定してください。OpenStack環境変数の詳細については、OpenStack環境変数を参照してください。

5. 次のコマンドを使用してロードバランサーを作成します。

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <subnet-name> --provider <netscaler>
```

**例**:

```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
```

ロードバランサーを作成(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-lb-create.png)

ロードバランサーが正常に作成されると、ステータスはPENDING_CREATEからACTIVEに変わります。

ロードバランサーのステータス変更(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-lb-create-status.png)

6. 次のコマンドを使用してリスナーを作成します。

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number> --default-tls-container-id<container_url>
```

**例**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
neutron lbaas-listener-create --name hp-lb-test-list  --loadbalancer
hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-
tls-container-id `http://10.106.43.15:9311/v1/containers/d688676f-
c256-4a0d-b84d-a310419dc0aa`
```

**注**

SSLオフロードサポートなしでリスナーを作成する場合は、コンテナに場所を指定せずに次のコマンドを実行します。

`neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

SSLオフロードなしでリスナーを作成(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-listener-create.png)

7. 次のコマンドを使用してプールを作成します。

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener
<listener-name> --protocol <protocol_type> --name <pool-name>
```

**例**:

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener
demolistener --protocol http --name demopool
```

プールを作成(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-pool-create.png)

8. 次のコマンドを使用してメンバーを作成します。

```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-
address of the web server> --protocol-port <port_number>  <pool-name>
```

**例**:

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --
protocol-port 80 hp-lb-test-pool
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メンバーを作成(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-member-create.png)

### NetScaler ConsoleでのOpenStackアプリケーションの監視

テナントは、OpenStackの資格情報を使用してNetScaler Consoleにログインし、OpenStackから作成されたVIPとプールをどのブラウザからでも監視できます。URLは次の形式である必要があります。

```
http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html
```

ここで、`mas-ip-address`はOpenStackに登録されているNetScaler ConsoleのIPアドレスです。

**注**

- OpenStack VIPは、NetScaler Consoleの仮想サーバーに対応します。
- OpenStackプールは、NetScaler Consoleのサービスグループに対応します。
- OpenStackプールメンバーは、NetScaler Consoleのサービスグループメンバーに対応します。

## レイヤー7コンテンツスイッチングの構成

NetScaler ConsoleはOpenStackと連携して、NetScalerインスタンス上でレイヤー7 (L7) スイッチングまたはコンテンツベースのスイッチング機能を構成します。コンテンツスイッチングは、特定の種類の要求を特定のサーバーに転送できる点で、単純なロードバランシングとは異なります。NetScalerインスタンスをプロバイダーとしてOpenStackでL7構成が作成されると、NetScaler ConsoleはNetScalerインスタンスを割り当て、L7構成に対応するコンテンツスイッチングおよびレスポンダー構成を展開します。NetScalerインスタンスは、要求のアプリケーション層の特性に基づいて、ユーザー要求を分散およびロードバランシングできます。

OpenStackのレイヤー7 (L7) ロードバランシング機能は、ロードバランシングとコンテンツスイッチングを組み合わせて、特定の種類のコンテンツの最適化された配信を提供します。これにより、コンテンツに適用可能なポリシーのみを実行することで、ロードバランサーのパフォーマンスが向上します。レイヤー7ロードバランシングは、アプリケーションインフラストラクチャの効率向上も促進します。タイプ、URI、またはデータに基づいてコンテンツを分離する機能により、アプリケーションインフラストラクチャにおける物理リソースのより良い割り当てが可能になります。たとえば、`http://example-sports.com/about-us` を閲覧するエンドユーザーには、会社とサービスに関するコンテンツをホストするサーバープールがサービスを提供し、`http://`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`example-sports.com/shopping-cart-football` を閲覧するユーザーには、オンライン購入を可能にする別のサーバープールがサービスを提供します。

L7スイッチングでは、ロードバランサーは、ユーザーからのHTTP要求を受け入れ、それらの要求をアプリケーションサーバーに分散するコンテンツスイッチング仮想サーバーとして実装されます。L7スイッチングまたはコンテンツスイッチングにより、さまざまなバックエンドサービス（たとえば、Webアプリケーション、Webサービスポータル、Webメールだけでなく、モバイル管理、異なる言語のコンテンツなど）にアクセスするための単一のエントリポイントを持つことができます。つまり、ユーザーに提供するすべてのサービスに対して1つのパブリックIPアドレスを提供できます。

下位レベルのロードバランシングとは異なり、レイヤー7スイッチングでは、プール内のすべてのサーバーが同じコンテンツを持つ必要はありません。L7スイッチングを使用するロードバランサー構成では、異なるプールからのアプリケーションサーバーまたはバックエンドサーバーが異なるコンテンツを持つことを想定しています。L7スイッチは、URI、ホスト、HTTPヘッダー、またはアプリケーションメッセージ内のその他のものに基づいて要求を転送できます。アプリケーションサーバーは、本質的に特定の種類のコンテンツを提供します。たとえば、あるサーバーは画像のみを提供し、別のサーバーはPHPやASPなどのサーバーサイドスクリプト言語を実行し、さらに別のサーバーはHTML、CSS、JavaScriptなどの静的コンテンツを提供できます。

**L7ルール**

トラフィックを評価するために、ルールには次の属性が定義されており、それらはルールで定義された値と比較されます。

- ホスト名: HTTP要求のホスト名は、ルール内の値パラメーターと比較されます。例: 「www.example-sports.com」
- パス: HTTP URIのパス部分は、ルール内の値パラメーターと比較されます。例: 「www.example-sports.com/shopping-cart/football_pump.html」
- file_type: URIの最後の部分は、ルール内の値パラメーターと比較されます。例: txt、html、jpg、PNG、xlsなど。
- ヘッダー: キーパラメーターで定義されたヘッダーは、ルール内の値パラメーターと比較されます。
- Cookie: キーパラメーターで指定されたCookieは、ルール内の値パラメーターと比較されます。Cookieリクエストヘッダーフィールドの値には、そのURLに保存されている情報の名と値のペアが含まれます。一般的な構文は次のとおりです - Cookie: name=value。たとえば、「stores」という名前のCookieで、「football-」で始まる値を探すルールは次のようになります: type = Cookie, compare_type=StartsWith, key = stores value = football-。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 比較タイプ

トラフィックを評価する際、L7ポリシーはルールで定義された属性に対して次の式を比較します。

- 正規表現: Perlタイプの正規表現マッチング
- starts_with: 文字列が次で始まる
- ends_with: 文字列が次で終わる
- contains: 文字列が次を含む
- equal_to: 文字列が次と等しい

**注**

ホスト名、パス、ヘッダー、およびCookie属性はすべての比較タイプをサポートしますが、file_type属性は正規表現とequal_toのみをサポートします。

### L7ポリシー

L7ポリシーは、受信HTTPトラフィックを処理し、ポリシーで定義されたすべてのルールが一致した場合に「true」の値を返します。

任意のL7ポリシーでは、すべてのルールが論理的にAND演算子で結合されます。ポリシーが「true」の値を返すためには、リクエストがすべてのルールに一致する必要があります。ロードバランサーが実行するアクションは、ポリシーによって返される値に基づいています。ルール間の論理OR演算を実現するために、同じアクションを持つ2番目のポリシーを作成できます。

たとえば、受信HTTPリクエストに「EXAMPLE-SPORTS」、「SPORTS-FOOTBALL」、または「EXAMPLE-FOOTBALL」という単語が含まれるポリシーを作成し、ロードバランサーがこれらのリクエストをExample-sports eコマース企業のサーバープールに転送して、要求されたコンテンツを提供するという適切なアクションを実行するようにできます。同じアクションを実行するが、「example-sports」、「example-sports-football」、または「example-football」に一致する別のポリシーを作成できます。ユーザーがこれら6つのキーワードのいずれかを含むHTTPリクエストを送信すると、ロードバランサーはリクエストをExample-Sportsサーバーに転送します。

ポリシーで定義されたルールに応じて、L7ポリシーは次のいずれかのアクションを実行できます。

- プールにリダイレクト - L7ポリシーに関連付けられたルールによって識別されるアプリケーションサーバープールにリクエストを転送します。つまり、ドメイン名に基づいて特定のロードバランサープールにリクエストを誘導するアプリケーションルールを作成できます。たとえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ば、example-football.comへの一部のリクエストをpool_1に、example-sports-online_purchase.comへの他のリクエストをpool_2に誘導するルールを作成できます。

- URLにリダイレクト - クライアントにリダイレクトHTTP応答を送信し、そのロケーション応答ヘッダーに新しいロケーションを含めます。ブラウザはアドレスバーを新しいロケーションで更新し、新しいリクエストを発行します。ユースケースは多数あります。たとえば、ウェブサイトのアドレスが変更された場合、リクエストを破棄する代わりに新しいアドレスにリダイレクトできます。または、ウェブサイトのメンテナンス中に、ユーザーを読み取り専用サイトにリダイレクトできます。
- 拒否 - リクエストを拒否し、それ以上のアクションを実行しません。たとえば、制限されたウェブページへのユーザーのアクセスを拒否するために、401 Unauthorized応答を返すことができます。

コンテンツスイッチング構成は、コンテンツスイッチング仮想サーバー、ロードバランシング仮想サーバーとサービスからなるロードバランシング設定、およびコンテンツスイッチングポリシーで構成されます。コンテンツスイッチング仮想サーバーとポリシーを作成した後、各ポリシーをコンテンツスイッチング仮想サーバーにバインドします。ポリシーをコンテンツスイッチング仮想サーバーにバインドするときに、ターゲットロードバランシング仮想サーバーを指定します。リクエストがコンテンツスイッチング仮想サーバーに到達すると、仮想サーバーは関連付けられたコンテンツスイッチングポリシーをそのリクエストに適用します。ポリシーの優先順位は、コンテンツスイッチング仮想サーバーにバインドされたポリシーが評価される順序を定義します。

リスナーIDを持つ任意のプールは、トラフィックが転送される仮想サーバーのデフォルトプールとして割り当てることができます。プールはリスナーと緩やかに結合されており、L7ポリシーの実装を通じてのみリスナーと関連付けられます。プールは、必ずしもリスナーに紐付けられることなく、ロードバランサーの直下に直接作成することもできます。そのような場合、プールは「pending_create」状態として作成されます。L7ポリシーはリスナーと密接に結合されているため、プールが「active」になりトラフィック要求の受信を開始するには、プールIDを含むL7ポリシーを作成し、実装する必要があります。

1つのプールは複数のL7ポリシーによってサービスを提供できますが、少なくとも1つのポリシーがアタッチされている限り、「active」状態を維持します。最後のポリシーが削除されると、別のポリシーが作成されて関連付けられるまで、プールは「pending_create」状態に戻ります。プール自体が削除された場合、本来受信するはずだったすべてのHTTPリクエストはデフォルトプールにリダイレクトされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### OPENSTACK L7ポリシーとNETSCALERエンティティ間のマッピング

| OpenStack | NetScalerエンティティ | 説明 |
| --- | --- | --- |
| アクションがREDIRECT_TO_POOLのL7ポリシー | コンテンツスイッチングポリシー > コンテンツスイッチングアクション | NetScaler Consoleは、コンテンツスイッチング仮想サーバーにバインドされ、コンテンツの取得とユーザーへの提示のためのアプリケーションサーバーのターゲットプールを指定するコンテンツスイッチングアクションに関連付けられたコンテンツスイッチングポリシーを作成します。 |
| アクションがREDIRECT_TO_URLのL7ポリシー | レスポンダーポリシー > レスポンダーアクション | NetScaler Consoleは、コンテンツスイッチング仮想サーバーにバインドされ、ユーザーに提示されるターゲットURLを指定するレスポンダーアクションに関連付けられたレスポンダーポリシーを作成します。 |
| アクションがREJECTのL7ポリシー | レスポンダーポリシー > リクエストを破棄 | NetScaler Consoleは、コンテンツスイッチング仮想サーバーにバインドされ、リクエストを破棄するレスポンダーアクションに関連付けられたレスポンダーポリシーを作成します。 |

「true」と評価されるL7ポリシーのアクションが「create_pending」状態のプールにトラフィックをリダイレクトする場合、NetScaler Consoleは指定されたプールとロードバランシング仮想サーバーを実装します。NetScaler ConsoleはL7ポリシーからコンテンツスイッチングポリシーを作成し、対応するコンテンツスイッチングアクションを使用して、そのプールに関連付けられたロードバランシング仮想サーバーにリクエストをリダイレクトします。2番目のL7ポリシーが同じプールにリダイレクトする場合、NetScaler Consoleはコンテンツスイッチングポリシーとコンテンツスイッチングアクションを作成し、トラフィックをそのプールに関連付けられた既存のロードバランシング仮想サーバーにリダイレクトします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ポリシーの配置

OpenStackにおけるL7ポリシーの評価は、その優先順位によって決定されます。OpenStackでは、デフォルトで、ポリシーは作成された順序で優先順位が割り当てられます。最初に作成されたポリシーには「1」が割り当てられ、その後作成されたポリシーには連番が割り当てられます。ただし、ポリシーの優先順位を変更し、異なる優先順位を割り当てることもできます。ポリシーは常に優先順位の順に評価されます。特定のリクエストに一致する最初のポリシーが常に最初に実行されます。

ポリシーを作成する際は、以下の点に注意してください。

- 新しいポリシーに既存のポリシーと同じ優先順位を割り当てると、新しいポリシーがその優先順位を取得します。既存のポリシーの優先順位は下がります。必要に応じて、ポリシーが評価される順序を維持するために、他のポリシーの優先順位も下げられます。
- 位置を指定せずに新しいポリシーを作成した場合、新しいポリシーはリストの末尾に追加されます。
- 新しいポリシーを作成し、リストに既に存在するポリシーの数よりも大きい位置を割り当てた場合、新しいポリシーはリストの末尾に追加されます。つまり、新しいポリシーは常に次に利用可能な優先順位を取得します。たとえば、優先順位1、2、3の3つのポリシーA、B、Cがあり、優先順位8のポリシーを作成した場合、新しいポリシーの優先順位は4になります。
- リストにポリシーを追加したり、リストからポリシーを削除したりすると、ポリシーの位置の値は番号をスキップせずに1から再順序付けされます。たとえば、ポリシーA、B、C、Dが位置値1、2、3、4を持っている場合、リストからポリシーBを削除すると、ポリシーCが2番目の位置になり、ポリシーDが3番目の位置になります。

NetScaler Consoleでは、常に優先順位1の`csvserver`に関連付けられたデフォルトポリシーがあります。このデフォルトポリシーは、`lbvserver`が任意の時点で処理するTCP接続の数を指定します。したがって、NetScalerで対応するレスポンダーポリシーとコンテンツスイッチングポリシーが作成される場合、それらは常に、対応するL7ポリシーの優先順位よりも1大きい優先順位が割り当てられます。たとえば、優先順位1のL7ポリシーが評価され、優先順位2のコンテンツスイッチングポリシーが作成される場合です。同様に、優先順位2のL7ポリシーが評価され、優先順位3のレスポンダーポリシーが作成される場合です。

OpenStackでは、「reject」または「redirect_to_url」ポリシーが最初に評価され、次に「redirect_to_pool」ポリシーが評価されます。NetScalerインスタンスでは、レスポンダーポリシーが常に最初に評価され、リクエストを破棄するか、リダイレクトされたWebアドレスをユーザーに提示し、コンテンツスイッチングポリシーが最後に評価されます。この評価順序は、コンテンツスイッチングポリシーとレスポンダーポリシーが相互に排他的である場合、通常は競合を引き起こしません。つまり、2つのL7ポリシーが同一の式を持つべきではありません。このような

© 1997–2026 Citrix Systems, Inc. All rights reserved.

競合を避けるために、導出された式がレスポンダーポリシーとコンテンツスイッチングポリシーに追加されます。たとえば、「sports-football.com」へのすべてのリクエストを拒否する式と、「example-sports-football.com」へのリクエストを許可する別の式を作成します。リクエストを拒否するすべてのレスポンダーポリシーが評価リストの最上位に配置され、その後にWebダイレクト用のレスポンダーポリシー、その後にコンテンツスイッチングポリシーが続くようにL7ポリシーを作成します。

NetScaler Consoleでは、常に優先順位1の`csvserver`に関連付けられたデフォルトポリシーがあります。このデフォルトポリシーは、`lbvserver`が任意の時点で処理するTCP接続の数を指定します。したがって、NetScalerで対応するレスポンダーポリシーとコンテンツスイッチングポリシーが作成される場合、それらは常に、対応するL7ポリシーの優先順位よりも1大きい優先順位が割り当てられます。たとえば、優先順位1のL7ポリシーが評価され、優先順位2のコンテンツスイッチングポリシーが作成される場合です。同様に、優先順位2のL7ポリシーが評価され、優先順位3のレスポンダーポリシーが作成される場合です。

OpenStackでは、「reject」または「redirect_to_url」ポリシーが最初に評価され、次に「redirect_to_pool」ポリシーが評価されます。NetScalerでは、レスポンダーポリシーが常に最初に評価され、リクエストを破棄するか、リダイレクトされたWebアドレスをユーザーに提示し、コンテンツスイッチングポリシーが最後に評価されます。この評価順序は、コンテンツスイッチングポリシーとレスポンダーポリシーが相互に排他的である場合、通常は競合を引き起こしません。つまり、2つのL7ポリシーが類似の式を持つことはありません。このような競合を避けるために、類似の導出された式がレスポンダーポリシーとコンテンツスイッチングポリシーに追加されます。たとえば、「sports-football.com」へのすべてのリクエストを拒否する式と、「example-sports-football.com」へのリクエストを許可する別の式を作成します。リクエストを拒否するすべてのレスポンダーポリシーが評価リストの最上位に配置され、その後にWebダイレクト用のレスポンダーポリシー、その後にコンテンツスイッチングポリシーが続くようにL7ポリシーを作成します。

#### 構成タスク

L7ポリシーとアクションの実装は、Neutron LBaaSコマンドを通じて実行されます。

OpenStackで環境変数を設定し、ロードバランサー（例：LB1）を作成します。ロードバランサーが正常に作成されたら、リスナーとプール（例：L1、P1、P2）を作成し、プールにメンバーとモニターを追加します。たとえば、P1はL1のデフォルトプールであり、P2はLB1に紐付けられ、アプリケーションサーバーを管理するプールです。

コマンドラインを使用してLBaaS V2を構成する方法の詳細については、コマンドラインを使用したLBaaS V2の構成を参照してください。

以下のコマンドは、ポリシーを作成し、特定のアクションを定義します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リクエストを破棄するL7ポリシーを作成する

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action&lt;action-name>
```

**例**:

neutron lbaas-l7policy-create --name policy11 --action REJECT --listener L1

上記のコマンドは、リクエストを拒否するために、応答ポリシーであるpolicy11を作成し、コンテンツスイッチングサーバーにバインドします。このポリシーに対してルールが作成されていないため、ポリシーは「false」と評価され、リクエストは拒否されます。
リクエストを特定のURLにリダイレクトするL7ポリシーを作成する

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-url &lt;redirect-
url>
```

**例**:

neutron lbaas-l7policy-create --name policy12 --action REDIRECT_TO_URL --listener admin-list1 --redirect-url `http://example-sports/about-us.html`

上記のコマンドは、リクエストをURLにリダイレクトする応答アクションを作成し、アクションを含む応答ポリシーを作成し、このポリシーをコンテンツスイッチング仮想サーバーにバインドします。

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
value &lt;value-string> &lt;L7 policy name>



neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
&lt;value-string> &lt;L7 policy name>
```

上記の2つのルールは、AND演算子で接続して、応答ポリシーの式を導き出すことができます。
リクエストをプールにリダイレクトするL7ポリシーを作成する

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-pool &lt;redirect-
pool>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**例**:

neutron lbaas-l7policy-create --name policy13 --action REDIRECT_TO_POOL --listener admin-list1 --redirect-pool admin-pool2

これが最初のL7ポリシーである場合、上記のコマンドはLB1とともにP2を実装し、コンテンツスイッチングリダイレクトアクションを作成して、リクエストをLB1にリダイレクトします。P2がすでに存在する場合、コマンドはコンテンツスイッチングリダイレクトアクションを作成して、リクエストをLB1にリダイレクトします。

### OpenStackでのNetScaler VPXインスタンスの手動プロビジョニング

一部のエンタープライズネットワークでは、セキュリティ上の理由から、NetScaler VPXインスタンスがNetScalerライセンスサーバーに接続してライセンスを自動的にダウンロードできません。このようなシナリオでは、OpenStackプラットフォームにNetScaler VPXインスタンスを手動で展開する必要があります。Citrixから受け取ったライセンスアクセスコードを使用して、適切なNetScaler VPXライセンスをダウンロードし、ローカルシステムに保存してください。

**OpenStackにNetScaler VPXインスタンスを手動でプロビジョニングするには：**

1. NetScalerドライバーソフトウェアをインストールし、NetScaler ConsoleをOpenStackに登録します

    a. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** に移動します。

    b. **Configure OpenStack Settings** をクリックします。**Configure OpenStack Settings** ページで、NetScaler ConsoleでOpenStackを構成するためのパラメーターを設定できます。ここには、**Default** と **Customized** の2つのオプションがあります。

    c. OpenStackサービスがデフォルトポートで実行されている場合は、**Default** を選択します。

2. **Orchestration** \> **Cloud Orchestration** \> **OpenStack** に移動し、**Deployment Settings** をクリックします。

    a. **Management Network** - 自動プロビジョニングされたNetScaler VPXが接続されるOpenStack上の管理ネットワークを選択します。

    b. **Profile Name** - ドロップダウンリストからプロファイルを選択します。NetScaler Consoleは、このプロファイルに含まれるパスワードを使用して、新しく自動プロビジョニングされたNetScaler VPXインスタンスを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Glance内のNetScaler VPXイメージ - NetScaler VPXインスタンスの作成に使用される、OpenStack Glanceで利用可能なNetScaler VPXイメージを選択します。ドロップダウンリストには、OpenStack Glanceに存在するイメージのみが表示されます。

3. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Service Packages** に移動し、**Add** をクリックします。
4. **Service Package** ページで、次のパラメーターを指定します。

   a. **Name** - サービスパッケージの名前。たとえば、SVC-PKG-GOLDと入力します。

   b. **NetScalerインスタンス割り当て** - サービスパッケージで定義されているインスタンス割り当てのタイプとして、**Dedicated** または **Partitioned** を選択します。

   c. **NetScalerインスタンスのプロビジョニング** - 設定中にNetScalerインスタンスを作成するには、「**Create Instance OnDemand**」を選択します。

   d. **自動プロビジョニングプラットフォーム** - 「**OpenStack Compute**」を選択します。デフォルトでは、インスタンスタイプとしてNetScaler VPXが選択されます。

   e. **OpenStackテナント/配置ポリシーの割り当て** - セクションの「OpenStack Tenants」の下で、「**Add**」をクリックし、テナントを選択します。

   f. 「**Continue**」をクリックし、次に「**Done**」をクリックします。

5. 「**System**」 \> 「**System Administration**」 \> 「**Change System Settings**」に移動し、ドロップダウンリストから「**http**」を選択します。
6. 「**Infrastructure > Instances > NetScaler VPX**」に移動します。
7. 「**NetScaler VPX**」ページで、「**Admin**」ドロップダウンリストをクリックし、「**Provision Device**」を選択します。

   NetScaler VPXページ(/en-us/netscaler-application-delivery-management-software/media/orchestration-openstack-manual-provision-device.png)

   a. 「**Device Provisioning**」ページで、デバイスの名前を入力し、前の手順で作成したサービスパッケージを選択します。

   b. 「**OK**」をクリックします。

8. 「**Orchestration**」 \> 「**Cloud Orchestration**」 \> 「**OpenStack**」 \> 「**Requests**」タブに移動します。リクエストを選択し、「**Tasks**」をクリックしてタスクを表示します。タスクのステータスが「**Finished**」に変わると、NetScaler VPXがNetScaler Consoleにプロビジョニングされたことを意味します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 「**Infrastructure > Instances**」 \> 「**NetScaler VPX**」に移動し、NetScaler VPXインスタンスがNetScaler VPXページに表示されていることを確認します。
10. NetScaler VPXインスタンスをクリックします。ブラウザウィンドウでNetScaler VPXインスタンスが開いたら、インスタンスにログオンします。「**Configuration**」 \> 「**System**」 \> 「**Licenses**」に移動し、新しいライセンスを手動で追加します。新しいライセンスの追加方法の詳細については、「NetScaler Licensing Overview」を参照してください。
11. NetScaler VPXインスタンスを再起動します。

    NetScaler VPXを再起動(/en-us/netscaler-application-delivery-management-software/media/orchestration-openstack-ns-reboot.jpg)
12. 数分後、OpenStackにログインし、**System** \> **Instances** で、NetScaler VPXインスタンスがOpenStackにデプロイされていることを確認できます。
13. LBaaS V2 APIの実装は、Neutron LBaaSコマンドを通じて実行されます。任意のNeutronクライアントに接続し、構成タスクを実行します。構成コマンドの実行方法の詳細については、「コマンドラインを使用したLBaaS V2の構成」を参照してください。

### OpenStack上でのStyleBookを使用したNetScaler VPXインスタンスのプロビジョニング

OpenStackオーケストレーションワークフローでは、NetScaler Consoleは現在、`os-cs-lb-mon` StyleBookを使用して、OpenStackテナントに割り当てられたNetScalerインスタンスにLBaaS構成を展開します。OpenStackユーザーによって作成された各ロードバランサーに対して、設定パックが作成されます。

OpenStackワークフローでStyleBookを構成に使用すると、次の利点があります。

- すべての構成オブジェクトを表示することで、視覚化が向上します。
- ロールバックによる信頼性。
- さまざまなNetScalerインスタンスタイプ（NetScaler HA、パーティション、VPX、CPX、MPXなど）のサポート。
- 独自のStyleBookを使用してOpenStackテナントの構成を展開することによるカスタマイズ。

NetScaler Console管理者として、**Applications** > **Configurations** に移動して、NetScalerインスタンスに展開されている設定パックを表示します。 次のタスクを実行できます。

- ロードバランサーに展開されている`os-cs-lb-mon`設定パックを表示するためにスクロールします。
- `os-cs-lb-mon` StyleBookパネルで**View Definition**をクリックして、インスタンスに展開されている構成を確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **View Object**をクリックして、インスタンスに展開されているNetScalerオブジェクトまたはエンティティのリストを表示します。

### StyleBookを使用してインスタンスをプロビジョニングする前の注意点

NetScaler Console 12.1 build 49.23以降、OpenStackオーケストレーションワークフローのアーキテクチャが更新されました。このワークフローでは、NetScaler Console StyleBookを使用してNetScalerインスタンスを構成するようになりました。バージョン12.0またはバージョン12.1 build 48.18からNetScaler Console 12.1 build 49.23にアップグレードする場合は、次の移行スクリプトを実行する必要があります。

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

- 移行スクリプトを実行すると、既存のOpenStack構成に対応する`os-cs-lb-mon` StyleBookの設定パックが作成されます。
- これらの以前のビルドからOpenStack構成を展開していた場合、この移行スクリプトの実行は必須です。
- バージョン 12.1 ビルド 49.23 からの移行スクリプトを実行した後にのみ、`os-cs-lb-mon` StyleBook を使用してインスタンスに新しい構成を展開できます。
- 移行スクリプトが実行されるまで、OpenStack から試行されたすべての構成は失敗します。

**注**

- 移行スクリプトを実行すると、NetScaler Console の以前のビルドにダウングレードすることはできません。
- OpenStack LBaaS V2 用の NetScaler ドライバーを最新バージョンにアップグレードしていることを確認してください。最新の NetScaler Console 13.0 ビルドとともに提供される NetScaler バンドルファイルを使用してください。

LBaaS V2 API の実装は、Neutron LBaaS コマンドを介して実行されます。任意の Neutron クライアントに接続し、構成タスクを実行します。構成コマンドの実行方法の詳細については、「Configuring LBaaS V2 using Command Line」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### OpenStack環境におけるVPXチェックイン/チェックアウトライセンスおよびプールライセンスのサポート

OpenStackオーケストレーションワークフローでは、**OpenStack Compute**を含むサービスパッケージを選択すると、NetScaler Consoleは必要に応じてNetScaler VPXインスタンスを作成します。現在、NetScaler Consoleのオーケストレーション機能のサービスパッケージページが強化され、必要に応じて作成されるNetScaler VPXインスタンスにインストールする必要があるライセンスを提供するようになりました。提供されるライセンスは、VPXチェックイン/チェックアウトライセンスまたはプールライセンスのいずれかです。

この機能を使用するには、まずNetScaler Consoleにライセンスをアップロードし、その後、OpenStack Computeを使用するサービスパッケージを作成する必要があります。

- チェックイン/チェックアウトライセンスの場合、利用可能なさまざまなライセンスの中からインストールするライセンスを選択できます。

  

- プールライセンスの場合、インストールする帯域幅とライセンスエディションの両方を選択できます。

  

NetScaler ConsoleをプロバイダーとしてNetScaler最初のロードバランサーを展開するたびに、NetScaler ConsoleはNetScaler VPXインスタンスを作成し、サービスパッケージで指定されたライセンスを新しく作成されたインスタンスにインストールします。

また、既存のロードバランシングインスタンスを削除すると、そのインスタンスは不要になります。インスタンスは廃止され、ライセンスはNetScaler Consoleに返却されます。これにより、NetScaler Consoleで利用可能なライセンスを最適に利用できます。

**注**

NetScaler Consoleが高可用性モードで展開されている場合、ライセンスは現在アクティブな、またはプライマリのNetScaler ConsoleであるMAS-HA-1にアップロードされていると見なされます。最初の要求を展開し、NetScaler ConsoleがNetScaler VPXインスタンスを作成すると、インスタンスはMAS-HA-1から必要なライセンスをチェックアウトします。後で、ライセンスを持たないセカンダリのNetScaler ConsoleであるMAS-HA-2が現在アクティブであると仮定します。NetScaler VPXインスタンスはMAS-HA-2からライセンスをチェックアウトできず、そのため、新しいユーザーのためにインスタンスを作成できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このような場合は、MAS-HA-1が稼働しており、現在のプライマリノードであることを確認してください。つまり、NetScaler ConsoleをMAS-HA-2からMAS-HA-1に手動でフェイルオーバーします。その後、OpenStackから構成を再試行する必要があり、インスタンスは適切なライセンスで再作成されます。NetScaler Consoleの高可用性展開におけるライセンスサポートの詳細については、高可用性を参照してください。

### 管理パーティションの共有VLANサポート

プライベートネットワークから接続するテナントの場合、NetScaler Consoleは分離ポリシーをサポートしており、各テナントが専用のパーティション、専用のVLAN、専用のサーバーを持つことができます。パブリックネットワークから接続するテナントの場合、専用VLANでは、使用するIPアドレスが多すぎることになります。共有VLANは、各パーティションに1つの仮想IPアドレスを作成することでこの問題を回避し、単一のIPサブネットを作成します。

テナントがVIPまたはリスナーを構成すると、そのテナントのためにNetScalerデバイスに管理パーティションが作成されます。作成されたその管理パーティションに、すべてのロードバランサー構成がプッシュされます。テナントがロードバランサーを作成するために共有ネットワークまたは外部ネットワークを使用している場合、そのネットワークのVLANが追加され、共有機能が有効になります。別のテナントが同じ共有ネットワークを使用してロードバランサーを作成する場合、VLANはNetScalerに再度追加されませんが、そのVLANは2番目のパーティションにもバインドされます。したがって、同じ共有ネットワークを使用するすべてのテナントは、同じVLANにバインドされたパーティションを取得します。

NetScaler Consoleは仮想宛先MACアドレスをサポートしています。テナントがVLANを共有する場合、NetScaler Consoleは、NetScalerデバイス上のパーティションに異なるMACアドレスを割り当てます。これにより、VLANをパーティション間、またはすべてのテナントとすべてのトラフィックドメイン間で共有できます。

#### NetScalerインスタンスからの共有VLANの構成

1. NetScalerインスタンスで、**Configuration** \> **System** \> **Network** \> **VLANs** に移動し、VLANプロファイルを選択し、**Edit** をクリックしてパーティション共有パラメーターを設定します。
2. **Configure VLAN** ページで、**Partitions Sharing** チェックボックスを選択します。
3. **OK** をクリックします。

#### OpenStack Orchestrationからの共有VLANの構成

1. OpenStackで、**Admin** \> **System** \> **Networks** に移動し、次に **Create Network** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Create Network** で、次のパラメーターを設定します。

    a. 名前 - ネットワークの名前を入力します

    b. プロジェクト - ドロップダウンリストからプロジェクトを選択します

    c. プロバイダーネットワークタイプ - ドロップダウンリストから**VLAN**を選択します。これにより、仮想ネットワークがVLANとして確立されることが定義されます。

    d. 物理ネットワーク - ここではデフォルトの物理ネットワークが選択されています。これを編集できます。

    e. 管理状態 - デフォルトでは、ネットワークの管理状態はUPです。

    f. **共有**および**外部**ネットワークを選択して、VLANが共有され、外部ネットワークを使用していることを定義します。

3. **ネットワークの作成**をクリックします。

    ネットワークの作成(/en-us/netscaler-application-delivery-management-software/media/shared-vlan-openstack.jpg)

## トライアルライセンスのワークフロー

OpenStackオーケストレーションを使用してNetScaler VPXインスタンスを自動プロビジョニングする際、NetScaler ConsoleはOpenStack Computeを使用してNetScaler VPXインスタンスを起動します。新しくプロビジョニングされたNetScaler VPXインスタンスは、セットアップ中にCitrixライセンスポータルに接続し、ライセンスアクセスコードを使用してライセンスファイルを自動的にダウンロードしてインストールします。

### トライアルライセンス

テクニカルサポートスタッフは、現場でNetScaler ConsoleおよびNetScaler VPXデバイスをインストールする際にトライアルライセンスを使用します。NetScaler VPXのトライアルライセンスまたは評価ライセンスは90日間有効です。複数のNetScalerを評価する必要がある場合、または90日を超えてテストを延長する必要がある場合は、新しい評価ライセンスを要求する必要があります。NetScaler Consoleは、トライアルライセンスファイルの自動インストールではなく、代替ソリューションを提供します。ライセンスファイルを手動でダウンロードし、NetScaler VPXにインストールして、インスタンスのインストールを完了できます。

NetScaler VPXがインターネットに接続できない場合は、NetScaler ConsoleをCitrixライセンスポータル用のプロキシサーバーとして機能するように構成し、ライセンスファイルをインストールします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トライアルライセンスを持つNetScaler VPXインスタンスは、NetScaler ConsoleとHTTPのみで通信できます。NetScaler ConsoleでHTTP通信を構成するには、**System** \> **System Administration** に移動し、**Change System Settings** をクリックします。ドロップダウンリストから **http** を選択して通信方法を設定し、**OK** をクリックします。

システム設定の変更(/en-us/netscaler-application-delivery-management-software/media/trial-licensing-system-settings.jpg)

## OpenStack Heatサービスとの統合

OpenStack Neutron LBaaSは、アプリケーション向けに、ロードバランシング、SSLオフロード、コンテンツスイッチングなどのコアロードバランシングサービスを可能にします。LBaaSはREST APIを介して管理され、APIによりテナントはRESTコールを行ってLBaaSオブジェクトを作成、更新、削除できます。LBaaSはロードバランシングサービスを提供するため、オーケストレーションプロセス中にNetScalerのより高度な機能を使用することはできません。NetScaler Heatプラグインはこの制限を克服します。

### Heatオーケストレーションサービス

OpenStack Heatオーケストレーションサービスは、テンプレートに基づいて複雑なクラウドアプリケーションの展開を可能にします。Heatオーケストレーションテンプレート（HOT）は、人間が読み書きでき、バージョン管理ツールで管理できるテキストファイルでクラウドアプリケーションのインフラストラクチャを記述します。これらのテンプレートの作成には、構造化言語であるYAMLが使用されます。HOTテンプレートを使用すると、ほとんどのOpenStackリソースタイプを作成し、その中で定義されているリソース間の関係を指定できます。NetScaler Heatプラグインを使用すると、任意のNetScalerインスタンスで高度なNetScaler機能を構成できます。

### NetScaler StyleBooks

NetScaler Console StyleBooksは、NetScaler機能を作成および構成するために使用できます。Heatテンプレートと同様に、StyleBooksもYAMLで記述されています。機能ごとに個別のStyleBooksを作成でき、単一のStyleBooksを使用して複数のNetScalerインスタンスに構成を展開できます。

NetScalerとOpenStackの統合中、NetScaler ConsoleはすべてのNetScaler Console StyleBooksをHeatサービスのリソースとして公開します。これには、NetScaler Consoleに同梱されているStyleBooksと、ユーザーが後で作成したStyleBooksの両方が含まれます。Heatテンプレートを使用すると、これらのStyleBooksリソースを使用してNetScalerの高度な機能を構成できます。

### Heatを使用してNetScalerインスタンスを構成するワークフロー

以下のフローチャートは、Heatスタックを展開するためのワークフローを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Heatを使用してNetScalerインスタンスを構成するワークフローの図(/en-us/netscaler-application-delivery-management-software/media/openstack-heat-integration-workflow-kopis-console.png)

クラウド管理者として、以下のタスクを実行します。

**OpenStackでHeatサービスを構成するには：**

1. OpenStack用NetScalerバンドルをダウンロードする

   OpenStackにNetScalerバンドルをインストールします。NetScaler Consoleで、**Downloads**に移動し、NetScalerドライバーバンドルをダウンロードし、バンドルを解凍し、バンドル内のHeatフォルダーの内容をOpenStackのHeatエンジンリソースディレクトリにコピーします。ディレクトリパスは次のとおりです。 /opt/stack/heat/heat/engine/resources/netscaler_resources

2. heat.confファイルに「netscaler_plugin」セクションを作成し、そのセクションで以下のパラメーターを更新します。

   a. 通信がHTTPの場合、パラメータは次のように更新されます。

      NMAS_BASE_URI=<`http://10.146.103.45:80`>

      NMAS_USERNAME=<openstack_driver_username>

      NMAS_PASSWORD=<openstack_driver_password>

   b. 通信がHTTPSの場合、パラメータは次のように更新されます。

      NMAS_BASE_URI=`https://common_name_used_in_certificate`

      NMAS_USERNAME=\<openstack_driver_username

      NMAS_PASSWORD=\<openstack_driver_password\>

      SSL_CERT_VERIFY=\<True_or_False\>

      CERT_FILE_PATH=\<path_of_the_certificate_file\>

      ユーザーがssl_cert_verifyを「False」に設定すると、NetScaler Consoleはリクエスト呼び出しでverify=Falseを送信し、SSL証明書の検証を無効にします。ssl_cert_verifyが「True」に設定されており、cert_file_pathエントリが存在する場合、NetScaler Consoleはリクエストのverifyパラメータにこのパスを送信します。それ以外の場合、NetScaler Consoleはverify=Trueを送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

NetScaler Consoleを「高可用性」モードで展開するには、heat.confファイルで次のパラメータを更新します。

NMAS_BASE_URI=\<フロントエンド仮想サーバーのIPアドレス\>

3. OpenStackでHeatサービスを再起動します。

   OpenStackでNetScaler Heatサービスを再起動すると、定義されているすべてのNetScaler Console StyleBookがリソースとしてHeatにインポートされます。また、NetScalerネットワークリソースと証明書リソースも、NetScaler HeatリソースとしてOpenStackにインポートされます。

4. NetScaler ConsoleをOpenStackに登録します。

   a. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** の順に移動し、**Configure OpenStack Settings** をクリックします。

   b. **Configure OpenStack Settings** ページで、OpenStackを構成するためのパラメーターを設定できます。ここでは、DefaultとCustomizedの2つのオプションがあります。

   c. OpenStackサービスがデフォルトポートで実行されている場合は、**Default** を選択します。次のパラメーターを入力します。

      i. OpenStackコントローラーのIPアドレス

      ii. 管理者ユーザー名

      iii. パスワード

      iv. OpenStack管理者テナント

      v. NetScalerドライバーとHeatのパスワード

   **注**

   これは、heat.confファイルに入力したパスワード (NMAS_PASSWORD) と同じです。

5. サービスパッケージを作成し、テナントとのSLAを定義します。

   OpenStack登録中に、各ユーザーに対してNetScaler Consoleにテナントが作成され、そのテナント情報はLBaaSドライバーとHeatプラグインの両方で使用されます。Heatプラグインはこ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

の情報を使用してNetScaler Consoleに接続し、StyleBookをOpenStackのHeatリソースとしてインポートします。

**注記**

NetScaler ConsoleおよびOpenStackでのサービスパッケージの作成やその他の事前設定タスクの詳細については、NetScaler ConsoleとOpenStackプラットフォームの統合を参照してください。

6. NetScaler Consoleの関連するすべてのStyleBookがOpenStack Heatにリソースとしてインポートされていることを確認してください。また、NetScalerネットワークリソースとNetScaler証明書リソースもOpenStack Heatにリソースとしてインポートされていることを確認してください。

   **注記**

   現在、NetScaler Consoleに同梱されているStyleBookのみを使用できます。

   テナントは現在、OpenStackでHeatテンプレートを作成し、必要なHeatパラメーターの値を入力して、Heatスタックを展開できます。Heatスタックが展開されると、構成がNetScaler Consoleにプッシュされ、必要なNetScalerインスタンスが構成されます。

**Heatテンプレートを準備してHeatスタックを起動するには：**

1. OpenStackでは、テナントはHeatリソースを使用してHeatオーケストレーションテンプレート（HOT）を作成できます。
2. OpenStack Horizonでは、テナント管理者は**Project** \> **Orchestration** \> **Stacks**に移動して、Heatテンプレートを作成し、Heatスタックを起動できます。HOTを作成する方法は2つあります。

   - **ファイル** - ローカルディレクトリから更新されたテンプレートを選択します
   - **直接入力** - ウィンドウのテンプレートからYAMLコンテンツをコピーして貼り付けます

   **注記**

   スタックの展開に成功した後、テナントはChange Stack Templateを使用してスタックを更新できます。ただし、スタックの作成時に最初に提供されたサブネット情報と仮想IPアドレス（VIP）は変更できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

テナントがスタックを展開した後、NetScaler Consoleの**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Requests**に移動してタスクのリストを確認します。また、NetScaler Consoleの**Applications** \> **Configuration**に移動して、NetScalerインスタンスがStyleBooks構成パックの形式で正常に構成されていることを確認します。

**NetScaler Console スタイルブックの例：**

以下の画像は、NetScaler Console StyleBooksがどのように構築され、そのコンポーネントが簡単に説明されている例を示しています。NetScaler Console StyleBooksの詳細と、付属のStyleBooksの使用方法については、StyleBooksを参照してください。

**Heatテンプレートの例:**

以下の画像は、YAMLで定義されたHeatテンプレートの構造を示し、Heatリソースとしてインポートされるstylebooksリソースとnetscalerネットワークリソースを指しています。

Heatサービスとテンプレートの作成方法の詳細については、OpenStack Heatドキュメントを参照してください。

### サービスパッケージの分離ポリシー

#### 専用分離ポリシー

専用ポリシーのNetScaler Consoleサービスパッケージに関連付けられているすべてのテナントには、このサービスパッケージの一部であるインスタンスの中からNetScalerインスタンスが割り当てられます。この割り当てられたNetScalerインスタンスは、他のテナントと共有されません。

#### パーティション分離ポリシー

パーティションポリシーのサービスパッケージに関連付けられているすべてのテナントには、そのサービスパッケージの一部であるNetScalerインスタンスの専用論理管理者パーティションが割り当てられます。

#### 共有分離ポリシー

サービスパッケージに関連付けられているテナントは、サービスパッケージの一部であるNetScalerインスタンスを共有します。テナントのすべての構成は、1つのNetScalerインスタンスに割り当てられます。このモードでは、複数のテナントの構成を同じNetScalerインスタンスでホストできます。デバイスタイプとして**NetScaler VPX**または**NetScaler MPX**を選択できます。サー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ビスパッケージに1つのNetScalerインスタンスのみを割り当てるか、多数のインスタンスを割り当てるかを選択できます。つまり、複数のテナントがNetScalerデバイスの1つまたは複数の仮想インスタンスを共有できます。

**注**

NetScaler SDXにはNetScaler VPXがプロビジョニングされているため、サービスパッケージにはNetScaler SDXインスタンスをNetScaler VPXインスタンスとしてのみ追加してください。



**注**

テナント名やIDだけでなく、他のカスタム属性に基づいてポリシーを柔軟に配置するポリシーを作成することもできます。柔軟な配置ポリシーの詳細については、「柔軟なポリシーベースのデバイス割り当て」を参照してください。

### 柔軟なポリシーベースのデバイス割り当て

NetScaler Console は、テナントと合意した SLA に基づいて、NetScaler 仮想インスタンスをテナントに割り当てます。仮想インスタンスをテナントに割り当てることで、インスタンスとテナントの間に1対1の関係が作成され、テナントはデータセンター内の1つのサービスパッケージにのみ割り当てることができます。

状況によっては、テナントが複数のインスタンスを必要とする場合や、インスタンスの割り当てがテナントを基準とするのではなく、ネットワーク ID やアプリケーションなどの他の要因に基づく場合があります。このような場合、NetScaler Console を使用すると、ユーザー定義の式に基づいて配置ポリシーを正確に定義し、ロードバランサー構成を管理対象インスタンスの1つに割り当てることができます。

配置ポリシーは、ユーザーが作成する各ロードバランサー構成で使用される NetScaler インスタンスを決定する柔軟性を提供します。NetScaler Console の柔軟な配置ポリシーは、テナントに基づいて NetScaler インスタンスを割り当てる既存の方法に加えて、追加のオプションを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

インスタンスは手動でテナントに割り当てることも、作成された式に基づいてインスタンスを割り当てるために配置ポリシーを使用することもできます。これら両方の方法を単一のサービスパッケージで同時に使用することはできません。

配置ポリシーは、プールやロードバランサーなどの主要な LBaaS 構成オブジェクトのプロパティで定義されたブール式に基づいています。NetScaler Console の配置ポリシーユーザーインターフェイスは、カスタマイズされたポリシーを定義するために選択できる事前定義された式を提供します。異なる式に対して複数の配置ポリシーを作成できます。したがって、各テナントはテナントの要件によって定義された複数のデバイスを持つことができます。

まず、後で構成する必要があるルートオブジェクトに一致する式を選択する必要があります。ルートオブジェクトは、LBaaS V1 の場合はプールオブジェクト、LBaaS V2 の場合はロードバランサーオブジェクトになります。したがって、NetScaler Console のポリシーベースの配置は、LBaaS V1 と V2 の両方の API でサポートされています。これらの配置ポリシーは、その後サービスパッケージに関連付けられます。ルートオブジェクトがインスタンスに配置されると、モデル内の後続のオブジェクトがそのインスタンスに追加されます。

たとえば、プール構成オブジェクトには次のプロパティを含めることができます。

- tenant_id
- 名前
- 説明
- プロトコル
- lb_method
- subnet_id
- subname_name
- admin_state_up
- ステータス
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以下は、ポリシーの式を定義するためにプールプロパティを使用する式の例です。

1. プール名に基づくポリシー式

```
config["pools"]["name"] =="high-end-pool"
```

2. プールサブネット名に基づくポリシー式

```
config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
```

3. ロードバランサーサブネット名に基づくポリシー式

```
config["loadbalancers"]["subnet_name"] == "mas-subnet"
```

### 配置ポリシーの追加

1. NetScaler Consoleのホームページから、**Orchestration** > **Cloud Orchestration** > **Placement Policy** の順に移動し、**Add** をクリックします。
2. **Add Placement Policy** ページで、次のパラメーターを設定します。
   a. 名前 - 配置ポリシーの名前を入力します
   b. よく使用される式 - ドロップダウンリストから式を選択します。
   c. 式 - このフィールドには、前のフィールドで選択した式に基づいて論理 (ブール) 式が入力されます。必要に応じてフィールド名を編集します。

> **注**
>
> 複数のポリシーを作成する場合は、ポリシーが相互に排他的であることを確認してください。

3. **OK** をクリックします。
4. **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages** に移動し、**Add** をクリックします。
5. **Service Package** ページで、次のパラメータを設定します。
   a. 名前 - サービスパッケージの名前を入力します
   b. 分離ポリシー - **Shared** ポリシーを選択します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

共有分離ポリシーでは、テナントのロードバランサー構成は、テナントに割り当てられたデバイス内で他のテナントのロードバランサー構成と共存します。

c. デバイスタイプ - 事前プロビジョニングされた **NetScaler VPX** または **NetScaler MPX** を選択します

テナントのすべてのロードバランサー構成を1つのデバイスに紐付けたい場合は、**Allot one device** を選択します。テナントの各ロードバランサー構成を配置ポリシーに基づいて複数のデバイスに分散させたい場合は、**Allot many devices** を選択します。

> **注**
>
> NetScaler SDX は、NetScaler VPX インスタンスとしてのみサービスパッケージに追加する必要があります。これは、NetScaler SDX に NetScaler VPX がプロビジョニングされているためです。

d. 配置方法 - 「**最小構成**」を選択します。

「最小構成」が選択されている場合、その時点で構成されているプールメンバーの数が最も少ないNetScalerインスタンスが、テナントのデバイスとして選択されます。

サービスパッケージ(/en-us/netscaler-application-delivery-management-software/media/openstack-flexi-policy-ser-pack.png)

6. 「**続行**」をクリックします。
7. 「**デバイスの割り当て**」セクションで、利用可能なNetScalerデバイスを構成済みデバイスリストに追加します。

サービスパッケージ - 最小構成配置方法(/en-us/netscaler-application-delivery-management-software/media/openstack-flexi-policy-assign-device.jpg)

8. 「**続行**」をクリックします。
9. 「**配置ポリシー/OpenStackテナントの割り当て**」セクションで、以前に作成した配置ポリシーを追加します。

配置ポリシーの割り当て(/en-us/netscaler-application-delivery-management-software/media/openstack-flexi-policy-assign-policy.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

ポリシーが見つからない場合、フォールバックメカニズムが復活し、NetScaler Consoleはテナントに基づいてNetScalerインスタンスを割り当てます。テナントがいずれのサービスパッケージにも含まれていない場合、NetScaler Consoleは次のエラーメッセージを表示します。

「テナント `admin` はどのサービスパッケージにも属しておらず、デフォルトのサービスパッケージもありません。」.

10. 「**続行**」をクリックし、次に「**完了**」をクリックします。

## NSX Manager: NetScalerインスタンスの手動プロビジョニング

NetScaler Consoleは、VMwareネットワーク仮想化プラットフォームと統合し、NetScalerサービスの展開、構成、管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが解消され、vSphere/vCenter管理者はNetScalerサービスをより迅速にプログラムで展開できるようになります。

この記事では、VMware NSX ManagerとNetScaler Consoleの両方で実行する必要があるタスクのリストを示します。

**注**

VMware NSX for vSphere 6.2以降がインストールおよび構成されており、ロードバランシングする必要があるエッジゲートウェイ、DLR、および仮想マシンがすでに作成されていることを確認してください。

### 前提条件

- 最小要件を満たすハードウェアを備えたVMware ESXiバージョン4.1以降をインストールします。
- 最小システム要件を満たす管理ワークステーションにVMware Clientをインストールします。
- 最小システム要件を満たす管理ワークステーションにVMware OVF Tool（VMware ESXiバージョン4.1に必要）をインストールします。
- サポートされているいずれかのハイパーバイザーにNetScaler Consoleをインストールします。

  サポートされているいずれかのハイパーバイザーにNetScaler Consoleビルド13.1をインストールするタスクについては、「NetScaler Consoleの展開」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### VMware ESXiのハードウェア要件

次の表に、NetScaler Console仮想アプライアンスをインストールするためにVMware ESXiサーバーで必要となる仮想コンピューティングリソースを示します。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 8 GB |
| 仮想CPU | 8 |
| ストレージ容量 | 500 GB |
| 仮想ネットワークインターフェイス | 1 |
| スループット | 1 ギガビーピーエス |

**注**

上記で指定されたメモリとハードディスクの要件は、ホスト上で他の仮想マシンが実行されていないことを考慮して、VMware ESXiサーバーにNetScaler Consoleを展開するためのものです。VMware ESXiサーバーのハードウェア要件は、その上で実行される仮想マシンの数によって異なります。

### VMware NSXの構成

- 異なる容量のNetScaler VPXインスタンスのプールを作成し、それらを異なるサービスパッケージに追加します。

例:

- VPX1000 (1 Gbps) の NetScaler VPX インスタンスを5つ作成します。これらのインスタンスは、Gold サービスパッケージに追加されます。
- VPX10 (10 Mbps) の NetScaler VPX インスタンスを5つ作成します。これらのインスタンスは、Bronze サービスパッケージに追加されます。

1. vSphere Client で、**Networking** に移動し、VLAN トランキングタイプのポートグループを、例えば 101-105 の範囲で作成します（全範囲を指定することもできますが、必要な VLAN のみに対して VLAN タイプのポートグループを作成してください）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vSphere Client でポートグループを構成する (/en-us/netscaler-application-delivery-management-software/media/nsx-manager-configure-settings.jpg)

2. 各 NetScaler VPX インスタンスに新しいインターフェイスを作成し、上記で作成した VLAN 範囲トランクポートグループにアタッチします。

   NSVPX-ESX 設定 (/en-us/netscaler-application-delivery-management-software/media/nsx-manager-edit-settings.jpg)

3. vSphere Client で、**Networking** に移動し、VLAN タイプのポートグループを作成します。

   例えば、最初のトランクポートグループが 101-105 の範囲で作成された場合、VLAN ごとに1つずつ、合計5つの VLAN ポートグループを作成します。つまり、VLAN 101 のポートグループ、VLAN 102 のポートグループ、といった具合に、VLAN 105 まで作成します。

   vSphere Client で VLAN ポートグループを作成する (/en-us/netscaler-application-delivery-management-software/media/nsx-manager-configure-dlr-settings.jpg)

### NetScaler Console で NetScaler VPX インスタンスを追加する

NetScaler Console で NetScaler VPX インスタンスを追加し、各デバイスのトランクグループの VLAN 範囲を指定します。

1. NetScaler Console で、**Infrastructure** \> **Instances** \> **NetScaler VPX** に移動し、**Add** をクリックします。
2. **Add NetScaler VPX** ページで、インスタンスのホスト名、各インスタンスの IP アドレス、または IP アドレスの範囲のいずれかを指定し、**Profile Name** リストからインスタンスプロファイルを選択します。+ アイコンをクリックして新しいインスタンスプロファイルを作成することもできます。
3. **OK** をクリックします。
4. **NetScaler VPX** ページの一覧から新しく追加された NetScaler VPX インスタンスを選択し、**Action** フィールドの下矢印ボタンをクリックします。**Configure Interfaces for Orchestration** を選択します。

   

5. **インターフェース**ページで、管理インターフェースを選択し、**無効にする**をクリックして、VLANが管理インターフェースにバインドされないようにします。

   

6. **インターフェース**ページで、必要なインターフェースを選択し、**VLAN範囲の構成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. NSX Managerで構成されているVLAN範囲を入力し、**OK**をクリックし、次に**閉じる**をクリックします。



### NetScaler ConsoleへのVMware NSX Managerの登録

VMware NSX ManagerをNetScaler Consoleに登録して、両者間の通信チャネルを作成します。

1. NetScaler Consoleで、ドロップダウンリストから**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager**に移動し、**NSX Manager設定の構成**をクリックします。
2. **NSX Manager設定の構成**ページで、次のパラメーターを設定します。
   a. NSX Manager IPアドレス - NSX ManagerのIPアドレス。
   b. NSX Managerユーザー名 - NSX Managerの管理者ユーザー名。
   c. パスワード - NSX Managerの管理者ユーザーのパスワード。
3. **NSX Managerが使用するNetScaler Consoleアカウント**セクションで、NSX ManagerのNetScaler Driverユーザー名とパスワードを設定します。NetScaler Consoleは、これらのログオン資格情報を使用して、NSX Managerからのロードバランサー構成要求を認証します。
4. **OK**をクリックします。
5. **Orchestration** \> **System** \> **Deployment Settings** に移動します。トランクポートグループで設定されたVLAN範囲を指定します。

   VLANネットワークの展開設定(/en-us/netscaler-application-delivery-management-software/media/nmas-vlan-deployment-setting.jpg)
6. vSphere Web ClientでNSX Managerにログオンし、**Service Definitions** \> **Service Managers** に移動します。

   Citrix NetScaler Consoleがサービスマネージャーの1つとして表示されます。これは、登録が成功し、NSX ManagerとNetScaler Console間の通信チャネルが確立されたことを示します。

   展開されたVLAN設定の表示(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-service-defn-settings.jpg)

### NetScaler Consoleでのサービスパッケージの作成

1. NetScaler Consoleで、**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Service Packages** に移動し、**Add** をクリックして新しいサービスパッケージを追加します。
2. **Service Package** ページで、**Basic Settings** セクションの次のパラメーターを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 名前 – サービスパッケージの名前を入力します

b. 分離ポリシー – デフォルトでは、分離ポリシーはDedicatedに設定されています

c. デバイスタイプ – デフォルトでは、デバイスタイプはNetScaler VPXに設定されています

> **注**
>
> これらの値は、このバージョンではデフォルトで設定されており、変更することはできません。

d. **Continue** をクリックします。

サービスパッケージ(/en-us/netscaler-application-delivery-management-software/media/nsx-orch-service-package-settings.jpg)

3. 「**Assign Devices**」セクションで、このパッケージ用に事前プロビジョニングされたVPXを選択し、「**Continue**」をクリックします。
4. 「**Publish Service Package**」セクションで、「**Continue**」をクリックしてサービスパッケージをVMware NSXに公開し、その後「**Done**」をクリックします。

この手順では、NSX Managerでサービスパッケージを構成します。1つのサービスには複数のデバイスを追加でき、複数のエッジが同じサービスパッケージを使用してNetScaler VPXインスタンスをNetScaler Consoleにオフロードできます。

5. vSphere Web ClientでNSX Managerにログオンし、「**Service Definitions**」 \> 「**Services**」に移動します。

NetScaler Consoleサービスパッケージが登録されていることを確認できます。

### エッジのロードバランサーサービス挿入の実行

以前に作成したNSX Edgeゲートウェイでロードバランサーサービス挿入を実行します（ロードバランシング機能をNSX LBからNetScalerにオフロードします）。

1. NSX Managerで、「**Home**」 \> 「**NSX Edges**」に移動し、構成したエッジゲートウェイを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 「**Manage**」をクリックし、「**Load Balancer**」タブで「**Global Configuration**」を選択し、「**Edit**」をクリックします。

3. 「**Enable Load Balancer**」、「**Logging**」、「**Enable Service Insertion**」を選択して有効にします。

   a. 「**サービス定義**」で、NetScaler Consoleで作成され、NSX Managerに公開されたサービスパッケージを選択します。

   「サービス定義」(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-edit-load-balancer-global-settings.jpg)

4. 既存のランタイムNICを選択し、編集アイコンをクリックして、NetScaler VPXが割り当てられるときに接続する必要があるランタイムNICを編集します。

   「ランタイムNIC」(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-runtime-nics.jpg)

5. NICの名前を編集し、接続タイプを「**データ**」として指定し、「**変更**」をクリックします。

   「NIC名を編集」(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-edit-runtime-nics.jpg)

6. 適切なWeb論理スイッチを選択します。

   「論理スイッチを選択」(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-runtime-nics-select-logical-switch.jpg)

7. 「**プライマリIP割り当てモード**」で、ドロップダウンリストから「IPプール」を選択し、「IPプール」フィールドのドロップダウン矢印ボタンをクリックします。

   「プライマリIP割り当てモード」(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-runtime-nics-ip-pool.jpg)

8. 「**IPプールを選択**」ウィンドウで、適切なIPプールを選択し、「**OK**」をクリックします。

   「IPプールを選択」(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-runtime-nics-select-ip-pool.jpg)

   IPアドレスが取得され、NetScaler VPXアプライアンスのソースネットIPアドレスとして設定されます。NSX ManagerでL2ゲートウェイが作成され、VXLANをVLANにマッピングします。

   「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

」

すべてのデータインターフェイスはランタイムNICとして接続され、DLRのインターフェイスの一部です。

9. ビューを更新して、ランタイムの作成を確認します。



10. VMが起動すると、Statusの値が**In Service**に、Install Stateの値が**Enabled**に変わります。



**注**

NetScaler Consoleで、**Orchestration** \> **Requests**に移動して、LBサービス挿入の完了の進行状況の詳細を確認します。

### NSX ManagerでのL2ゲートウェイの表示

1. vSphere Web ClientでNSX Managerにログオンし、**NSX Edges**に移動して、作成されたDLRを選択します。



2. DLRページで、**Manage** \> **Bridging**に移動します。リストにL2ゲートウェイが表示されます。



**注**

各データインターフェイスに対してL2ゲートウェイが作成されます。

### 割り当てられたNetScalerの表示

1. NetScaler Consoleに表示されているIPアドレスを使用してNetScaler VPXインスタンスにログオンします。次に、**Configuration** \> **System** \> **Networking** に移動します。右側のペインに、2つのIPアドレスが追加されていることが確認できます。詳細を表示するには、IPアドレスのハイパーリンクをクリックします。



サブネットIPアドレスは、NSXに追加されたWebインターフェイスのIPアドレスと同じです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. **Configuration** \> **System** \> **Licenses** に移動し、このインスタンスに適用されているライセンスを表示します。

### StyleBookを使用したNetScaler VPXインスタンスの構成

1. NetScaler Consoleで、**オーケストレーション** \> **SDNオーケストレーション** \> **NSX Managerの構成** \> **エッジゲートウェイ** に移動します。

   StyleBookを介した負荷分散構成を適用する必要がある、該当するEdge Gatewayに割り当てられているNetScalerインスタンスのIPをメモします。

2. 新しいStyleBookを作成します。**Applications** \> **Configuration** に移動し、StyleBookをインポートして、リストからStyleBookを選択します。

   新しいStyleBookを作成するには、独自のStyleBookを作成する を参照してください。

3. 必要なすべてのパラメーターの値を指定します。



4. これらの構成設定を実行するNetScaler VPXインスタンスを指定します。



5. 先ほどメモしたIPインスタンスを選択し、**Select** をクリックします。

   「IPインスタンスを指定する」(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebook-config-3.jpg)

6. 選択したデバイスに構成を適用するには、**作成**をクリックします。

   「構成パックを作成する」(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebook-config-4.jpg)

### ロードバランサー構成の表示

1. NetScaler VPXインスタンスにログオンし、**Configuration** \> **Traffic Management** \> **Load Balancing** に移動して、作成されたロードバランシング仮想サーバーを表示します。

   「ロードバランサー構成を表示する」(/en-us/netscaler-application-delivery-management-software/media/nmas-view-lb-config-view.jpg)

   作成されたサービスグループも表示できます。

   「サービスグループを表示する」(/en-us/netscaler-application-delivery-management-software/media/nmas-view-sg-config-view.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. サービスグループを選択し、**メンバーの管理**をクリックします。**サービスグループメンバーの構成**ページに、サービスグループに関連付けられているメンバーが表示されます。

   「サービスグループメンバーを構成する」(/en-us/netscaler-application-delivery-management-software/media/nmas-view-sg-members.jpg)

### ロードバランサーサービスの削除

1. NetScaler Consoleで、**Applications** \> **Configuration** に移動し、**X**アイコンをクリックしてアプリケーション構成を削除します。
2. vSphere Web ClientでNSX Managerにログオンし、NetScaler VPXインスタンスが接続されているエッジゲートウェイに移動します。
3. **Manage** \> **Load Balancer** \> **Global Configuration** に移動し、ランタイムエントリを右クリックして、**プロビジョニング解除**をクリックします。

   **注**

   NetScaler Consoleのエッジゲートウェイは、NSX Managerのランタイムエントリに対応します。

   アンプロビジョニング(/en-us/netscaler-application-delivery-management-software/media/nmas-delete-lb-service-2.jpg)

   NetScaler VPXインスタンスはサービス対象外になります。
4. NetScaler Consoleで、**オーケストレーション** \> **SDNオーケストレーション** \> **NSX Managerの構成** \> **エッジゲートウェイ** に移動します。削除されたインスタンスへのエッジゲートウェイの対応するマッピングが存在しないことを確認します。

## NSX Manager: NetScalerインスタンスの自動プロビジョニング

### 概要

NetScaler Consoleは、VMwareネットワーク仮想化プラットフォームと統合し、NetScalerサービスの展開、構成、および管理を自動化します。この統合により、物理ネットワークトポロジに関連する従来の複雑さが抽象化され、vSphere/vCenter管理者はNetScalerサービスをより迅速にプログラムで展開できるようになります。

VMware NSX Managerでのロードバランシングサービスの挿入および削除中に、NetScaler ConsoleはNetScalerインスタンスを動的にプロビジョニングおよび破棄します。この動的プロビジョニングには、NetScaler ConsoleでのNetScaler VPXライセンス割り当ての自動化が必要で

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。NetScalerライセンスがNetScaler Consoleにアップロードされると、NetScaler Consoleはライセンスサーバーの役割を果たします。

### 前提条件

**注**

この統合は、**VMware NSX for vSphere 6.1以前**のみでサポートされています。

- NetScaler Console、バージョン13.0、高可用性構成でESXにインストール済み。
- NetScaler VPX、バージョン13.0
- NetScaler VPXインスタンス用のNetScaler VPXライセンス、バージョン13.0
- 最小要件を満たすハードウェアを備えたVMware ESXiバージョン4.1以降をインストールします。
- 最小システム要件を満たす管理ワークステーションにVMware Clientをインストールします。
- 最小システム要件を満たす管理ワークステーションにVMware OVF Tool (VMware ESXiバージョン4.1に必要) をインストールします。

### NetScaler ConsoleとNetScalerインスタンスの高可用性展開

NetScaler Console HAセットアップをプロビジョニングするには、NetScalerサイトからダウンロードしたNetScaler Consoleイメージファイルをインストールします。NetScaler Console HAセットアップのプロビジョニング方法の詳細については、「高可用性でのNetScaler Consoleの展開」を参照してください。

### NetScaler Console HAエンドポイントの詳細設定

HAモードで展開されているNetScaler ConsoleにVMware NSX Managerを統合するには、まずロードバランシングNetScalerインスタンスの仮想IPアドレスを入力する必要があります。また、NetScalerロードバランシング仮想サーバーに存在する証明書ファイルをNetScaler Consoleファイルシステムにアップロードする必要があります。

#### NetScaler Consoleでロードバランシング構成情報を提供するには：

1. NetScaler Console HAノードで、**System** \> **Deployment** の順に移動します。
2. 右上隅にある をクリックし、 ページで をクリックします。

   HA設定(/en-us/netscaler-application-delivery-management-software/media/nsmas-nsx-ha-endpoints-1.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ページで、ロードバランシングNetScalerインスタンスにすでに存在するのと同じ証明書をアップロードします。
4. ロードバランシングNetScalerインスタンスの仮想IPアドレスを入力し、 をクリックします。

   HAエンドポイントの詳細(/en-us/netscaler-application-delivery-management-software/media/nsmas-nsx-ha-endpoints-2.jpg)

### VMware NSX ManagerをNetScaler Consoleに登録する

2つのNetScaler Consoleサーバーを高可用性でセットアップすると、2つのサーバーノードはアクティブ/パッシブモードになります。プライマリNetScaler Consoleサーバーノードにログオンして、HAモードのNetScaler ConsoleにVMware NSX Managerを登録し、両者間の通信チャネルを作成します。

**HAモードのNetScaler ConsoleにVMware NSX Managerを登録するには：**

1. プライマリNetScaler Consoleサーバーノードで、**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** の順に移動します。
2. をクリックします。
3. ページで、次のパラメータを設定します。
   a. NSX Manager IPアドレス - NSX ManagerのIPアドレス。
   b. NSX Managerユーザー名 - NSX Managerの管理者ユーザー名。
   c. パスワード - NSX Managerの管理者ユーザーのパスワード。
4. NSX Managerで使用されるNetScaler Consoleアカウントセクションで、NSX ManagerのNetScaler Driverパスワードを設定します。
5. **OK**をクリックします。

### NetScaler Consoleでのライセンスのアップロード

NetScaler VPXライセンスをNetScaler Consoleにアップロードします。これにより、NetScaler ConsoleはNSXとのオーケストレーション中にインスタンスにライセンスを自動的に割り当てることができます。

**NetScaler Consoleにライセンスファイルをインストールするには：**

1. NetScaler Consoleで、**Infrastructure > Pooled Licensing**に移動します。
2. **License Files**セクションで、次のいずれかのオプションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **ローカルコンピューターからライセンスファイルをアップロード** - ライセンスファイルがローカルコンピューターにすでに存在する場合は、NetScaler Consoleにアップロードできます。ライセンスファイルを追加するには、**Browse**をクリックし、追加するライセンスファイル（.lic）を選択します。次に、**Finish**をクリックします。

b. **ライセンスアクセスコードを使用** - Citrixは、購入したライセンスのライセンスアクセスコードをメールで送信します。ライセンスファイルを追加するには、テキストボックスにライセンスアクセスコードを入力し、**Get Licenses**をクリックします。

> **注**
>
> いつでも、ライセンス設定からNetScaler Consoleにライセンスを追加できます。

☐

### NetScaler Console で NetScaler VPX イメージをアップロードする

サービスパッケージで定義されているとおりに NetScaler Console がこれらのイメージを使用できるように、NetScaler イメージを NetScaler Console に追加します。

**NetScaler Console で NetScaler VPX イメージをアップロードするには：**

1. NetScaler Console で、**オーケストレーション** \> **SDN オーケストレーション** \> **VMware NSX Manager** \> **ESX NSVPX イメージ** の順に移動します。
2. **Upload** をクリックし、ローカルストレージフォルダーから NetScaler VPX zip パッケージを選択します。

### NetScaler Console でサービスパッケージを作成する

NetScaler リソースの割り当て方法を規定する SLA のセットを定義するために、NetScaler Console でサービスパッケージを作成します。

**NetScaler Console でサービスパッケージを作成するには：**

1. NetScaler Console で、**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Service Packages** の順に移動し、**Add** をクリックして新しいサービスパッケージを追加します。
2. **Service Package** ページで、**Basic Settings** セクションの次のパラメーターを設定します。

   a. 名前 - サービスパッケージの名前

   b. 分離ポリシー - **Dedicated** を選択

   c. NetScaler インスタンスプロビジョニング - **Create Instance OnDemand** を選択

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 自動プロビジョニングプラットフォーム - **CitrixNetScaler SDX** を選択

e. **Continue** をクリックします。

3. 「**自動プロビジョニング設定**」セクションで、NSXプラットフォームに展開するために最近アップロードされたNetScaler VPX zipパッケージを選択し、対応するライセンスを選択して、「**続行**」をクリックします。

「

**注**

」

「**高可用性**」セクションで、HA用にNetScalerインスタンスをプロビジョニングするチェックボックスをオンにします。

自動プロビジョニング設定(/en-us/netscaler-application-delivery-management-software/media/nsx-autoprovisioning-mas-ha-service-package.jpg)

「

**注**

」

上図のリストボックスに表示されているライセンス名「VPX8000_Advanced, 2 number」は例であり、以下のように説明されます。

- VPX - このライセンスはNetScaler VPXインスタンスを展開するためのものです
- 8000 - 消費可能な帯域幅は8GBです
- Advanced - NetScaler®はStandard、Advanced、およびPremiumの3種類のライセンスを提供します
- 2 number - このライセンスを使用して2つのNetScaler VPXインスタンスを展開できます

「**ライセンス**」リストボックスに表示されるライセンス名は、Citrixから購入したライセンスによって異なります。

4. 「**続行**」をクリックします。

5. サービスパッケージはNSX Managerに公開されます。NSX Managerで、**Service Definitions** \> **Service Managers** に移動します。NetScaler Consoleがサービスマネージャーの1つとして

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示されます。これは、登録が成功し、NSX ManagerとNetScaler Consoleの間で双方向通信が確立されたことを示します。

「

**注**

」

高可用性展開のNetScaler Consoleの場合、ライセンスはNetScaler Consoleライセンスサーバーノードにのみアップロードされます。NetScaler Consoleノードはアクティブ/パッシブモードです。

### Edge へのロードバランサーサービス挿入の実行

既存の NSX Edge Gateway でロードバランサーサービス挿入を実行します。つまり、ロードバランシング機能を NSX ロードバランサーから NetScaler にオフロードします。

**NSX Edge Gateway にロードバランシングサービスを挿入するには：**

1. NSX Manager で、**Home** \> **Networking and Security** \> **NSX Edges** の順に移動し、構成済みのエッジゲートウェイをダブルクリックして選択します。
2. **Manage** をクリックし、**Load Balancer** タブで **Global Configuration** を選択し、**Edit** をクリックします。
3. **Enable Load Balancer** と **Enable Service Insertion** を選択して、それらを有効にします。
4. **Service Definition** で、NSX Manager に公開されたサービスパッケージを選択します。
5. 管理インターフェイス用に仮想NICを1つ、データインターフェイス用に仮想NICを1つ以上構成します。管理用とデータ用のネットワークをそれぞれ選択します。

   **注**

   プライマリIP割り当てモードでIPプールオプションを選択します。NetScaler Consoleは、IPアドレスの手動割り当てまたはDHCP割り当てをサポートしていません。

6. 更新アイコンをクリックして、ランタイムの作成を確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

HA展開で2つのNetScaler VPXインスタンスをデプロイしているため、NSX Manager に2つのランタイムが作成されます。

画面に表示されるランタイムを表示するには、画面を更新する必要がある場合があります。

7. ランタイムを選択し、**Actions** をクリックし、ポップアップメニューから **Install** を選択します。HAの場合、もう一方のランタイムについてもこれを繰り返します。
8. 仮想マシンが両方とも起動すると、Statusの値は「In Service」に、Install Stateの値は「Enabled」に変わります。

**注**

ステータスの変更を表示するには、画面を更新する必要がある場合があります。

9. NetScaler Consoleで、**Orchestration** \> **Requests** に移動して、サービス挿入の完了の進行状況の詳細を確認します。ランタイムを作成および更新するリクエストがNetScaler Consoleに届いていることがわかります。ランタイムが更新されたら、リクエストを選択し、**Tasks** ボタンをクリックして、NetScaler ConsoleがNSX Managerに追加されたことを確認します。

   HAの場合、NetScaler Consoleで2つのランタイムを作成および更新する2つのリクエストがあります。両方のランタイムが更新されたら、両方のリクエストを選択し、**Tasks** ボタンをクリックして、2つのNetScaler Console HAノードがNSX Managerに追加されたことを確認します。

10. NetScaler Consoleで、**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Edge Gateways** に移動します。右側のパネルで、NetScaler VPXがNSX Edge Gatewayに追加されたことを確認できます。

    HAの場合、HAモードの2つのNetScaler VPXインスタンスがNSX Edge Gatewayに追加されたことを確認できます。

11. NetScaler Consoleで、**Infrastructure > Pooled Licensing > VPX Licenses** に移動します。NetScaler VPXライセンスとインストールしたエディションを選択します。

    HAモードのNetScaler VPXインスタンスは2つのライセンスを消費し、ステータスは以下のように画面に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サービス挿入が完了したら、StyleBooksを使用して、次の2つの方法のいずれかでNetScalerインスタンスを構成できます。

- VMware NSX Manager GUIでNetScaler VPXの負荷分散サービスを構成する
- NetScaler Console GUIでNetScaler VPXの負荷分散サービスを構成する

### VMware NSX Manager GUIでNetScaler VPXの負荷分散サービスを構成する

組み込みのStyleBooksを使用して、NSX Edgeゲートウェイデバイスで負荷分散サービスの構成を有効にするには、次のタスクを実行します。

NSX Managerで、**Home** \> **Networking and Security** \> **NSX Edges** に移動し、設定済みのエッジゲートウェイをダブルクリックして選択します。

#### プールとプールメンバーの作成

異なる容量のサーバーとメンバーのプールを作成します。

1. **Manage** をクリックし、**Load Balancer** タブで **Pools** を選択し、「**+**」アイコンをクリックして新しいプールを追加し、次のパラメーターを設定します。
   a. 名前 - 新しいプールの名前
   b. アルゴリズム - プールが選択される基準となるアルゴリズムをドロップダウンリストから選択します。
   c. モニター - サービスモニターが default_http_monitor に設定されていることを確認します。
   d. メンバー - 「+」をクリックしてプールにメンバーを追加し、New Member ウィンドウで必要なパラメーターを入力します。
      i. 名前 - メンバーの名前
      ii. IPアドレス/VCコンテナ - 「選択」をクリックして利用可能なリストからオブジェクトを選択するか、オブジェクトのIPアドレスを入力します。
2. **OK** をクリックします。

必要な数のメンバーを追加します。

#### 仮想サーバーの作成

仮想サーバーのセットを作成し、各仮想サーバーにプールを割り当てます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**Manage**」をクリックし、「Load Balancer」タブで「**Virtual Servers**」を選択し、「**+**」アイコンをクリックして仮想サーバーを追加し、次のパラメータを設定します。

   a. アプリケーションプロファイル - デフォルトでは、NetScaler Consoleで作成したサービスプロファイルが表示されます。

   b. 名前 - 仮想サーバーの名前。

   c. IPアドレス - 「Select」をクリックして既存のIPアドレスプールを選択するか、新しいIPアドレスプールを作成します。

   d. デフォルトプール - ドロップダウンリストからデフォルトプールを選択します。

2. 「**OK**」をクリックします。
3. NetScaler Consoleで、**Orchestration** \> **Requests** に移動し、選択した1つ以上のNetScalerインスタンスでのサービス作成の完了に関する進行状況の詳細を確認します。
4. NetScaler Consoleで、**Applications** \> **Configuration** に移動し、`nsx-lb-mon` 設定パックが作成されていることを確認します。



### NetScaler Console GUIでのNetScaler VPXの負荷分散サービスの設定

NetScaler Console StyleBookを使用して、NetScalerインスタンスにロードバランサー構成を展開します。HAの場合、構成はHAにある両方のNetScalerインスタンスに展開されます。

**StyleBookを介して設定パックを作成するには：**

1. NetScaler Consoleで、**Applications** \> **Configuration** \> **Create New** に移動し、リストから「**HTTP/SSL LoadBalancing (with Monitors) StyleBook**」を選択します。StyleBookはユーザーインターフェイスページとして開き、このStyleBookで定義されているすべてのパラメータの値を入力します。
2. すべての必須パラメータの値を指定します。
3. NSX環境でプロビジョニングされたターゲットNetScaler VPXインスタンスを選択し、「**Create**」をクリックして、選択したデバイスに構成を適用します。HA展開の場合は、HAモードのインスタンスを選択します。

### NetScaler VPXインスタンスでの仮想サーバーとサービスグループの作成の確認

NetScaler VPXインスタンスにログインすることで、サービスグループと仮想サーバーが作成されていることを確認できます。

**サービスグループと仮想サーバーを表示するには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler VPXインスタンスにログオンします。HA展開の場合、HAにある両方のNetScalerインスタンスにログオンする必要があります。
2. **Configuration** \> **System** \> **Networking** に移動します。右ペインで、追加されたIPアドレスを表示できます。IPアドレスのハイパーリンクをクリックして詳細を確認します。サブネットIPアドレスが、NSXに追加されたWebインターフェースのIPアドレスと同じであることがわかります。
3. 次に、**Traffic Management** \> **Load Balancing** \> **Virtual Servers** に移動し、仮想サーバーの詳細を表示します。
4. 次に、**Service Groups** に移動し、サービスグループの詳細を表示します。
5. 最後に、**Configuration** \> **System** \> **Licenses** に移動して、このインスタンスに適用されているライセンスを表示します。

### ロードバランシングサービスの削除

NSX Managerに展開されたNetScaler VPXインスタンスでロードバランシングサービスが不要になった場合、以前に実行されたサービス挿入を削除できます。

**構成とサービス挿入を削除するには：**

1. NetScaler Consoleで、**Applications** \> **Configuration** に移動し、作成されたアプリケーション構成を選択して、「X」アイコンをクリックして構成を削除します。
2. NSX Managerで、NetScaler VPXインスタンスが接続されているエッジゲートウェイに移動します。**Manage** \> **Load Balancer** \> G**lobal Configuration** に移動し、ランタイムエントリを右クリックして、**Unprovision** をクリックします。仮想マシンはサービス停止状態になります。
3. NetScaler Consoleで、**Orchestration** \> **Cloud Orchestration** \> **Edge Gateways** に移動します。エッジゲートウェイと削除されたインスタンスの対応するマッピングがないことを確認します。

## NetScaler Console で Kubernetes Ingress 構成を管理する

Kubernetes (K8s) は、クラウドネイティブアプリケーションの展開、スケーリング、管理を自動化するオープンソースのコンテナオーケストレーションプラットフォームです。

Kubernetes は、クラスター外のクライアントトラフィックが Kubernetes クラスター内で実行されているアプリケーションのマイクロサービスにアクセスできるようにする Ingress 機能を提供します。NetScaler インスタンスは、Kubernetes クラスター内で実行されているアプリケーションへの Ingress として機能できます。NetScaler インスタンスは、クライアントから Kubernetes ク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ラスター内の任意のマイクロサービスへの南北トラフィックをロードバランシングし、コンテンツルーティングできます。

**注**

- NetScaler Console は、Kubernetes バージョン 1.14〜1.21 のクラスターで Ingress 機能をサポートしています。
- NetScaler Console は、NetScaler VPX および MPX アプライアンスを Ingress デバイスとしてサポートしています。
- Kubernetes 環境では、NetScaler インスタンスは「NodePort」サービスタイプのみをロードバランシングします。

複数の NetScaler インスタンスを、同じクラスターまたは異なるクラスターや名前空間で Ingress デバイスとして機能するように構成できます。インスタンスを構成した後、Ingress ポリシーに基づいて各インスタンスを異なるアプリケーションに割り当てることができます。

Kubernetes `kubectl` または API を使用して Ingress 構成を作成および展開できます。NetScaler Console から Ingress を構成および展開することもできます。

NetScaler Console で Kubernetes 統合の次の側面を指定できます。

- **クラスター** – NetScaler Console が Ingress 構成を展開できる Kubernetes クラスターを登録または登録解除できます。NetScaler Console でクラスターを登録するときは、Kubernetes API サーバー情報を指定します。次に、Kubernetes クラスターに到達し、Ingress 構成を展開できるエージェントを選択します。
- **ポリシー** – Ingress ポリシーは、クラスターまたは名前空間に基づいて NetScaler インスタンスを選択し、Ingress 構成を展開するために使用されます。ポリシーを追加するときは、クラスター、サイト、およびインスタンス情報を指定します。

### 開始する前に

Kubernetes クラスターで NetScaler インスタンスを Ingress デバイスとして使用するには、以下があることを確認してください。

- Kubernetes クラスターが配置されていること。
- NetScaler Consoleに登録されているKubernetesクラスター。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Kubernetesクラスターを管理するためのシークレットトークンでNetScaler Consoleを構成する

NetScaler ConsoleがKubernetesからイベントを受信できるようにするには、NetScaler Console用のサービスアカウントをKubernetesに作成する必要があります。そして、クラスター内で必要なRBAC権限を持つようにサービスアカウントを構成します。

1. NetScaler Console用のサービスアカウントを作成します。たとえば、サービスアカウント名は`citrixadm-sa`にすることができます。サービスアカウントの作成については、「複数のサービスアカウントを使用する」を参照してください。
2. `cluster-admin`ロールを使用してNetScaler Consoleサービスアカウントをバインドします。このバインディングにより、クラスター全体にわたる`ClusterRole`がサービスアカウントに付与されます。以下は、`cluster-admin`ロールをサービスアカウントにバインドするコマンドの例です。

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   NetScaler Consoleサービスアカウントを`cluster-admin`ロールにバインドすると、サービスアカウントはクラスター全体のアクセス権を持ちます。詳細については、「`kubectl` create `clusterrolebinding`」を参照してください。
3. 作成したサービスアカウントからトークンを取得します。

   たとえば、次のコマンドを実行して、`citrixadm-sa`サービスアカウントのトークンを表示します。

   ```
   kubectl describe sa citrixadm-sa
   ```
4. 次のコマンドを実行して、トークンのシークレット文字列を取得します。

   ```
   kubectl describe secret <token-name>
   ```

### NetScaler ConsoleにKubernetesクラスターを追加する

NetScalerエージェントを構成し、静的ルートを構成した後、NetScaler ConsoleにKubernetesクラスターを登録する必要があります。

Kubernetesクラスターを登録するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Orchestration** > **Kubernetes** > **Cluster** の順に移動します。 クラスターページが表示されます。
3. **Add** をクリックします。
4. 「**クラスターの追加**」ページで、次のパラメーターを指定します。

   a. **名前** - 任意の名前を指定します。

   b. **APIサーバーURL** - KubernetesメインノードからAPIサーバーURLの詳細を取得できます。

      i. Kubernetesメインノードで、コマンド `kubectl cluster-info` を実行します。

      

      ii. 「**Kubernetes master is running at.**」と表示されるURLを入力します。

   c. **認証トークン** - NetScaler Consoleを構成してKubernetesクラスターを管理する際に取得した認証トークン文字列を指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信アクセスを検証するために必要です。認証トークンを生成するには：

      i. Kubernetesメインノードで、次のコマンドを実行します。

      ```
      kubectl describe secret <token-name>
      ```

      ii. 生成されたトークンをコピーし、認証トークンとして貼り付けます。

      詳細については、Kubernetes ドキュメントを参照してください。

   d. リストからエージェントを選択します。

   e. 「**作成**」をクリックします。

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 設定

NetScaler Console は、インフラストラクチャのニーズに合わせて展開を構成し、統合するのに役立つ設定を提供します。以下のトピックは、これらの設定を構成するのに役立ちます。

- IPAM の構成
- アクションポリシーの構成
- 可観測性統合
- アクセス制御リストの構成
- NetScaler Console のログメッセージを使用してインフラストラクチャを管理および監視する

## IPアドレス管理 (IPAM) の構成

NetScaler Console IPAM を使用すると、NetScaler Console で管理されている構成で IP アドレスを自動的に割り当てたり解放したりできます。次の IP プロバイダーを使用して定義されたネットワークまたは IP 範囲から IP を割り当てることができます。

- NetScaler Console 組み込み IPAM プロバイダー。
- Infoblox IPAM ソリューション。

NetScaler Console IPAM は、次の用途で使用できます。

- **StyleBooks**: 構成を作成するときに、仮想サーバーに IP を自動割り当てします。
- **API gateway**: API プロキシに IP アドレスを自動割り当てします。

NetScaler Console で管理されている各ネットワークまたは IP 範囲の IP アドレスを追跡することもできます。

### 外部 IP アドレスプロバイダーの追加

NetScaler Console には、IP と IP 範囲を管理するための組み込み IPAM プロバイダーがあります。NetScaler Console に外部 IP アドレスプロバイダーを使用することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要:**

開始する前に、外部 IP アドレスプロバイダーで次の権限が有効になっていることを確認してください。

- プロバイダーに存在するネットワークを照会する機能。
- ネットワーク内の IP アドレスを予約する。
- ネットワークから IP アドレスを解放する。
- ネットワークから使用済みIPアドレスを取得します。
- ネットワークから利用可能なIPアドレスを取得します。

NetScaler Consoleで外部IPAMプロバイダーソリューションを追加するには、次の手順を実行します。

1. **>** に移動します。
2. で をクリックします。
3. IPAMプロバイダーを追加するには、次の詳細を指定します。
   - **名前** - NetScaler Consoleで使用するIPプロバイダー名を指定します。
   - **ベンダー** - リストからIPAMベンダーを選択します。
   - **URL** - NetScaler Console環境でIPアドレスを割り当てるIPAMソリューションのURLを指定します。URLは次の形式で指定してください。

     ```
     https://<host name>
     ```

     例: `https://myinfoblox.example.com`
   - **プライベートエンドポイントですか？** - Infoblox DDIがプライベートホストされている場合は、このチェックボックスをオンにしてからエージェントを選択します。
   - **ユーザー名** - IPAMソリューションにログインするためのユーザー名を指定します。
   - **パスワード** - IPAMソリューションにログインするためのパスワードを指定します。
4. をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 外部プロバイダーとしてのInfoblox DDI

現在、NetScaler® Console は Infoblox DDI を外部プロバイダーとしてサポートしています。Infoblox DDI は、公開アクセス可能であるか、または企業内の内部ネットワークからのみアクセス可能なプライベートホストであるかのいずれかです。プライベートホストの Infoblox DDI の場合、構成プロセス中に NetScaler エージェントを選択する必要があります。NetScaler エージェントは、企業のイントラネット内にあるプロバイダーにアクセスするためのプロキシとして機能します。

Infoblox プロバイダーと NetScaler Console IPAM を使用して、次のアクションを実行できます。

- IPAM ネットワークを一覧表示する
- IPAM ネットワークを作成、更新、および削除する
- IPAM ネットワークから IP アドレスを予約および解放する

#### IPAM ネットワークを作成する

Infoblox プロバイダーを使用して NetScaler Console IPAM ネットワークを作成するには、Infoblox 上に同じ CIDR IP 範囲を持つネットワークが存在する必要があります。

NetScaler Console 内で IPAM ネットワークを作成する場合、Console 内での Infoblox ネットワークの使用を登録するだけです。NetScaler Console は Infoblox と連携して、ネットワークから割り当てられた IP アドレスを管理します。Infoblox ネットワークは、NetScaler Console の外部でも引き続き使用できます。

同様に、NetScaler Console IPAM ネットワークを削除すると、NetScaler Console は Infoblox ネットワークの登録を解除します。これは、NetScaler Console がそのネットワークでの IP アドレス管理のために Infoblox と連携しなくなることを意味します。

#### Infoblox DDI のアプリケーションプログラミングインターフェース

NetScaler Console IPAM は、次の Infoblox API を使用して、それぞれのアクションを実行します。

- (/network) - 利用可能なすべての Infoblox ネットワークを一覧表示します
- (/network?network={id}) - 特定の Infoblox ネットワークの詳細を取得します
- (/ipv4address) - Infoblox ネットワーク上のすべての IP を一覧表示します
- (/record:host) - 特定の IP アドレスの詳細を取得します
- (/{IP}) - Infobloxネットワーク上のIPを予約および解放します

Infoblox APIの詳細については、Infoblox DDIで入手できるInfoblox REST APIリファレンスガイドを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# ネットワークを追加する

NetScaler Consoleで管理される構成でIPAMを使用するためにネットワークを追加します。

1. **Settings > IPAM**に移動します。
2. **Networks**の下で、**Add**をクリックします。
3. 以下の詳細を指定します。

   - **Network Name** - NetScaler Consoleでネットワークを識別するためのネットワーク名を指定します。
   - **Provider** - リストからプロバイダーを選択します。

     このリストには、NetScaler Consoleに追加されたプロバイダーが表示されます。
   - **Network Type** - 要件に基づいて、リストから**IP range**または**CIDR**を選択します。
   - **Network Value** - ネットワーク値を指定します。

     **注記:**

     NetScaler Console IPAMはIPv4アドレスのみをサポートしています。

     **IP range**の場合、ネットワーク値を次の形式で指定します。

     ```
     <first-IP-address>-<last-IP-address>
     ```

     例:

     ```
     10.0.0.20-10.0.0.100
     ```

     **CIDR**の場合は、次の形式でネットワーク値を指定します:

     ```
     <IP-address>/<subnet-mask>
     ```

     例:

     ```
     10.70.124.0/24
     ```

4. **作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 割り当てられたIPアドレスを表示する

IPAMネットワークから割り当てられたIPアドレスの詳細を表示するには、次の手順を実行します:

1. **設定 > IPAM**に移動します。
2. **ネットワーク**タブで、**すべての割り当て済みIPを表示**をクリックします。

   このペインには、IPアドレス、プロバイダー名、プロバイダーベンダー、および説明が表示されます。また、このIPアドレスを予約したリソースの詳細も表示されます:

   - **モジュール**: IPアドレスを予約したNetScaler Consoleモジュールが表示されます。たとえば、StyleBooksがIPアドレスを予約した場合、この列にはモジュールとしてStyleBooksが表示されます。
   - **リソースタイプ**: そのモジュール内のリソースタイプが表示されます。StyleBooksモジュールの場合、構成リソースタイプのみがIPAMネットワークを使用します。そのため、この列には「構成」と表示されます。
   - **リソースID**: リンク付きの正確なリソースIDが表示されます。このリンクをクリックすると、IPアドレスを使用しているリソースにアクセスできます。構成リソースタイプの場合、構成パックIDがリソースIDとして表示されます。

**注:**

IPアドレスを解放する場合は、解放するIPアドレスを選択し、**割り当て済みIPを解放**をクリックします。

# アプリケーションイベント通知を受信するためのアクションポリシーを構成する

既存のアプリケーションイベントの分析ビューとは別に、アクションポリシーを構成して、Slack、Eメール、PagerDuty、またはServiceNowを介してアプリケーションイベント通知を受け取ることができます。アプリケーションイベントには、パフォーマンスの問題、ボットおよびWAF違反、サービスグラフ違反が含まれます。管理者として、アクションポリシーを使用すると、イベント通知をリアルタイムで受け取ることができます。

アクションポリシーを使用すると、次のことができます。

- アプリケーションイベントの特定の条件を事前定義する。
- Slack、Eメール、PagerDuty、およびServiceNowを介して、以下のイベントの通知を受け取る。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| イベントカテゴリ | イベントサブカテゴリ | イベント |
| --- | --- | --- |
| セキュリティ違反 | すべてのセキュリティ違反 | すべてのボット違反（ボット違反のリストの詳細については、「違反カテゴリ」を参照してください）。 |
| | | すべてのWAF違反（WAF SQL違反、WAF XSS違反、WAF Infer XML違反） |
| | クライアントごとのすべてのセキュリティ違反 | クライアントごとのボット違反 |
| | | クライアントごとのWAF違反 |
| | | **注:** WAF違反通知を受信するには、最小違反トランザクションは20%である必要があります。たとえば、100トランザクションのうち、最低20は違反トランザクションである必要があります。 |
| アプリケーションパフォーマンス | | アプリスコア違反 |
| | | クライアントネットワーク遅延 |
| | | サーバーネットワーク遅延 |
| | | サーバー処理時間 |
| | | 応答時間 |
| | | リクエスト |
| | | 帯域幅 |
| | | サービスグラフ違反 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| イベントカテゴリ | イベントサブカテゴリ | イベント |
|---|---|---|
| アプリケーション使用状況 | | 1秒あたりのリクエスト数 |
| | | スループット |
| | | データ量 |

## アクションポリシーの構成

1. 「**Settings > Action > Action Policies**」に移動します。
2. 「**Add**」をクリックします。
3. 「**Create Action Policy**」ページで、次のように設定します。

   a. **ポリシー名** – 任意のポリシー名を入力します。

   b. **有効** – このオプションはデフォルトで選択されています。

   c. **次のイベントが発生した場合** – リストからイベントを選択します。

   d. **次の条件が満たされた場合** – リストから、通知を受けたい条件を定義するために選択します。**+** をクリックして条件を追加できます。条件を削除するには、**–** をクリックします。

   次の演算子を使用してアクションポリシーを設定できます。演算子は、選択した条件に基づいて表示されます。

| 演算子 | 説明 |
|---|---|
| 等しい | 定義された値と等しい |
| 等しくない | 定義された値と等しくない |
| より大きい | 定義された値より大きい |
| 以上 | 定義された値以上 |
| 未満 | 定義された値より小さい |
| 以下 | 定義された値以下 |
| 含む | 定義された用語または値を含む |
| で始まる | 定義された用語または値で始まる |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 演算子 | 説明 |
| --- | --- |
| で終わる | 定義された用語または値で終わる |
| IN | 複数の値を選択できます |

e. **次に以下を実行** – 「**通知**」を選択します。「**通知**」を選択すると、「通知タイプ」オプションが表示されます。

f. **通知タイプ** – 通知タイプとして、Email、Slack、PagerDuty、またはServiceNowを選択します。選択した通知タイプに応じて、対応するオプション（配布リスト、Slackプロファイル、PagerDutyプロファイル、またはServiceNowプロファイル）が表示されます。リストからプロファイルを選択します。

新しいプロファイルを作成する場合は、「**追加**」をクリックします。

g. 「**ポリシーの作成**」をクリックします。

ポリシーが構成されました。構成されたポリシーの詳細を表示できます。

ポリシーを構成した後、ポリシーを選択して以下をクリックできます。

- アクションポリシーを更新または変更するには、「**編集**」をクリックします。更新後、「ポリシーの更新」をクリックします。
- アクションポリシーを削除するには、「**削除**」をクリックします。複数のポリシーを選択し、「**削除**」をクリックして削除できます。
- 時間、実行されたアクション、ポリシー名、アラートタイプ、アラートメッセージなどの詳細を表示するには、「**アクション履歴**」をクリックします。

次の表に、アクションポリシー構成の詳細を示します。

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| **すべてのセキュリティ違反** | インスタンスIP | NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。 |
| | 違反数 | 通知を受け取りたい違反数。たとえば、違反数を10以下に設定した場合、ボット違反ト |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | | ランザクションが10以下で受信されると通知されます。 |
| | 違反率 | この値は、特定のトランザクションからの合計違反数を示し、値は0から1の間でなければなりません。たとえば、100件のトランザクションのうち20件が違反であり、そのようなシナリオで通知を受け取りたい場合は、0.2を入力する必要があります。 |
| **すべてのボット違反** | ボットプロファイル | NetScalerインスタンスでボット管理を設定するために使用されるボットプロファイル名。 |
| | インスタンスIP | NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。 |
| | 違反数 | 通知を受け取りたい違反数。たとえば、違反数を10以下に設定した場合、ボット違反トランザクションが10以下で受信されると通知されます。 |
| | 違反率 | この値は、特定のトランザクションからの合計違反数を示し、値は0から1の間でなければなりません。たとえば、100件のトランザクションのうち20件が違反であり、そのようなシナリオで通知を受け取りたい場合は、0.2を入力する必要があります。 |
| **すべてのWAF違反、WAF SQL違反、WAF XSS違反、WAF推論XML違反** | WAFプロファイル | NetScalerインスタンスでWAFセキュリティ設定を構成 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | | するために使用されるWAFプロファイル名。 |
| | インスタンスIP | NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。 |
| | 違反数 | 通知を受けたい違反数。WAF違反の通知を受けるための最低要件は20%です。 |
| | 違反率 | この値は、特定のトランザクションからの合計違反数を示し、値は0から1の間でなければなりません。たとえば、100件のトランザクションのうち20件がWAF SQL違反トランザクションであり、そのようなシナリオで通知を受けたい場合は、0.2を入力する必要があります。 |
| **クライアントごとのすべてのセキュリティ違反** | アプリケーション名 | カスタムアプリケーション名。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。 |
| | インスタンスIP | NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。 |
| | クライアントIP | ボットの発生元。IPアドレスを指定します。 |
| | 合計攻撃数 | 通知を受け取りたい合計攻撃数。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | リクエストURL | ブロックするように構成したいURL。URLを指定します。 |
| | 仮想サーバー名 | カスタムアプリケーション用に構成された関連アプリケーション。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。 |
| **クライアントごとのボット違反** | アプリケーション名 | カスタムアプリケーション名。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。 |
| | インスタンスIP | NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。 |
| | クライアントIP | ボットの発生元。IPアドレスを指定します。 |
| | 合計攻撃数 | 通知を受け取りたい攻撃の合計数。 |
| | 違反タイプ | リストからボット違反を選択します。 |
| | リクエストURL | ブロックするように構成したいURL。URLを指定します。 |
| | 仮想サーバー名 | カスタムアプリケーション用に構成された関連アプリケーション。リストからアプリケーションを選択します。この条件を追加しない場合、 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | | NetScalerインスタンスのすべてのアプリケーションが考慮されます。 |
| **クライアントごとのWAF違反** | アプリケーション名 | カスタムアプリケーション名。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。 |
| | インスタンスIP | NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。 |
| | クライアントIP | ボットの発生元。IPアドレスを指定します。 |
| | 総攻撃数 | 通知を受け取りたい攻撃の総数。 |
| | 違反タイプ | リストからWAF違反を選択します。 |
| | リクエストURL | ブロックするように設定したいURL。URLを指定します。 |
| | 仮想サーバー名 | カスタムアプリケーション用に構成された関連アプリケーション。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。 |
| **アプリスコア違反** | パフォーマンスインジケーター | アプリスコアコンポーネントとそのしきい値。リストからアプリスコアコンポーネントを選択します。詳細については、「アプリスコアコンポー |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | | ネントを選択してしきい値を設定する」を参照してください。 |
| | 違反回数 | 通知を受け取りたい違反回数。たとえば、応答時間に対して違反回数を5に設定した場合、応答時間のしきい値が5回違反したときに通知を受け取ります。 |
| | アプリケーション名 | **アプリケーションの選択**をクリックして、違反通知を受け取りたいアプリケーションを選択します。 |
| **クライアントネットワーク遅延** | クライアントネットワーク平均遅延 | 通知を受け取りたいクライアント遅延（クライアントからNetScalerまで）の値をミリ秒単位で指定します。 |
| | クライアントネットワーク遅延異常 | 通知を受け取りたいネットワーク遅延の異常数を指定します。 |
| | アプリケーション名 | 違反の通知を受け取りたいアプリケーションを選択するには、**Select Applications** をクリックします。 |
| **サーバーネットワーク遅延** | サーバーネットワーク平均遅延 | 通知を受け取りたいサーバー遅延（サーバーからNetScalerまで）の値をミリ秒単位で指定します。 |
| | サーバーネットワーク遅延異常 | 通知を受け取りたいネットワーク遅延の異常数を指定します。 |
| | アプリケーション名 | 違反の通知を受け取りたいアプリケーションを選択するに |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | | は、**Select Applications** をクリックします。 |
| **応答時間** | 応答平均時間 | 通知を受けたい値（ミリ秒単位）を指定します。 |
| | 応答平均時間の異常 | 通知を受けたい異常カウントを指定します。 |
| | アプリケーション名 | **アプリケーションの選択**をクリックして、通知を受けたいアプリケーションを選択します。アプリケーションを選択しない場合、すべてのアプリケーションに適用されます。 |
| **リクエスト** | 合計リクエスト | 通知を受けたい合計リクエスト数を指定します。 |
| | アプリケーション名 | **アプリケーションの選択**をクリックして、通知を受けたいアプリケーションを選択します。アプリケーションを選択しない場合、すべてのアプリケーションに適用されます。 |
| **帯域幅** | 合計帯域幅 | 通知を受けたい帯域幅（MB）を指定します。 |
| | アプリケーション名 | **アプリケーションの選択**をクリックして、通知を受けたいアプリケーションを選択します。アプリケーションを選択しない場合、すべてのアプリケーションに適用されます。 |
| **サーバー処理時間** | サーバー処理平均時間 | 通知を受け取りたいサーバー処理（サーバーからNetScalerへ）の値をミリ秒単位で指定します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | サーバー処理時間の異常 | 通知を受け取りたいサーバー処理時間の異常数を指定します。 |
| | アプリケーション名 | **アプリケーションの選択**をクリックして、違反の通知を受け取りたいアプリケーションを選択します。 |
| **サービスグラフ違反** | | 設定されたしきい値を超えるマイクロサービス。詳細については、「サービスグラフでしきい値を構成する」を参照してください。 |
| **1秒あたりのリクエスト数** | 1秒あたりのリクエスト数（平均） | アプリケーションが1秒あたりに受信するリクエスト数。通知を受け取るには、平均値を指定します。 |
| | 1秒あたりのリクエスト数（平均）の異常 | 通知を受け取りたい平均異常数を指定します。 |
| | | **注:** このイベントにAND条件を使用している場合、1秒あたりのリクエスト数（平均）とアプリケーション名、または1秒あたりのリクエスト数（異常平均）とアプリケーション名のいずれかを構成できます。 |
| | アプリケーション名 | 違反通知を受け取りたいアプリケーションを選択するには、**[アプリケーションの選択]** をクリックします。 |
| **スループット** | スループット平均 | 特定の期間に送信されたデータの合計。通知を受け取る平均値 (MB単位) を指定します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 違反名 | 条件 | 説明 |
| --- | --- | --- |
| | スループット平均異常 | 通知を受け取りたい平均異常数を指定します。 |
| | | **注:** このイベントにAND条件を使用している場合、スループット平均とアプリケーション名、またはスループット平均異常とアプリケーション名のいずれかを設定できます。 |
| | アプリケーション名 | 違反通知を受け取りたいアプリケーションを選択するには、**[アプリケーションの選択]** をクリックします。 |
| **データ量** | 総データ量 | 特定の期間に転送されるデータの合計。通知を受け取る値 (MB単位) を指定します。 |
| | データ量異常 | 通知を受け取りたい異常数を指定します。 |
| | | **注:** このイベントにAND条件を使用している場合、[Total Data Volume]と[Application Name]、または[Data Volume Anomalies]と[Application Name]のいずれかを設定できます。 |
| | アプリケーション名 | **[Select Applications]** をクリックして、違反通知を受け取りたいアプリケーションを選択します。 |

## 検索バーを使用する

検索バーを使用すると、結果をフィルタリングできます。検索バーをクリックすると、検索候補のリストが表示されます。コンポーネントを選択し、要件に基づいて結果をフィルタリングできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクションポリシー検索バー(/en-us/netscaler-application-delivery-management-software/media/awp-search.png)

### 監査ログオプションを使用する

をクリックし、リストから期間を選択して、選択した期間に作成、変更、削除されたアクションポリシーを表示し、 をクリックします。

**注**

データストレージポリシーは、今後のリリースで変更される予定です。これらの変更により、ストレージ制限を超過した履歴データを保存できなくなります。現時点では、ストレージを追加するか、ライセンスエンタイトルメントの制限内にストレージを維持することをお勧めします。

## 可観測性統合

最新のアプリケーションの複雑さが増しているため、管理者は次の課題に直面しています。

- アプリケーションの監視とトラブルシューティング。
- インフラストラクチャとアプリケーションの動作を可視化する。

可観測性は、インフラストラクチャ全体にわたるこれらのインサイトを提供することで、このギャップを埋めます。NetScaler Console の可観測性統合機能を使用すると、次のことができます。

- NetScaler Console を Splunk と統合する(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/security/splunk-integration.html)。
- NetScaler Console を New Relic と統合する(/ja-jp/netscaler-application-delivery-management-software/current-release/analytics/security/new-relic-integration.html)。
- デフォルトスキーマを使用して、インサイトを Prometheus にエクスポートするように NetScaler インスタンスを構成する(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/netscaler-prometheus-integration.html)。

### Splunkとの統合

NetScaler ConsoleをSplunkと統合して、以下の分析を表示できるようになりました。

- WAF違反
- ボット違反

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSL証明書のインサイト
- ゲートウェイのインサイト
- イベントとメトリック
- HDX™インサイト
- NetScaler® Console監査ログ

Splunkアドオンを使用すると、次のことが可能になります。

- 他のすべての外部データソースを結合します。
- 分析の可視性を一元的に高めます。

NetScaler Consoleは、ボット、WAF、SSLイベントを収集し、定期的にSplunkに送信します。Splunk Common Information Model (CIM) アドオンは、イベントをCIM互換データに変換します。管理者として、CIM互換データを使用して、Splunkダッシュボードでイベントを表示できます。

統合を成功させるには、次のことを行う必要があります。

- SplunkがNetScaler Consoleからデータを受信するように構成する
- NetScaler Consoleを構成してSplunkにデータをエクスポートする
- Splunkでダッシュボードを表示する

### Splunkを構成して、オンプレミスのNetScaler Consoleからデータを受信する

Splunkでは、次の操作を行う必要があります。

1. Splunk HTTPイベントコレクターエンドポイントをセットアップし、トークンを生成する
2. Splunk Common Information Model (CIM) アドオンをインストールする
3. CIMノーマライザーをインストールする（WAFおよびボットインサイトにのみ適用）
4. Splunkでサンプルダッシュボードを準備する

#### Splunk HTTPイベントコレクターエンドポイントをセットアップし、トークンを生成する

まず、SplunkでHTTPイベントコレクターをセットアップする必要があります。このセットアップにより、NetScaler ConsoleとSplunk間の統合が可能になり、データが送信されます。次に、Splunkでトークンを生成して、次の操作を行う必要があります。

- NetScaler ConsoleとSplunk間の認証を有効にします。
- イベントコレクターエンドポイントを介してデータを受信します。

1. Splunkにログオンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Settings > Data Inputs > HTTP event collector** に移動し、**Add new** をクリックします。
3. 次のパラメーターを指定します。
    a. **名前**：任意の名前を指定します。
    b. **ソース名の上書き（オプション）**：値を設定すると、HTTPイベントコレクターのソース値が上書きされます。
    c. **説明（オプション）**：説明を指定します。
    d. **出力グループ（オプション）**：デフォルトでは、このオプションは「なし」として選択されています。
    e. **インデクサーの確認を有効にする**：NetScaler Consoleはこのオプションをサポートしていません。このオプションを選択しないことをお勧めします。

    イベントコレクターのパラメーター(/en-us/netscaler-application-delivery-management-software/media/splunk-event-collector-parameter.png)
4. **次へ**をクリックします。
5. オプションで、**入力設定**ページで追加の入力パラメーターを設定できます。
6. **レビュー**をクリックしてエントリを確認し、**送信**をクリックします。

    トークンが生成されます。NetScaler Consoleで詳細を追加する際に、このトークンを使用する必要があります。

    Splunkトークン(/en-us/netscaler-application-delivery-management-software/media/splunk-token.png)

### Splunk共通情報モデルをインストールする

Splunkでは、Splunk CIMアドオンをインストールする必要があります。このアドオンにより、NetScaler Consoleから受信したデータが正規化され、同等のイベントに対して同じフィールド名とイベントタグを使用して共通の標準に一致することが保証されます。

**注**

Splunk CIMアドオンをすでにインストールしている場合は、この手順をスキップできます。

1. Splunkにログオンします。
2. **Apps > Find More Apps**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Splunkのその他のアプリを検索(/en-us/netscaler-application-delivery-management-software/media/splunk-find-apps.png)

3. 検索バーに「**CIM**」と入力し、**Enter**キーを押して**Splunk Common Information Model (CIM)**アドオンを取得し、**Install**をクリックします。

   スプランク CIM(/en-us/netscaler-application-delivery-management-software/media/splunk-cim.png)

### CIMノーマライザーをインストールする

CIMノーマライザーは、SplunkでWAFとボットのインサイトを表示するためにインストールする必要がある追加のプラグインです。

1. Splunkポータルで、**Apps > Find More Apps**に移動します。

   Splunkのその他のアプリを検索(/en-us/netscaler-application-delivery-management-software/media/splunk-find-apps.png)

2. 検索バーに**NetScaler Consoleサービスイベント/データ用CIM正規化**と入力し、**Enter**を押してアドオンを取得し、**Install**をクリックします。

   CIMノーマライザー(/en-us/netscaler-application-delivery-management-software/media/splunk-cim-normalizer.png)

### Splunkでサンプルダッシュボードを準備する

Splunk CIMをインストールしたら、WAFとボット、SSL証明書のインサイト、イベントとメトリクス用のテンプレートを使用してサンプルダッシュボードを準備する必要があります。ダッシュボードテンプレート (`.tgz`) ファイルをダウンロードし、任意のエディター (メモ帳など) を使用してその内容をコピーし、Splunkにデータを貼り付けてダッシュボードを作成できます。

**注：**

サンプルダッシュボードを作成する以下の手順は、すべてのユースケースに適用できます。必要な`json`ファイルを使用する必要があります。

1. Citrixダウンロードページにログオンし、3rd party Endpoints用サンプルダッシュボードから入手できるサンプルダッシュボードをダウンロードします。
2. ファイルを解凍し、任意のテキストエディタで`json`ファイルを開き、ファイルからデータをコピーします。

   解凍後、3つの`json`ファイルが取得されます。以下を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `adm_splunk_security_violations.json`ファイルを使用してWAFおよびBotサンプルダッシュボードを作成します。
- `adm_splunk_ssl_certificate.json`ファイルを使用してSSL証明書インサイトサンプルダッシュボードを作成します。
- `adm_splunk_events_and_metrics_history.json`ファイルを使用してNetScaler Consoleイベントおよびメトリックダッシュボードを作成します。

3. Splunkポータルで、**Search & Reporting > Dashboards**に移動し、**Create New Dashboard**をクリックします。



4. **Create New Dashboard**ページで、次のパラメータを指定します。
   a. **ダッシュボードのタイトル** - 任意のタイトルを指定します。
   b. **説明** - 必要に応じて、参照用に説明を指定できます。
   c. **権限** - 要件に基づいて、**Private**または**Shared in App**を選択します。
   d. **Dashboard Studio**を選択します。
   e. いずれかのレイアウト（**Absolute**または**Grid**）を選択し、**Create**をクリックします。



**Create** をクリックした後、レイアウトから **Source** アイコンを選択します。



5. 既存のデータを削除し、ステップ2でコピーしたデータを貼り付けて、**Back** をクリックします。
6. **Save** をクリックします。

   サンプルダッシュボードを表示できます。

   以下は、WAFおよびボットのサンプルダッシュボードの例です。



### NetScaler Consoleオンプレミスを構成してSplunkにデータをエクスポートする

これでSplunkの準備がすべて整いました。最後のステップは、サブスクリプションを作成し、トークンを追加してNetScaler Consoleを構成することです。

以下の手順を完了すると、NetScaler Consoleで現在利用可能な更新されたダッシュボードをSplunkで表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleにログオンします。
2. **Settings > Observability Integration** に移動します。
3. **Integrations** ページで、**Add** をクリックします。
4. **Create Subscription** ページで、以下の詳細を指定します。

    a. **Subscription Name** フィールドに任意の名前を指定します。

    b. **NetScaler Console** を **Source** として選択し、**Next** をクリックします。

    c. **Splunk** を選択し、**Configure** をクリックします。**Configure Endpoint** ページで:

        i. **エンドポイントURL** – Splunkエンドポイントの詳細を指定します。エンドポイントは `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>` 形式である必要があります。

        > **注:**
        >
        > セキュリティ上の理由から、HTTPSを使用することをお勧めします。

        - **SPLUNK_PUBLIC_IP** – Splunk用に構成された有効なIPアドレス。
        - **SPLUNK_HEC_PORT** – HTTPイベントエンドポイント構成時に指定したポート番号を示します。デフォルトのポート番号は8088です。
        - **Services/collector/event** – HECアプリケーションのパスを示します。

        ii. **認証トークン** – Splunkから認証トークンをコピーして貼り付けます。

        iii. **Submit** をクリックします。

    d. **Next** をクリックします。

    e. **Add Insights** をクリックし、**Select Feature** タブで、エクスポートする機能を選択して **Add Selected** をクリックします。

    > **注:**
    >
    > **NetScaler Console Audit Logs** を選択した場合、Splunkに監査ログをエクスポートする頻度として、**Daily** または **Hourly** を選択できます。

    f. **Next** をクリックします。

    g. 「**インスタンスの選択**」タブで、「**すべてのインスタンスを選択**」または「**カスタム選択**」のいずれかを選択し、「**次へ**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**すべてのインスタンスを選択**」 - すべてのNetScalerインスタンスからSplunkにデータをエクスポートします。
- 「**カスタム選択**」 - リストからNetScalerインスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択されたNetScalerインスタンスからのみSplunkにエクスポートされます。

h. 「**送信**」をクリックします。

**注:**

選択されたインサイトのデータは、NetScaler Consoleで違反が検出された直後にSplunkにプッシュされます。

### Splunkでダッシュボードを表示

NetScaler Consoleでの設定が完了すると、データはNetScaler Consoleからエクスポートされ、イベントがSplunkに表示されます。

追加の手順なしで、Splunkで更新されたダッシュボードを表示する準備が整いました。

Splunkに移動し、作成したダッシュボードをクリックして、更新されたダッシュボードを表示します。

以下は、更新されたWAFおよびBotダッシュボードの例です。

以下のダッシュボードは、更新されたSSL証明書インサイトダッシュボードの例です。

以下のダッシュボードは、更新されたイベントおよびメトリックダッシュボードの例です。

**注記：**

メモリ、CPU、ディスクの使用状況データは、NetScaler Consoleからの現在の値を示します。これらの値の上下の傾向は、5分ごとの以前の値との比較に基づいて表示されます。

イベントダッシュボード(/en-us/netscaler-application-delivery-management-software/media/splunk-updated-events_dashboard.png)

ダッシュボードとは別に、サブスクリプションを作成した後、Splunkでデータを表示することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Splunkで、**Search & Reporting**をクリックします。
2. 検索バーで：

   - `sourcetype="metrics"`と入力し、リストから期間を選択して、NetScaler Consoleのメトリックデータを表示します。
   - `sourcetype="event"`と入力し、リストから期間を選択して、NetScaler Consoleのイベントデータを表示します。
   - `sourcetype="bot"`または`sourcetype="waf"`と入力し、リストから期間を選択して、ボット/WAFデータを表示します。
   - `sourcetype="ssl"`と入力し、リストから期間を選択して、SSL証明書のインサイトデータを表示します。
   - `sourcetype="gateway_insights"`と入力し、リストから期間を選択して、Gatewayインサイトデータを表示します。
   - `sourcetype="hdx_insights"`と入力し、リストから期間を選択して、Gatewayインサイトデータを表示します。
   - `sourcetype= "audit_logs"`と入力し、リストから期間を選択して、監査ログデータを表示します。

## New Relic との統合

NetScaler Console を New Relic と統合して、WAF、Bot、SSL、Gateway Insights、および NetScaler Console の監査ログの分析を New Relic ダッシュボードで表示できるようになりました。この統合により、次のことが可能になります。

- New Relic ダッシュボード内の他のすべての外部データソースを結合します。
- 分析を一元的に可視化します。

NetScaler Console は Bot および WAF イベントを収集し、選択に応じてリアルタイムまたは定期的に New Relic に送信します。管理者として、New Relic ダッシュボードで Bot および WAF イベントを表示することもできます。

### 前提条件

統合を成功させるには、次のことを行う必要があります。

- 次の形式で New Relic イベントエンドポイントを取得します。

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イベントエンドポイントの設定の詳細については、New Relic ドキュメントを参照してください。

アカウント ID の取得の詳細については、New Relic ドキュメントを参照してください。

- New Relic キーを取得します。詳細については、New Relic ドキュメントを参照してください。
- NetScaler Console にキーの詳細を追加します

**NetScaler Console にキーの詳細を追加します**

トークンを生成したら、New Relic と統合するために NetScaler Console に詳細を追加する必要があります。

1. NetScaler Console にログオンします。
2. **設定 > 可観測性統合**に移動します。
3. **統合**ページで、**追加**をクリックします。
4. **サブスクリプションの作成**ページで、次の詳細を指定します。
   a. **サブスクリプション名**フィールドに任意の名前を指定します。
   b. **ソース**として **NetScaler® Console** を選択し、**次へ**をクリックします。
   c. **New Relic** を選択し、**構成**をクリックします。**エンドポイントの構成**ページで:
      i. **エンドポイント URL** – New Relic エンドポイントの詳細を指定します。エンドポイントは `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` 形式である必要があります。

      **注**

      セキュリティ上の理由から、HTTPS を使用することをお勧めします。

   d. **認証トークン** – New Relic から認証トークンをコピーして貼り付けます。
      i. **送信**をクリックします。
   e. **次へ**をクリックします。
   f. **インサイトの追加**をクリックし、**機能の選択**タブで、エクスポートする機能を選択して**選択した項目を追加**をクリックします。
   g. **次へ**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

h. 「**インスタンスの選択**」タブで、「**すべてのインスタンスを選択**」または「**カスタム選択**」のいずれかを選択し、「**次へ**」をクリックします。

- **すべてのインスタンスを選択** - すべてのNetScalerインスタンスからNew Relicにデータをエクスポートします。
- **カスタム選択** - リストからNetScalerインスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択したNetScalerインスタンスからのみNew Relicにエクスポートされます。

i. 「**送信**」をクリックします。

> **注:**
>
> 選択したインサイトのデータは、NetScaler Consoleで違反が検出された直後にNew Relicにプッシュされます。

設定が完了しました。「**サブスクリプション**」ページで詳細を表示できます。

サブスクリプションページ(/en-us/netscaler-application-delivery-management-software/media/new-relic-subscriptions.png)

### New Relicダッシュボード

イベントがNew Relicにエクスポートされると、「**メトリックとイベント**」の下で、次のJSON形式でイベントの詳細を表示できます。

`<subsription_name>_adm_<event name>` イベント名には、Bot、WAFなどが指定できます。

次の例では、ADMSTAGINGは`<subscription_name>`で、botは`<event_name>`です。

ダッシュボード(/en-us/netscaler-application-delivery-management-software/media/new-relic-example.jpg)

JSONデータがNew Relicダッシュボードに取り込まれると、管理者としてNRQL (New Relic Query Language) を使用し、取り込まれたデータに関するクエリを構築することで、選択に基づいてファセットとウィジェットを含むカスタムダッシュボードを作成できます。詳細については、`https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`を参照してください。

以下は、NRQLを使用して作成されたダッシュボードの例です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このダッシュボードを作成するには、以下のクエリが必要です。

- ウィジェット 1: イベントテーブル内の合計ユニーク攻撃数

  ```
  SELECT count(total_attacks) from <event_name> since 30 days ago
  ```

- ウィジェット 2: イベントテーブル内のユニークなトランザクション ID

  ```
  SELECT uniqueCount(transaction_id) from <event_name> since 30 days ago
  ```

- ウィジェット 3: 合計ユニークボットタイプとそのカウント

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago
  ```

- ウィジェット 4: ボット違反を検出した合計ユニークアプリ名

  ```
  SELECT uniques(appname) from <event_name> since 30 days ago
  ```

## Microsoft Sentinel との統合

NetScaler Console から Microsoft Sentinel に次の分析データをエクスポートするために、NetScaler Console を Microsoft Sentinel と統合できます。

- WAF 違反
- Bot 違反
- SSL 証明書のインサイト
- ゲートウェイのインサイト
- メトリックとイベント
- NetScaler® Console の監査ログ

Microsoft Sentinel は、アプリケーション、サーバーなど、さまざまなソースからデータを収集する一元化されたデータ収集機能を提供します。管理者として、Microsoft Sentinel でインサイトや違反が報告された後、データを表示して意思決定を行うことができます。

統合を成功させるには、アクティブな Azure サブスクリプションがあることを確認し、各セクションの手順に従ってください。

### Log Analytics ワークスペースを構成する

収集されたデータを保存および分析するには、Log Analytics ワークスペースが必要です。

1. Azure にログインします。
2. **リソースの作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソース (/en-us/netscaler-application-delivery-management-software/media/sentinel-resource-create.png)

3. 検索バーに「log analytics workspace」と入力し、「**Log Analytics Workspace**」の下にある「**作成**」をクリックします。



4. 「**Log Analytics Workspace**」のメインページで、「**作成**」をクリックします。



5. 「**Log Analytics ワークスペースの作成**」で:

   a. アクティブなサブスクリプションとリソースグループを選択します。

   > **注:**
   >
   > 権限がある場合は、「**新規作成**」をクリックしてリソースグループを追加することもできます。

   b. 任意の名前を指定します。

   c. リストから地域を選択します。

   d. 「**確認 + 作成**」をクリックします。



   e. 検証成功メッセージが表示されます。「**作成**」をクリックしてワークスペースをデプロイします。



   f. デプロイの進行状況メッセージが表示されます。デプロイ完了メッセージが表示されたら、「**リソースに移動**」をクリックします。



   ワークスペースが正常に作成されました。

### Microsoft Entra アプリケーションを作成する

Log Analytics Workspace の代わりに通信するために、Azure サブスクリプションに関連付けられた Entra アプリケーションを作成する必要があります。アプリケーションを作成したら、**Microsoft Sentinel Contributor** ロールでアクセス許可を付与する必要もあります。アプリケーションは、**クライアント ID**、**テナント ID**、**クライアント シークレット**などの詳細も提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これらの詳細をメモしておくことをお勧めします。これらの詳細は、NetScaler Console でサブスクリプションを作成して統合プロセスを完了する際に必要になります。

1. Azure ポータルで、検索バーにキーワードを入力します。
2. **Microsoft Entra ID** をクリックします。



3. **追加** をクリックし、**アプリの登録** を選択します。



4. アプリの名前を指定し、**サポートされているアカウントの種類** で既定のオプションを選択し、**登録** をクリックします。



5. アプリケーションを登録した後:

   a. **クライアント ID** と **テナント ID** をメモします。



   b. アプリケーションのシークレット ID を作成します。**証明書とシークレット** をクリックし、**クライアント シークレット** で **新しいクライアント シークレット** をクリックします。説明と有効期間を指定し、**追加** をクリックしてアプリケーションのシークレット ID を作成します。



   c. アプリケーションの詳細が表示されます。シークレットが作成された直後に、**値**の下に表示されるIDを必ずメモしてください。他のGUIオプションに移動すると、この値は非表示になります。



### Microsoft Entra IDデータコネクタを使用してMicrosoft Sentinelにデータを送信する

Microsoft Entra IDログは、Entraテナントにアクセスするユーザー、アプリケーション、ネットワークに関する包括的な情報を提供します。詳細については、「Microsoft Entra IDデータコネクタを使用してMicrosoft Sentinelにデータを送信する」を参照してください。

## データ収集エンドポイントを構成する

エンドポイントURLを取得するには、データ収集エンドポイントを作成する必要があります。これは、NetScaler Consoleでサブスクリプションを作成する際に必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Azureポータルで、**Azureサービス**の下にある**データ収集エンドポイント**を選択するか、検索バーにキーワードを入力します。

   

2. **データ収集エンドポイント**ページで**作成**をクリックします。

   

3. **データ収集エンドポイントの作成**で:

   a. 任意のデータ収集エンドポイント名を指定します

   b. **サブスクリプション**、**リソースグループ**、および**リージョン**を選択します。

   c. **確認 + 作成**をクリックします。

   d. 「検証に成功しました」というメッセージが表示されたら、「**作成**」をクリックします。

エンドポイントURLをメモしておく必要があります。「**データ収集エンドポイント**」のメインページで、作成したエンドポイントを選択し、「**JSONビュー**」をクリックして、エンドポイントIDをメモします。

DCR ID(/en-us/netscaler-application-delivery-management-software/media/sentinel-dcr-id.png)

### データエクスポート用のテーブルを作成する

NetScaler ConsoleからMicrosoft Sentinelにエクスポートする各インサイトについて、テーブルを作成し、JSON情報を提供する必要があります。各インサイトのテーブル要件については、以下の詳細を参照してください。

| インサイト | 必要なテーブルの総数 |
|---|---|
| SSLインサイト | 3 |
| WAF | 1 |
| ボット | 1 |
| Gatewayインサイト | 5 |
| イベント | 1 |
| メトリック | 1 |
| 監査ログ | 1 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

各データ収集ルール (DCR) につき、最大 10 個のテーブルを作成できます。10 個を超えるテーブルを作成する場合は、別の DCR を作成する必要があります。

1. Azure ポータルでワークスペースに移動し、 の下にある をクリックします。
2. をクリックし、 を選択します。

   

3. で:

   a. テーブル名を指定します。テーブル名は **console_insightname** の形式である必要があります。例: **console_ns_sslvserver**、**console_ns_ssl_certkey**。各インサイトに適用されるテーブル名については、手順 4 を参照してください。

   b. テーブル名に関する詳細情報を追加するための説明を入力します。これはオプションです。

   c. 新しいデータ収集ルールを作成して追加します。

   d. リストからデータ収集エンドポイントを選択します。

      テーブルパラメータ(/en-us/netscaler-application-delivery-management-software/media/sentinel-table-parameters.png)

   e. **次へ**をクリックします。

4. 「**スキーマと変換**」タブで、エクスポートするインサイトのJSONサンプルログをアップロードする必要があります。各インサイトについて、以下のサンプルJSONを使用してアップロードするJSONファイルを作成できます。

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| SSL (1) | `{"id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name":` | console_ns_sslvserver |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite": "DISABLED", "skipclientcertpolicycheck": "", "tls13sessionticketsperauthcontext": 1, "cipherredirect": "DISABLED", "dropreqwithnohostheader": "NO", "sessionticketlifetime": -1, "maxage": 0, "pushenctrigger": "Always", | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "strictsigdigestcheck": "f", "sslredirect": "DISABLED", "sessionkeylifetime": -1, "alpnprotocol": "", "clientauthuseboundcachain": "", "sesstimeout": 120, "clientcert": "", "snihttphostmatch": "CERT", "preload": "NO", "prevsessionkeylifetime": -1, "sessionticketkeydata": "", "encrypttriggerpktcount": 45, "cleartextport": "", "ssliocspcheck": "", "hsts": "f", "sslinterception": "", "commonname": "", "sslireneg": "", "ocspstapling": "DISABLED", "quantumsize": 8192, "insertionencoding": "Unicode", "sslimaxsessperserver": -1, "cipherurl": "", "pushflag": 0, "zerorttearlydata": "DISABLED", "allowextendedmastersecret": "", "dhekeyexchangewithpsk": "NO", "clientauth": "DISABLED", "denysslreneg": "NONSECURE", | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "sendclosenotify": "YES", "dhcount": 0, "snienable": "DISABLED", "table_name": "ns_sslvserver"} | |
| SSL (2) | {"id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 | console_ns_ssl_certkey |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT ,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "no_of_bound_entities": 0, "partition_name": "", "display_name": "10.106.186.141", "hostname": "athulsadc", "key_name": "", "subjaltname": "", "managed_by": "", "certificate_dn": "", "linkcertkeyname": "", "table_name": "ns_ssl_certkey"} | |
| WAF | [{"ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, | console_af_threat_exporter _data_l2 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "violation_threat_index": 5, "app_threat_index": 5, "http_method": 0, "violation_action": 3, "violation_action_desc": "Blocked", "severity_type": 2, "severity_type_desc": "Medium", "iprep_score": 0, "iprep_category": 0, "counter_value": 0, | |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "appname": "vserver_1_10.106.185.156_lb", "violation_category": 12, "violation_category_desc": "Start URL", "source_ipv6_address": "", "true_client_ip": "\\N", "backend_vserver": "", "backend_appname": "", "transactionId": "0", "table_name": "af_threat_exporter_data_l2"}] | |
| ボット | {"ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": | console_af_bot_attack_details_l2 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"} | |
| ゲートウェイインサイト (1) | {"adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"} | console_af_vpn_error_details |
| ゲートウェイインサイト (2) | {"adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", | console_ns_vpnvserver |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"} | |
| ゲートウェイインサイト (3) | {"adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1} | console_af_vpn_session_details |
| ゲートウェイインサイト (4) | {"active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"} | console_af_vpn_active_session_1 |
| ゲートウェイインサイト (5) | {"adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports"} | console_af_vpn_error_reports |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| イベント | {"rpt_sample_time": -1, "category": "HealthMonitoring", "entity": "10.106.186.148:HealthMonitoring:System Disk Usage", "counter_threshold_value": "", "id": "0f2607cf-f97d-4f71-9162-11e580262e93", "timestamp": 1712927472, "message": "Disk Usage High: 63.24%", "severity": "Critical", "user_name": "", "device_entity_type": "", "device_type": "", "counter_actual_value": "", "cmd_auth_status": "", "source": "10.106.186.148", "history": "Update Time= Fri, 12 Apr 2024 06:32:49 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:27:46 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:22:44 UTC ,Previous Severity= Critical ,New Severity= Critical, | console_event |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:17:41 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:12:38 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:07:36 U", "config_cmd": "", "failureobj": "System Disk Usage", "operation_type": "undefined", "device_entity_name": "", "cmd_exec_status": "", "device_family": "", "source_event_id": -1, "source_system_ip": "10.106.186.148", "trap_id": 35, "table_name": "event"} | |
| メトリック | {"memory_free": 28830060544.0, "disk_used": 81248694272.0, "disk_free": 29632114688.0, "node_type": "", "memory_total": 34355544064.0, "cpu_usage": 0.49, | console_mps_health |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| インサイト | JSON | 使用するテーブル名 |
| --- | --- | --- |
| | `"disk_total": 120522616832.0, "disk_usage": 73.28, "node_id": "", "id": "1be15a09-d078-469c-868a-bfbfcffe5ef1", "disk_total_capacity": 0.0, "page_size": 4096.0, "memory_usage": 16.08, "table_name": "mps_health"}` | |
| 監査ログ | `{"system_gmt_time":1721868291, "source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage", "instance_ip":"X.X.X.X", "app_name":""}` | console_syslog_messages |

JSON をアップロードすると、次の詳細を表示できます。

- 「**Transformation editor**」をクリックし、適切なインサイトに適用できる次のクエリを入力し、「**Run**」をクリックして、NetScaler Console のポーリング時間からデータを承認します。

  - **SSL** - `source | extend TimeGenerated = todatetime(poll_time) | project-rename sslvserver_id = id`
  - **WAF** および **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
  - **ゲートウェイインサイト** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. **次へ** をクリックし、**作成** をクリックして完了します。
6. **データ収集ルール** に移動し、作成したDCRをクリックします。
7. **構成** の下で、**データソース** をクリックして、作成されたテーブルを表示します。



DCR (データ収集ルール) には、**Monitoring Metrics Publisher** ロールへのアクセスが必要です。

a. Azureポータルの **最近** の下からアクセスできるDCRに移動します。
b. DCRページから **アクセス制御 (IAM)** をクリックし、**ロールの割り当てを追加** をクリックします。



c. 検索バーに「monitor」と入力して **Monitoring Metrics Publisher** を選択し、**次へ** をクリックします。
d. **メンバー** タブで、**メンバーの選択** をクリックし、作成したEntraアプリを選択します。
e. **レビュー + 割り当て** をクリックします。

データ収集ルールIDをメモする必要があります。データ収集ルールページに移動し、DCRを選択して、JSONビューをクリックし、IDをメモします。



## NetScaler Consoleでサブスクリプションを作成する

これで準備が整いました。最後のステップは、サブスクリプションを作成し、必要な詳細を追加してNetScaler Consoleを設定することです。NetScaler Consoleでサブスクリプションを作成するには、メモした以下の詳細が必要です。

- エンドポイントURL
- データ収集ルールID
- テナントID
- クライアントID
- クライアントシークレット

1. NetScaler Consoleにログインします。
2. **設定 > 可観測性統合**に移動します。
3. **統合**ページで、**追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **サブスクリプションの作成**ページで、次の詳細を指定します。

   a. サブスクリプション名フィールドに任意の名前を指定します。

   b. **ソース**として**NetScaler Console**を選択し、**次へ**をクリックします。

   c. 「**Microsoft Sentinel**」を選択し、「**Configure**」をクリックします。「**Configure Endpoint**」ページで、すべての詳細を入力し、「**Submit**」をクリックします。

   d. 「**Next**」をクリックします。

5. 「**Add Insights**」をクリックし、「**Select Feature**」タブで、Microsoft Azureに追加したテーブルに応じて、エクスポートする機能を選択し、「**Add Selected**」をクリックしてから「**Next**」をクリックします。

6. 「**Select Instance**」タブで、「**Select All Instances**」または「**Custom select**」のいずれかを選択し、「**Next**」をクリックします。

   - **Select All Instances** - すべてのNetScalerインスタンスからMicrosoft Sentinelにデータをエクスポートします。
   - **Custom select** - リストからNetScalerインスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択したNetScalerインスタンスからのみMicrosoft Sentinelにエクスポートされます。

7. 「**Submit**」をクリックします。

### Microsoft Azureでログを表示する

すべての設定が完了したら、Microsoft Azureで詳細を表示するために30分ほど待つことをお勧めします。

1. Azureポータルで、「**Log Analytics Workspace**」に移動します。
2. 「**Logs**」をクリックし、テーブル名を入力して、「**Run**」をクリックして結果を表示します。

   ログを表示(/en-us/netscaler-application-delivery-management-software/media/sentinel-view-results.png)

ログを使用して構成のトラブルシューティングと検証を行うこともできます。たとえば、構成されたインサイトに対してNetScaler Console GUIの「Poll Now」オプションを使用し、次の手順を実行します。

1. SSHクライアントを使用してNetScaler Consoleにログインします。
2. 「shell」と入力してbashモードに入ります。
3. ログを表示するには、次のコマンドを使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
tail -f /var/mps/log/nbs/nbs_api.log
```

以下の例は、トラブルシューティングのために考えられるエラーを分析するのに役立ちます。

1. このログは、NetScaler Console (**Settings > Observability Integrations**) で Microsoft Sentinel サブスクリプションに無効なクライアント ID を指定したことを示しています。

   **回避策:** 正しいクライアント ID をコピーしたことを確認し、正しいクライアント ID を指定してサブスクリプションを編集してください。詳細については、Microsoft Entra アプリケーションを作成する を参照してください。

2. このログは、Microsoft Azure で必要な ssl_certkey テーブルが構成されていないことを示しています。

   **回避策:** Microsoft Azure で ssl_certkey のテーブルを構成してください。詳細については、データをエクスポートするテーブルを作成する を参照してください。

## デフォルトスキーマを使用して、Prometheus へのインサイトのエクスポートのために NetScaler® インスタンスを構成する

NetScaler は、メトリクスを Prometheus に直接エクスポートすることをサポートしています。NetScaler インスタンスが提供する豊富なメトリクスセットを使用して、NetScaler の健全性とアプリケーションの健全性を監視できます。たとえば、CPU とメモリの使用状況に関するメトリクスを収集して、NetScaler の健全性を把握できます。同様に、1 秒あたりの HTTP リクエスト数やアクティブなクライアント数などのメトリクスを使用して、アプリケーションの健全性を監視できます。

メトリクスを Prometheus にエクスポートするには、タイプが時系列である分析プロファイルを構成する必要があります。詳細については、「Prometheus を使用した NetScaler、アプリケーション、およびアプリケーションセキュリティの監視」を参照してください。

NetScaler Console のオブザーバビリティ統合機能を使用すると、デフォルトスキーマを使用して、Prometheus へのインサイトのエクスポートを構成できます。

1. **Settings > Observability Integration** に移動します。
2. **Integrations** ページで、**Add** をクリックします。
3. **Create Subscription** ページで、次の詳細を指定します。
   a. **Subscription Name** フィールドに任意の名前を指定します。
   b. **Source** として **NetScaler** を選択し、**Next** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 宛先として **Prometheus** を選択します。

d. エクスポートするデフォルトのインサイトには **Default** を選択します。

e. **Add Instances** をクリックし、Prometheus にインサイトをエクスポートするインスタンスを選択します。

f. **Submit** をクリックします。

### 失敗した構成のログを表示する

サブスクリプションを作成した後、**Settings > Observability Integration** で、作成したサブスクリプションのステータスを表示できます。ステータスが **Failed** と表示されている場合は、クリックして詳細を表示します。

失敗しました(/en-us/netscaler-application-delivery-management-software/media/observability-failed-config-status.png)

「**設定ジョブの詳細**」の下にある「**詳細を表示**」をクリックします。

詳細を表示(/en-us/netscaler-application-delivery-management-software/media/observability-failed-config-details.png)

問題の詳細を表示するには、「**ログを表示**」をクリックします。

ログ(/en-us/netscaler-application-delivery-management-software/media/observability-failed-config-logs.png)

## NetScaler®メトリックと監査ログのSplunkへのエクスポートを構成する

NetScalerは、メトリックのSplunkへのJSON形式での直接エクスポートをサポートしています。NetScalerは、アプリケーションの健全性とアプリケーションセキュリティの健全性を監視するための豊富なメトリックを提供します。NetScalerが提供するメトリックをSplunkにエクスポートすることで、メトリックを視覚化し、意味のあるインサイトを得ることができます。

監査ロギングを使用すると、NetScalerのさまざまなモジュールによって収集されたNetScalerの状態とステータス情報をログに記録できます。ログを確認することで、問題やエラーをトラブルシューティングして修正できます。

詳細については、以下を参照してください。

- NetScalerからSplunkへの監査ログの直接エクスポート
- NetScalerからSplunkへのメトリックの直接エクスポート

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleを介してメトリックと監査ログのSplunkへのエクスポートを構成するには：

1. **設定 > 可観測性統合**に移動します。
2. **統合**ページで、**追加**をクリックします。
3. **サブスクリプションの作成**ページで、次の詳細を指定します。

    a. **サブスクリプション名**フィールドに任意の名前を指定します。

    b. **ソース**として**NetScaler**を選択し、**次へ**をクリックします。

    c. **宛先**として**Splunk**を選択し、**構成**をクリックします。エンドポイントの構成：

    - **エンドポイントURL** - Splunkエンドポイントの詳細を指定します。エンドポイントは`https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event``形式である必要があります。
    - **認証トークン** - Splunkから認証トークンをコピーして貼り付けます。
    - 「**送信**」をクリックします。

    d. 「**次へ**」をクリックします。

    e. 「**インサイトの追加**」をクリックし、「**NetScalerメトリック**」と「**NetScaler監査ログ**」を選択して、「**選択した項目を追加**」をクリックします。

    f. 「**次へ**」をクリックします。

    g. 「**インスタンスの追加**」をクリックして、インスタンスを選択します。

    h. 「**送信**」をクリックします。

### 失敗した構成のログを表示

サブスクリプションを作成した後、作成したサブスクリプションのステータスを「**設定 > 可観測性統合**」で確認できます。ステータスが「**失敗**」と表示されている場合は、クリックして詳細を表示します。

「**構成ジョブの詳細**」の下にある「**詳細を表示**」をクリックします。

「**ログを表示**」をクリックして、問題の詳細を表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# アクセス制御リスト

アクセス制御リスト (ACL) は、ネットワークアプライアンスに適用して IP トラフィックをフィルタリングし、不正アクセスからアプライアンスを保護するための一連の条件です。

NetScaler Console GUI で ACL を構成して、NetScaler Console へのアクセスを制限および制御できます。NetScaler Console の ACL は、14.1-29.x ビルド以降でサポートされています。

## 使用ガイドライン

- NetScaler Console を 14.1-29.x ビルドにアップグレードすると、ACL 機能はデフォルトで無効になります。
- 管理者として、NetScaler Console の ACL を介して受信パケットのみを制御できます。
- NetScaler Console での構成は、既存の ACL 構成の変更を必要としません。

## ACL の構成方法

ACL の構成には以下が含まれます。

- ACL 機能を有効にする
- ACL ルールを作成する
- ACL ルールを有効にする

### ACL 機能を有効にする

1. NetScaler Console GUI にログオンし、**Settings > Access Control List (ACL)** に移動します。
2. トグルボタンを使用して、ACL 機能をオンにします。

   ACL有効化(/en-us/netscaler-application-delivery-management-software/media/acl-1.png)

### ACLルールを作成する

1. ACLページで、**ルールを作成**をクリックします。
2. **ルールを作成**ウィンドウで、次の表に記載されている詳細を追加します。

| オプション | 説明 |
| --- | --- |
| 名前 | 任意の名前を指定します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| オプション | 説明 |
| --- | --- |
| プロトコル | メニューからプロトコルを選択します。デフォルトでは、TCPが選択されています。すべてのプロトコルを許可するには、ANYを選択できます。 |
| 送信元IPアドレス/サブネット | ルールが適用される送信元IPアドレスまたは送信元サブネットを指定します。すべての受信トラフィックにルールを適用する必要がある場合は、ANYを選択します。 |
| 宛先IP | NetScaler ConsoleのIPアドレスは、宛先IPとして自動入力されます。このフィールドは編集できません。 |
| 宛先ポート | ルールが適用される宛先ポートを指定します。すべての宛先ポートにルールを適用する場合は、 を選択します。 |
| アクション | ルールの動作を選択します。許可または拒否です。 |
| 優先度 | ルールが評価される順序を指定するために優先度を割り当てます。優先度番号は、ACLルールが受信パケットと照合される順序を決定します。優先度番号が小さいほど優先度が高くなります。たとえば、優先度番号1は優先度番号2よりも優先度が高くなります。いずれのルールも受信パケットと一致しない場合、パケットはブロックされます。 |

3. ルールを作成するには、 をクリックします。

ルールが作成されると、無効な状態になります。ルールを有効にするには、ルールを有効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記：**

ルールを有効にするには、ACL機能が有効になっている必要があります。機能が無効な状態でACLルールを有効にしようとすると、「ACLが実行されていません」というメッセージが表示されます。

### ACLルールを有効にする

1. 有効にしたいルールにマウスを重ね、3つの点がある円をクリックします。
2. メニューから を選択します。
3. または、そのルールのラジオボタンを選択し、 タブをクリックします。
4. プロンプトが表示されたら、 をクリックして確認します。

## ACLルールのその他のアクション

ACLルールには、次のアクションを適用できます。

- ACLルールを無効にする
- ACLルールを編集する
- ACLルールを削除する
- ACLルールの優先順位を振り直す

### ACLルールを無効にする

1. 無効にするルールにマウスカーソルを合わせ、3つの点がある円を選択します。
2. リストから**Disable**をクリックします。
3. または、そのルールのラジオボタンを選択し、**Disable**ボタンをクリックします。
4. **Yes**をクリックして確定します。

**注：**

ルールを無効にすると、そのルールは受信トラフィックに適用されなくなります。ただし、ルールの設定はACL設定に残ります。

### ACLルールを編集する

1. 編集するルールにマウスカーソルを合わせ、3つの点がある円を選択します。
2. リストから**Edit Rule**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. または、そのルールのラジオボタンを選択し、**Edit Rule**ボタンをクリックします。
4. 編集を行い、**OK**をクリックします。

> **注:**
>
> 有効状態と無効状態の両方でルールを編集できます。すでに有効になっているルールを編集した場合、変更はすぐに適用されます。無効状態のルールの場合、変更はルールを有効にしたときに適用されます。

### ACLルールを削除する

1. ルールが無効状態であることを確認してください。有効状態のルールは削除できません。
2. 削除したいルールにマウスカーソルを合わせ、3つの点がある円を選択します。
3. リストから**Delete Rule**をクリックします。
4. または、そのルールのラジオボタンを選択し、**Delete Rule**ボタンをクリックします。
5. 確認のため、**Yes**をクリックします。

### ACLルールの優先順位を振り直す

1. 優先順位を振り直したいルールにマウスカーソルを合わせ、3つの点がある円を選択します。リストから**Renumber Priority**をクリックします。
2. または、そのルールのラジオボタンを選択し、**Select Action**リストから**Renumber Priority**を選択します。

NetScaler®は、既存のすべてのルールに、10の倍数である新しい優先順位番号を自動的に割り当てます。

要件に応じて優先度番号を割り当てるようにルールを編集します。ルールの編集方法の詳細については、「ACLルールを編集するには」セクションを参照してください。

既存の優先度番号の例:

既存の優先度(/en-us/netscaler-application-delivery-management-software/media/example-existing-acl-priority.png)

NetScaler Consoleによる再番号付けされた優先度の例:

再番号付けされた優先度(/en-us/netscaler-application-delivery-management-software/media/example-renumbered-acl-priority.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### トラブルシューティング

ACLルールが不適切に設定されている場合、すべてのユーザーアカウントがアクセスを拒否される可能性があります。不適切なACL設定が原因で、NetScaler Consoleへのすべてのネットワークアクセスを不注意により失った場合は、アクセスを取得するために次の手順に従ってください。

1. SSHクライアントを使用してNetScaler Consoleにログオンします。
2. コマンド `pfctl –d` を実行します。
3. NetScaler Console GUIにログオンし、それに応じてACLを再構成します。

## インフラストラクチャの管理と監視のためにNetScaler Console監査ログを使用する

NetScaler Consoleサービスを使用して、NetScaler Console上のすべてのイベントと、NetScaler Consoleで管理されているNetScalerインスタンスで生成されたsyslogイベントを追跡できます。これらのメッセージは、インフラストラクチャの管理と監視に役立ちます。しかし、ログメッセージはレビューして初めて優れた情報源となり、NetScaler Consoleはログメッセージのレビュー方法を簡素化します。

フィルターを使用して、NetScaler Consoleのsyslogおよび監査ログメッセージを検索できます。フィルターは、結果を絞り込み、探しているものをリアルタイムで正確に見つけるのに役立ちます。組み込みの検索ヘルプは、ログをフィルタリングするのに役立ちます。ログメッセージを表示するもう1つの方法は、PDF、CSV、PNG、JPEG形式でエクスポートすることです。これらのレポートのエクスポートを、指定されたメールアドレスにさまざまな間隔でスケジュールできます。

NetScaler Console GUIから、次の種類のログメッセージを確認できます。

- NetScalerインスタンス関連の監査ログ
- NetScaler Console関連の監査ログ
- アプリケーション監査ログ

### NetScalerインスタンス関連の監査ログ

NetScaler ConsoleからNetScalerインスタンス関連のsyslogメッセージを表示する前に、NetScaler ConsoleサービスをNetScalerインスタンスのsyslogサーバーとして構成します。構成が完了すると、すべてのsyslogメッセージはインスタンスからNetScaler Consoleにリダイレクトされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Consoleサービスをsyslogサーバーとして構成する

NetScaler Consoleをsyslogサーバーとして構成するには、次の手順に従います。

1. NetScaler Console GUIから、**Infrastructure > Instances** に移動します。
2. syslogメッセージを収集してNetScaler Consoleに表示するNetScalerインスタンスを選択します。
3. **Select Action** リストで、**Configure Syslog** を選択します。
4. **Enable** をクリックします。
5. 「**Facility**」ドロップダウンリストで、ローカルまたはユーザーレベルのファシリティを選択します。
6. syslogメッセージに必要なログレベルを選択します。
7. 「**OK**」をクリックします。

NetScaler Consoleでsyslogを構成する(/en-us/netscaler-application-delivery-management-software/media/configure-syslog-adm.png)

これらの手順により、NetScalerインスタンス内のすべてのsyslogコマンドが構成され、NetScaler Consoleはsyslogメッセージの受信を開始します。メッセージは、**Infrastructure > Events > Syslog Messages**に移動して表示できます。組み込みの検索ヘルプを開くには、「**Need Help?**」をクリックします。詳細については、「syslogメッセージの表示とエクスポート」を参照してください。

NetScaler Console上のsyslogメッセージ(/en-us/netscaler-application-delivery-management-software/media/adm-syslog-messages.png)

ログメッセージをエクスポートするには、右上隅の矢印アイコンをクリックします。

次に、「**Export Now**」または「**Schedule Export**」をクリックします。詳細については、「syslogメッセージの表示とエクスポート」を参照してください。

## NetScaler Console関連の監査ログ

事前設定されたルールに基づいて、NetScaler Consoleは対応するイベントの監査ログメッセージを生成し、インフラストラクチャの健全性を監視するのに役立ちます。

### 監査ログとシェルログを監視するためのsyslogサーバーの構成

NetScaler Consoleの展開で監査ログイベントとシェルログイベントを監視するために、外部syslogサーバーを構成できます。バージョン14.1-34.x以降では、syslogサーバーを構成してシェル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ログイベントも受信できます。これは、既存の監査ログ構成に追加されるものです。監査ログと同様に、シェルログも異なるログレベルで構成できます。

NetScaler Consoleでsyslogサーバーを構成するには、次の手順に従います。

1. **UI Settings > Audit logs > Syslog servers**に移動します。
2. 監査ログ、シェルログ、またはその両方についてログレベルを選択します。
    - **すべて**：監査またはシェル関連イベントのリストされたすべてのログレベルを選択します。
    - **なし**：すべての選択を解除し、ログレベルは選択されません。
    - **カスタム**：チェックボックスとして表示される利用可能なリストから特定のログレベルを選択できます。
3. **OK**をクリックして、選択した構成を続行します。これにより、NetScaler Consoleは監査および/またはシェル関連イベントを構成済みのsyslogサーバーに送信できるようになります。

NetScaler Consoleに存在するすべての監査ログメッセージを表示するには、**設定 > 監査ログメッセージ**に移動します。

ログメッセージをエクスポートするには、右上隅にある矢印アイコンをクリックします。

## アプリケーション関連の監査ログ

すべてのNetScaler Consoleアプリケーション、または特定のアプリケーションの監査ログメッセージを表示できます。

- NetScaler Consoleに存在するすべてのアプリケーションのすべての監査ログメッセージを表示するには、**インフラストラクチャ > ネットワーク機能 > 監査**に移動します。
- NetScaler Consoleで特定のアプリケーションの監査ログメッセージを表示するには、**アプリケーション > ダッシュボード**に移動し、仮想サーバーをクリックして**監査ログ**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScalerライセンス

NetScaler Consoleを使用すると、NetScalerインスタンス全体でライセンスを管理、割り当て、監視できます。以下のトピックは、NetScalerライセンスの管理に役立ちます。

- ライセンスアクティベーションサービス
- ベストプラクティス
- ライセンス管理
- チェックアウトの最小および最大容量
- NetScaler Flexedライセンス
- ライセンスの構成
- ライセンスダッシュボード
- ライセンスレポート
- Flexedライセンスへの移行
- FlexedまたはPooledライセンスの有効期限切れと接続の問題の動作に関するシナリオ
- NetScaler ConsoleをFlexedまたはPooledライセンスサーバーとして構成する
- レガシーライセンス

## ライセンスアクティベーションサービス

**重要:**

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（Citrix Platform License/Universal Hybrid Multi-Cloud）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-premリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

NetScaler仮想CPUライセンス（Pooled vCPU）、NetScaler VPX Check-In and Check-Out（CICO）、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、法的または衡平法上のその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合には適用されません。
LASへの移行を開始する前に、NetScaler向けLAS を読むことをお勧めします。これにより、一般的な前提条件、サポートされているライセンスタイプとサポートされていないライセンスタイプ、特定のライセンスおよび展開タイプに対する正確なワークフロー、その他の重要な情報を確実に理解できます。

ライセンスアクティベーションサービス（LAS）は、従来のファイルベースのライセンスに代わる新しいクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品をアクティベートするための新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

- LASはライセンスメカニズムであり、ライセンスタイプではありません。
- ファイルベースのライセンスは、手動エンタイトルメントを使用した古いライセンス方法を指します。このドキュメントでは、「ファイルベースのライセンス」と「手動で管理されるエンタイトルメント」は、同じ概念を説明しているため、互換的に使用されます。

LASの主な利点は次のとおりです。

- エンタイトルメントブロブを介した自動エンタイトルメント配信。
- ライセンス通信のプロキシとしての外部エージェントはオプションです。
- LASは、NetScaler MPX™およびSDXインスタンスでのZ-Capソフトウェアライセンスファイルの必要性を排除します。

**注:**

- 新しい「ライセンスの同期」オプションを使用すると、オンデマンドで手動で同期をトリガーし、エンタイトルメントを即座に最新の状態に保つことができます。
- エンタイトルメント同期のデフォルトの頻度は、LASエンタイトルメントがNetScaler Consoleサービスと同期されていない場合は1時間に1回、その後は24時間に1回です。オンデマンド同期の場合は、`Sync Now`をクリックしてください。

## LASのNetScalerバージョン互換性

LASを使用するには、NetScalerインスタンスで次のいずれかの最小バージョンが実行されている必要があります。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

LASを使用するには、以下の前提条件を満たしていることを確認してください。

- 有効なCitrix Cloudアカウントが必要です。既存のクラウドアカウントの詳細、または新しいクラウドアカウントのオンボーディングについては、「アカウント管理」を参照してください。
- LASアクティベーションワークフローに使用されるCitrix Cloudアカウントにリンクされている組織ID（Org ID）は、有効な購入済みエンタイトルメントを所有している必要があります。現在のエンタイトルメントを表示するには、「エンタイトルメント」にアクセスしてください。
- NetScaler ConsoleとNetScalerインスタンスは、LAS互換バージョンを実行している必要があります。
- NetScalerインスタンスは、NetScaler Consoleで管理対象インスタンスとして追加されます。
- LASは、Flexedライセンス（UHMC/CPL）、プール型帯域幅ライセンス、および固定期間帯域幅ライセンスをサポートしています。Pooled vCPU、CICOなどの他のすべてのレガシーNetScalerライセンス形式は、LASではサポートされていません。
- SDXアプライアンスの場合、NetScaler SVMをLASでサポートされているビルドにアップグレードし、LASベースのライセンスに移行してください。特定のVPXビルドバージョンは、LASの互換性に影響しません。

次の図は、ConsoleオンプレミスCloud Connectを使用したLASのものです。



**注:**

NetScaler Consoleを初めて使用する場合は、「はじめに」から始めてください。

## LASへの移行

### Cloud ConnectでLASをアクティブ化

**Cloud ConnectでLASをアクティブ化**オプションは、クラウド接続されたConsoleオンプレミス展開用です。この展開により、エンタイトルメントの自動ダウンロードと、Consoleサービスからのタイムリーな更新の処理によって、ライセンス管理が簡素化されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記:**

- **Cloud Connect を有効にする**オプションが有効になっていることを確認して、**Cloud Connect を使用して LAS をアクティブ化する**展開方法を使用してください。このオプションを有効にするには、「Cloud Connect を有効にする」を参照してください。
- Cloud Connect が有効になると、LAS は自動的に有効になります。

Console GUI の右上隅を確認することで、Cloud Connect が有効になっていることを確認できます。NetScaler Console Service に接続すると、**License Management** の下の **LAS** タブに移動します。ここでは、最終更新日と次回の更新日を確認できますが、手動での操作は不要です。

LAS をアクティブ化するには、NetScaler Console on-prem でライセンスエンタイトルメントファイルまたはブロブを取得する必要があります。**NetScaler Licensing > License Management > LAS** に移動すると、License Activation Service (LAS) の概要が表示されます。

Console on-prem で LAS が有効になると、すべての NetScaler Flexed および Pooled ライセンスエンタイトルメントが、**NetScaler Licensing > License management > License Activation Service (LAS)** セクションに表示されます。

クラウド接続機能を使用して、Console on-prem は Console Service に接続し、LAS からライセンスエンタイトルメントファイルまたはブロブを取得します。

このエンタイトルメントファイルまたはブロブは 30 日間有効です。継続的なライセンスを確保するために、クラウド接続された Console は、このエンタイトルメントブロブを毎日 LAS と自動的に更新します。

ファイルベースのライセンスでは、適用されたエンタイトルメントと構成は、**NetScaler Licenses > License management > Manual License File management** タブの下に表示されます。

ライセンス管理ページのテレメトリステータスインジケーターは、テレメトリコンプライアンスを維持するための重要なアラートとして機能します。

- **赤色のアイコン**: 即座の対応が必要であることを示します。システムが、一部またはすべての管理対象 NetScaler インスタンスのテレメトリを収集していません。このステータスは、テレメトリの不遵守とライセンスへの影響の可能性を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **緑色のアイコン**: テレメトリがアクティブであることを確認します。これは、コンソールがすべての管理対象 NetScaler インスタンスからテレメトリを正常に送信していることを示します。

ステータスに即座の対応が必要な場合は、インジケーターをクリックしてテレメトリページにアクセスしてください。NetScaler テレメトリページで強調表示されているすべての問題が修正されていることを確認してください。詳細については、「テレメトリ収集およびアップロードの問題のトラブルシューティングのための診断」を参照してください。

### NetScalerインスタンスをLASにライセンス供与または移行する

**NetScaler Licenses > License management > License Activation Service (LAS)** に移動すると、GUIはNetScalerインスタンスの互換性に基づいて動的に更新されます。 LAS互換バージョンにNetScalerインスタンスがない場合、NetScalerをアップグレードまたは追加するよう指示するメッセージが画面に表示されます。

**注：**

NetScalerインスタンスの一部が互換バージョンにアップグレードされている場合、それらの特定のインスタンスにLASを使用できます。

1つ以上のNetScalerインスタンスがLASと互換性がある場合、それらは2つのカテゴリに分類されます。

**LASでNetScalerインスタンスをライセンス供与:** これらはまだLASを使用していませんが、互換性のあるインスタンスです。

**ライセンス供与されたNetScalerインスタンスをLASに移行:** これらは、別の方法で既にライセンス供与されており、LASに移行する資格のあるインスタンスです。

NetScaler GUIは、初めてのLASユーザー（LASにインスタンスがゼロ）であるか、既存のユーザー（既にLASにインスタンスがあり、さらに追加している）であるかに応じて動的に調整されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注：**

LASへのライセンス供与または移行が完了したら、SVM上のローカルファイルベースライセンスを削除します。ファイルベースライセンスはSVMフォルダー `/mpsconfig/license` にあり、シェルプロンプトを使用してこのフォルダーから削除する必要があります。この注意は、初めてのユーザーと既存のユーザーの両方に対する**LASでのライセンス供与**および**LASへの移行**ワークフローに適用されます。

**初めてのユーザー**

初めてのユーザーには次の画像が表示されます。



### LASでのNETSCALERインスタンスのライセンス供与

**LASでNetScalerインスタンスをライセンス供与**セクションには、現在ライセンス供与されていない、またはFlexed帯域幅またはPooled帯域幅のファイルベースライセンスを使用していないNetScalerインスタンスが一覧表示されます。

LASでインスタンスをライセンスするには、次の手順を実行します。

1. **License with License Activation Service (LAS)** を選択し、**Next** をクリックします。
2. インスタンスを選択し、**Continue** をクリックします。
3. 詳細を入力し、**Submit** をクリックします。 LASでライセンスを付与したい各NetScalerインスタンスについて、この手順を繰り返します。

**注:**

- SDXインスタンスを除き、ライセンスを有効にするために選択されたインスタンスが再起動します。

### 既存のライセンス済みNETSCALERインスタンスをLASに移行する

**Migrate existing licensed instances to LAS** セクションには、FlexedまたはPooledファイルベースのライセンスを持つすべてのNetScalerインスタンスが一覧表示されます。これらは次のように分類されます。

- **移行準備完了のインスタンス:** LAS互換のバージョンまたはビルドであり、LASへの移行準備が整っているインスタンスを一覧表示します。移行するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Migrate your existing licensed NetScaler instances to LAS** を選択し、**Next** をクリックします。

b. **Migrate to License Activation Service (LAS)** で、1つ以上のNetScalerインスタンスを選択し、**Migrate** をクリックします。

。

- **移行前にアップグレードが必要なインスタンス:** 移行前に互換性のあるバージョンまたはビルドにアップグレードする必要があるインスタンスを一覧表示します。アップグレードするには、次の手順を実行します。

  **前提条件:**

  LASベースのライセンスを使用するには、NetScalerインスタンスのエディションが、PooledまたはFlexedファイルベースのライセンスのエディションと一致している必要があります。移行を開始する前に、インスタンスのエディションを新しいライセンスと一致するように変更してください。

  a. 「**既存のライセンス済みNetScalerインスタンスをLASに移行**」を選択し、「**アップグレード**」をクリックします。

  b. 「**NetScalerのアップグレード**」ページで、インスタンスを選択し、インスタンスをLASと互換性のあるバージョンまたはビルドにアップグレードします。

**既存のLASユーザー**

既存のLASユーザーの場合、次のGUIが表示されます。

既存のLASユーザー(/en-us/netscaler-application-delivery-management-software/media/existing-las-user.png)。

**注:** LASでライセンスされたCPXインスタンスを表示するには、Flexed Dashboard GUIを参照してください。CPXインスタンスは、LASを使用するNetScalerインスタンスの下にはここにリストされません。

### LASでNETSCALERインスタンスをライセンスする

「**LASでNetScalerインスタンスをライセンスする**」セクションには、現在ライセンスされていない、またはFlexed帯域幅またはPooled帯域幅のファイルベースライセンス以外のライセンスを使用しているNetScalerインスタンスがリストされます。

LASでインスタンスをライセンスするには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**License Activation Service (LAS) でライセンス**」の下にある「**LASでライセンス**」をクリックします。
2. インスタンスを選択し、「**続行**」をクリックします。
3. 詳細を入力し、「**送信**」をクリックします。 LASでライセンスする各NetScalerインスタンスについて、この手順を繰り返します。

LASでライセンス(/en-us/netscaler-application-delivery-management-software/media/license-with-las.png)。

**注:**

- 選択したインスタンスは、SDXインスタンスを除き、ライセンスを有効にするために再起動します。

### ライセンスされたNETSCALERインスタンスをLASに移行する

「**ライセンスされたNetScalerインスタンスをLASに移行する**」セクションには、FlexedまたはPooledファイルベースライセンスを持つすべてのNetScalerインスタンスがリストされます。これらは次のように分類されます。

- **LAS内のインスタンス:** すでにLASベースのライセンスを使用しているインスタンスをリストします。
- **移行準備完了のインスタンス:** 移行準備が整っている互換性のあるインスタンスをリストします。移行するには、次の手順を実行します。

  a. 「**ライセンスされたNetScalerインスタンスをLASに移行する**」を選択し、「**移行**」をクリックします。

  b. 1つ以上のNetScalerインスタンスを選択し、「**移行**」をクリックします。

- **移行前にアップグレードが必要なインスタンス:** 互換性のあるバージョンにアップグレードする必要があるインスタンスをリストします。アップグレードするには、次の手順を実行します。

  **前提条件:**

  LASベースのライセンスを使用するには、NetScalerインスタンスのエディションがPooledまたはFlexedライセンスのエディションと一致している必要があります。移行を開始する前に、インスタンスのエディションを新しいライセンスと一致するように変更してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 「**移行前にアップグレードが必要なインスタンス**」を選択し、「**アップグレード**」をクリックします。

b. 1つ以上のNetScalerインスタンスを選択し、「**アップグレード**」をクリックします。

c. 詳細を入力し、「**送信**」をクリックします。

## ライセンスアクティベーションBLOBの動作

NetScalerインスタンスがConsole on-premから「**LASでライセンス供与またはLASに移行**」の一部として取得するライセンスアクティベーションBLOBは30日間有効です。NetScalerがConsole on-premとの接続を失い、その後再確立した場合、ライセンスアクティベーションBLOBはすぐに復元されます。

NetScalerが最大24時間Console on-premに再接続できない場合、猶予期間に入ります。 デフォルトでは、ライセンスアクティベーションBLOBは8時間ごとに更新されます。24時間で3回連続して8時間の更新試行が失敗した場合、NetScalerは猶予期間に入ります。

### ライセンス猶予期間アラート

ライセンス猶予期間アラートのタッチポイントは次のとおりです。

- Flexedダッシュボードに、インスタンスが猶予期間中であり、ライセンスアクティベーションBLOBの有効期限が切れるまでの残り日数を示す警告アイコンが表示されます。
- 管理者がNetScalerインスタンスGUIにログインするたびに、インスタンスが猶予期間中であり、ライセンスアクティベーションBLOBの有効期限が切れるまでの残り日数を示すポップアップメッセージが表示されます。
- 設定されたメールアドレスにメール通知が送信されます。詳細については、「メール設定の構成」を参照してください。

  **注:** ライセンス関連のメール通知を受信するには、システムイベントカテゴリで**ライセンス**を選択してください。

### ConsoleオンプレミスとConsoleサービス間の接続が切断された場合のNetScalerの動作の更新

クラウド接続展開では、LASはLASアクティベーションBLOBをNetScaler Consoleオンプレミスに直接発行します。NetScaler Consoleオンプレミス用のアクティベーションBLOBは毎日更新され、30日間、またはライセンスエンタイトルメントの有効期限が切れるまで（いずれか早い方）有効です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleオンプレミスがこの有効なアクティベーションBLOBを受信すると、ライセンスされたNetScalerインスタンスにダウンストリームアクティベーションBLOBを発行する権限が与えられます。NetScaler Consoleは、自身のBLOBが有効である間のみ、これらのダウンストリームBLOBを発行します。

NetScalerインスタンスに発行されるアクティベーションBLOBも、30日間、またはNetScaler ConsoleアクティベーションBLOBの残りの有効期限まで（いずれか早い方）有効です。

**シナリオA：NetScalerとNetScaler Consoleオンプレミス間の接続が切断される場合**

NetScalerがNetScaler Consoleオンプレミスへの接続を失うと、NetScaler Consoleオンプレミスはインスタンスのアクティベーションを更新できません。NetScaler Consoleオンプレミスは8時間ごとに更新を再試行します。3回の試行失敗（合計24時間）後、NetScalerインスタンスは**猶予**ステータスに入ります。影響を受けるNetScalerインスタンスは、NetScaler ConsoleオンプレミスGUIで**猶予**ステータスとしてフラグ付けされます。

**注:**

この動作は、LASをサポートするすべてのNetScaler Consoleオンプレミスビルドに適用されます。

**シナリオB：NetScaler ConsoleオンプレミスとNetScaler Consoleサービス間の接続が切断される場合**

NetScaler Console on-premises と NetScaler Console service 間のリンクが切断されると、NetScaler Console on-premises は自身のライセンスアクティベーションブロブを更新できません。

このような場合、NetScaler Console on-premises は標準の30日間ローリングアクティベーションブロブを発行できず、有効期間が短くなる（29、28、27...0日まで）ブロブをNetScalerインスタンスに発行します。接続が30日以内に復元されない場合、NetScalerインスタンスは完全な停止のリスクがあります。

以前のリリースでは、NetScalerインスタンスが管理者に警告するために**猶予**ステータスに入ることなく、突然この問題が発生していました。

リリース14.1-72.x以降、この動作は予期せぬ停止を防ぐために更新されました。NetScaler Console on-premises によってライセンス供与されたNetScalerインスタンスは、NetScaler Consoleサービス接続が切断され、NetScaler Console on-premises のブロブを更新できない場合、自動的に**猶予**ステータスに移行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console on-premises と NetScaler Console service 間の接続が30日以内に修復された場合、NetScalerインスタンスは猶予期間を正常に終了します。

この変更により、管理者はNetScaler Console GUIの**猶予**ステータスを使用して即座にアラートを受け取ることができ、停止が発生する前に接続の問題を特定し、トラブルシューティングし、修正することができます。

## LASライセンスワークフロー中にLASに送信される情報

このセクションでは、初回リクエスト時および各LASアクティベーションブロブ更新リクエスト時に、アクティベーションブロブのLASへのリクエストの一部として送信されるすべての情報を詳述します。 以下の表は、ライセンスワークフロー中にLASに送信されるパラメータをまとめたものです。

| パラメータ | 説明 | LASワークフローにおける必要性 |
|---|---|---|
| **エルエスジーユーアイディー** | UUID形式のオンプレミスConsoleの一意のID | LASバインディングパラメータ |
| **エルエスアイディー** | SHA256形式のオンプレミスConsoleの一意のID | LASバインディングパラメータ |
| **公開鍵** | NetScalerトークン配布に使用されるオンプレミスConsoleの公開キー | LASがこのConsoleを承認したことを保証します |
| **CCID** | オンプレミスConsoleのオンボーディングに使用されるCitrix Cloud ID | LASバインディングパラメータ |
| **LSビルド** | オンプレミスConsoleのビルドバージョン | LASアクティベーション要件 |
| **コンソールIPおよびホスト名** | IP_hostname形式のオンプレミスConsoleのホスト名 | LASアクティベーション要件 |
| **activated_clients** | LASライセンス、機能、および要求時間を持つNetScalerのリスト。注：NSIPは共有されません。LPEID（一意のID）のみが提供されます。 | このコンソールによって生成されたLASアクティベーションブロブを持つNetScalerのリスト。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 | LASワークフローにおける必要性 |
| --- | --- | --- |
| **最終アクティベーションID** | 更新時に提供される以前のLASアクティベーションID | LAS側での追跡用 |

**注：**

NetScaler Consoleオンプレミスリリース14.1-60.57以降、クラウド接続展開向けのLASベースのライセンスワークフローでは、IPアドレスとホスト名は使用されなくなりました。代わりに、LASはシステム識別子 (`lsguid`) を使用して、NetScaler Consoleオンプレミスのクラウド接続展開を一意に識別します。

# LASに移行したNetScaler Consoleオンプレミス環境（クラウド接続済み）を監視するためのベストプラクティス

このドキュメントでは、LASを使用するNetScaler環境を監視するために従うことができるベストプラクティスに焦点を当てています。このドキュメントは、ConsoleオンプレミスでLASを使用する展開に適用されます。

## 前提条件

- NetScaler用LASページ（ConsoleサービスでのLASに関するFAQを含む）をお読みください。
- ライセンスアクティベーションサービスをお読みになり、LAS移行を完了してください。
- 関連する通知を設定し、NetScaler GUIとCLIを定期的に監視していることを確認してください。

**注:**

通知の継続的な改善を目指しており、このドキュメントもそれに応じて更新し続けます。

NetScaler Consoleオンプレミスの場合、LASはクラウド接続されたNetScaler ConsoleオンプレミスにLASアクティベーションブロブを提供します。このブロブは30日間、またはライセンスエンタイトルメントの有効期限が切れるまでのいずれか早い方まで有効で、毎日更新されます。NetScaler ConsoleオンプレミスとNetScaler Consoleサービス間の接続が切断されると、NetScaler ConsoleオンプレミスはLASアクティベーションブロブを更新できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consoleオンプレミス LASアクティベーションブロブの有効期限の監視セクションでは、Consoleオンプレミス LASアクティベーションブロブの有効期限が30日以内になったときにトリガーされる通知について詳しく説明しています。これが発生した場合、クラウド接続には即座の対応が必要です。これを解決するには、クラウド接続診断ツールを実行して特定された問題を修復するか、Citrixサポートに連絡して支援を受けてください。

NetScaler Consoleオンプレミスが LASアクティベーションブロブを取得した後、NetScaler Consoleオンプレミスを介してライセンスを必要とするすべてのNetScalerインスタンスにアクティベーションブロブを発行する権限が与えられます。NetScaler Consoleオンプレミスは、自身の LASアクティベーションブロブが有効である間のみ、これを行うことができます。NetScalerインスタンスには、30日間の有効期間（または自身のブロブの有効期限が切れるまでのいずれか早い方）を持つLASアクティベーションブロブを発行します。

NetScalerとNetScaler Consoleオンプレミス間の接続が失われた場合：

- ConsoleはNetScalerインスタンスの LASアクティベーションブロブを更新できません。
- Consoleは8時間ごとに接続を再試行します。
- 3回の試行失敗（合計24時間）後、NetScalerは「猶予」ステータスに入り、これはConsole UIに反映されます。

(#monitor-netscaler-instances-las-activation-blob-expiry-netscaler-licensed-through-console-on-premises-cloud-connected)セクションでは、有効期限が近づいている（30日未満）LASアクティベーションブロブの通知について詳述しています。この状況が発生した場合、クラウド接続には直ちに対応が必要です。これを解決するには、クラウド接続診断ツールを実行して特定された問題を修復するか、Citrixサポートに連絡して支援を求めてください。

## Console on-premises LASアクティベーションブロブの有効期限を監視する

### GUIを使用して最終更新日を監視する

最終更新日またはアクティベーション日を監視するには、Console on-premises GUI > NetScaler Licensing > License Management > LAS に移動します。

更新/リフレッシュは毎日行われます。最終更新日/アクティベーション日が数日以上前である場合、接続またはアクティベーションの問題を示しています。

(/en-us/netscaler-application-delivery-management-software/media/renew-date-gui.png)

**通知**

**NetScaler Console on-premises GUI のバナー:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console on-premises がLASアクティベーションブロブの更新に失敗すると、次の図に示すように、NetScaler Console GUI に警告バナーが表示されます。 (/en-us/netscaler-application-delivery-management-software/media/banner-gui.png)

**クラウド接続の問題に関するシステムイベントベースの通知:**

NetScaler Console は、クラウド接続ステータスの変更に関するイベントを生成します。これらのイベントは、NetScaler Console on-premises と Console サービス間の接続状態が変化したときにトリガーされます。これには、次のような移行が含まれます。

- 接続済みから切断済みまたはエラーへ
- 切断済みまたはエラーから接続済みへ

これらのイベントを表示するには、**Console on-premises GUI > Settings > System Events** に移動します。

(/en-us/netscaler-application-delivery-management-software/media/event-notify.png)

クラウド接続関連の問題についても、メールベースの通知を設定できます。

1. **コンソール オンプレミス GUI > 設定 > イベント通知** に移動します。
2. カテゴリ **CloudConnectStatus** を選択します。
3. メール、SMS、PagerDuty など、1つ以上の通知形式を選択して設定します。
4. **Save** をクリックします。

システムイベントベースの通知(/en-us/netscaler-application-delivery-management-software/media/email-notify-configure.png)

**Console on-premises LASアクティベーションBLOBの有効期限切れに関するシステムイベントベースの通知:**

NetScaler Console on-premisesは、NetScaler Console on-premisesのLASアクティベーションBLOBの有効期限切れについて管理者に通知するイベントを生成します。これらのイベントに対して、メールベースのアラートを設定することもできます。

LASアクティベーションBLOBの有効期限切れに関する通知を設定するには:

1. **コンソール オンプレミス GUI > 設定 > イベント通知** に移動します。
2. **Licenses and License Pool** カテゴリを選択します。
3. メール、SMS、PagerDuty など、1つ以上の通知形式を選択して設定します。
4. **Save** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

設定されたイベントのリストには、他のユースケースや設定された通知に基づいて、これら2つ以上のものが含まれる場合があります。スクリーンショットは、簡潔にするためにこれら2つのみを示しています。

システムイベント通知(/en-us/netscaler-application-delivery-management-software/media/configure-system-notify.png)

## NetScalerインスタンスのLASアクティベーションBLOBの有効期限を監視する (オンプレミスでクラウド接続されたConsoleを介してライセンス供与されたNetScaler)

**GUIを使用してNetScalerインスタンスを表示する:**

猶予ステータスにあるNetScalerインスタンスを表示するには、**Console on-premises GUI > NetScaler Licensing > Flexed Licensing > Dashboard** に移動します。

ライセンスされたNetScalerインスタンスダッシュボード(/en-us/netscaler-application-delivery-management-software/media/on-prem-gui.png)

### CLIを使用してNetScalerインスタンスのステータスを表示する

猶予ステータスにあるNetScalerインスタンスと残りの猶予期間を表示するには、`sh licenseserver` コマンドを実行します。

**例:**

```
> sh licenseserver

     License Server: 10.102.123.31 Status: Disconnected

        Grace: Yes         Grace Time Left: 652

Done
```

### 通知

**NetScaler Consoleオンプレミス上のバナー:**

NetScaler ConsoleオンプレミスGUIは、LASアクティベーションBLOBがx日後に期限切れになるNetScalerインスタンスを一覧表示するバナーを表示します。ここで、xは30日未満です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleオンプレミス上のバナー(/en-us/netscaler-application-delivery-management-software/media/gui-banner.png)

**NetScaler GUI上のバナー:**

NetScalerインスタンスが猶予ステータスの場合、NetScaler ConsoleオンプレミスGUIはバナーを表示します。

NetScaler GUI上のバナー(/en-us/netscaler-application-delivery-management-software/media/banner-net-gui.png)

**システムイベントベースの通知:**

NetScaler Console on-premisesは、NetScalerインスタンスのLASアクティベーションブロブの有効期限が切れるとイベントを生成します。これらのイベントに対して、メールベースのアラートを設定することもできます。

LASアクティベーションブロブの有効期限に関する通知を設定するには:

1. **Console on-premises GUI > 設定 > イベント通知**に移動します。
2. **ライセンスとライセンスプール**カテゴリを選択します。
3. メール、SMS、PagerDutyなど、1つ以上の通知形式を選択して設定します。
4. 保存をクリックします。

**猶予ステータスに対してNetScalerによって生成されるSNMPトラップ:**

NetScalerインスタンスが猶予ステータスの場合、NetScalerは次のSNMPトラップを生成します。

- pooledLicenseGraceStarted: インスタンスが猶予期間に入ったときにトリガーされます。
- pooledLicenseGraceNormal: NetScalerが30日間猶予期間にあり、猶予期間が終了した場合にトリガーされます。これは、デプロイメントが影響を受けるか、ライセンスなしになることを意味します。
- pooledLicenseGracePeriodOver: 猶予期間が終了したときにトリガーされます。

**例:**

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceStarted
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceNormal
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGracePeriodOver
(nsPartitionName = default)
```

## ライセンスエンタイトルメントの有効期限を監視する

**ライセンスエンタイトルメントの有効期限**は、顧客のライセンスエンタイトルメントまたは契約の有効期限を指します。

GUIを使用してライセンスエンタイトルメントの有効期限情報を表示するには、**Console Service GUI > NetScaler Licensing > License Management > LAS**に移動します。

**有効期限までの日数**は、対応するライセンスのエンタイトルメントの有効期限を表示します。

### 通知

**NetScaler ConsoleサービスGUIバナー:**

NetScaler ConsoleサービスGUIには、ライセンスエンタイトルメントがx日後に有効期限切れになることを示すバナーが表示されます。

NetScaler Consoleオンプレミス上のバナー(/en-us/netscaler-application-delivery-management-software/media/gui-banner.png)

### メールベースの通知

メールベースの通知を設定するには:

1. **コンソールサービスGUI > NetScalerライセンス > ライセンス管理 > 通知設定**に移動します。
2. **ライセンスの有効期限が切れる何日前に通知を受け取りますか？**に必要な値を入力します。
3. **保存**をクリックします。

メールベースの通知(/en-us/netscaler-application-delivery-management-software/media/email-notification.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# ライセンス管理

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれる）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASとなり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレ: 14.1-51.x

  **注:** Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-prem リリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

負うことなくCitrixメンテナンスを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
続行する前に、以下の注記をお読みください。

**注:**

Universal Hybrid Multi-Cloud (UHMC) またはCitrix Platform License (CPL) を購入すると、提供されるNetScalerライセンスはFlexedライセンスと呼ばれます。

Flexedライセンスは、NetScaler Console on-prem 14.1および13.1リリースでサポートされています。Flexed GUIの表示とバンドルされたエンタイトルメントの提供によるより良い製品エクスペリエンスのために、NetScaler Console on-premをリリース14.1–12.34以降にアップグレードすることをお勧めします。

NetScaler Console on-premリリース14.1–12.34以降では:

- Flexedライセンスは、FlexedダッシュボードUI (NetScaler® **Licensing > Flexed Licensing)** を介して管理できます。
- Flexedライセンスを適用すると、アナリティクス用の無制限のNetScaler Console VIPのバンドルされたエンタイトルメントが利用可能になります。

NetScaler Console on-premリリース13.1および14.1-12.34より前の14.1ビルドの場合:

- Flexedライセンスを適用すると、NetScaler ConsoleはそれらをPooledライセンスと同じように扱い、PooledダッシュボードUI (**Infrastructure > Pooled Licensing**) に詳細を表示します。
- Flexedライセンスが適用されても、これらのリリースではアナリティクス用の無制限のNetScaler Console VIPのバンドルされたエンタイトルメントは利用できません。-

## LASベースのライセンス

LASを有効にすると、エンタイトルメントは**Console UI > License Management > License Activation Service (LAS)** セクションに表示されます。



### ライセンスサーバーポート

LASは、すべてのライセンス通信にポート443を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

LASを使用するには、NetScaler®インスタンスを管理対象インスタンスとして追加します。

## ライセンス有効期限情報

### ライセンスの有効期限を表示

1. **NetScaler Licensing > License Management** に移動します。
2. **ライセンスエンタイトルメントの有効期限情報**セクションには、有効期限が近づいているライセンスの詳細が表示されます。
   - **機能**: 有効期限が切れるライセンスの種類。
   - **カウント**: 影響を受けるインスタンスの数、または帯域幅 (Mbps)。
   - **有効期限までの日数**: ライセンスの有効期限 (契約終了日) までの日数。

LA を有効にしてクラウド接続を確立すると、プールまたはフレックスライセンスの初期エンタイトルメントは 1 時間以内にフェッチされます。その後の新規または更新されたプールまたはフレックスライセンスは 24 時間以内にフェッチされます。

### ライセンスの有効期限の動作

NetScaler Console を介して管理されているライセンスの有効期限が切れると、関連する NetScaler インスタンスはトラフィックの処理を停止し、その構成が失われる可能性があります。

### ライセンス終了日 (ライセンス契約終了日) の通知メールとポップアップバナー

NetScaler Console GUI では、ライセンス終了日に関連するポップアップメッセージが表示されます。デフォルトでは、ライセンス終了日の 30 日前 (デフォルト) から、GUI にポップアップメッセージ (ログインするたびに) が表示されます。 日数は、**通知設定 > ライセンスの有効期限設定**で設定できます。

管理者として、**通知設定**でメール通知が設定されている場合、ライセンス終了日の通知メールも受信します。通知メールは、ライセンス終了日の 30 日前、20 日前、10 日前の頻度で送信されます。

## 通知設定

LAS によって管理されている有効期限が近づいているフレックスライセンスまたはプールライセンスの通知を設定するには、次の手順に従います。

1. NetScaler の**ライセンス > ライセンス管理 > 通知設定**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 「通知設定」セクションで、「ライセンス使用状況について**通知する**」を選択します。通知を送信するために割り当てられる、フレキシブルまたはプールされたライセンス容量の割合としてアラートしきい値を設定します。
3. ライセンスがしきい値に達したとき、または期限切れになる前に送信する通知の種類を、適切なチェックボックスを選択して選択します。通知の種類は次のとおりです。

    - **メール**: 通知を送信するためのメールプロファイルまたは配布リスト。詳しくは、「メール配布リストの作成」を参照してください。
    - **Slack**: 通知を送信するためのSlackプロファイルの詳細。
    - **PagerDuty**: 通知を送信するためのPagerDutyプロファイル。
    - **ServiceNow**: Citrix ServiceNowプロファイルはデフォルトで指定されており、利用可能な唯一のオプションです。これらのプロファイルの作成について詳しくは、「通知の構成」を参照してください。

4. 通知の種類を選択し、**追加**をクリックして詳細を追加します。設定を保存する前に、各通知システムをテストすることもできます。
5. 有効期限までの日数（ライセンスの有効期限について通知を受けたい日数）を指定します。
6. **保存**をクリックします。

### メール配布リストの作成

メール配布リストを作成するには、次の手順を実行します。

1. **メール**を選択し、**追加**をクリックします。
2. **メール配布リストの作成**で、次の詳細を指定します。

    - **名前** - 配布リスト名を指定します。
    - **メールサーバー** - メール通知を送信するメールサーバーを選択します。メールサーバーを追加するには、 をクリックします。サーバー名/IPアドレスとポートを指定します。メールサーバーにアクセスするための認証を必須にするには、 を選択します。メールサーバーがSSL認証をサポートしている場合は、 を選択します。 をクリックします。
    - **差出人** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
    - **宛先** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
    - **Cc** - NetScaler Consoleがメッセージをコピーするメールアドレスを指定します。
    - **Bcc** - NetScaler Consoleがメッセージをブラインドカーボンコピー（メールアドレスは表示されません）するメールアドレスを指定します。
    - 「**作成**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### Slackプロファイルの作成

Slackプロファイルを作成するには、次の手順を実行します。

1. Slackで、「**追加**」をクリックします。
2. 「**Slackプロファイルの作成**」で、次の詳細を指定します。

   - **通知** - 有効にすると、アラートとイベント通知が指定されたSlackチャネルに直接送信されます。
   - **添付ファイル付き通知** - 有効にすると、トリガーされたアラートとイベントに関する詳細情報が、メールの添付ファイルまたはWebhook内のJSONペイロードとして送信されます。
   - **プロファイル名** - プロファイル名を指定します。この名前はSlackプロファイルリストに表示されます。
   - **チャネル名** - NetScaler Consoleが通知を送信するSlackチャネル名を指定します。
   - **Webhook URL** - チャネルのWebhook URLを指定します。受信Webhookは、外部ソースからSlackにメッセージを投稿する簡単な方法です。URLはチャネル名に内部的にリンクされています。このURLに送信されるすべてのイベント通知は、指定されたSlackチャネルに投稿されます。Webhookの例を次に示します。`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

### PagerDutyプロファイルの作成

PagerDutyを使用すると、登録済みの電話番号へのメール、プッシュ通知、電話による通知を設定できます。NetScaler ConsoleにPagerDutyプロファイルを追加する前に、PagerDutyで必要な設定が完了していることを確認してください。PagerDutyの利用を開始するには、PagerDutyのドキュメントを参照してください。

PagerDutyプロファイルを作成するには、次の手順を実行します。

1. PagerDutyで、**追加**をクリックします。
2. **PagerDutyプロファイルの作成**で、次の詳細を指定します。

   - **プロファイル名** - プロファイル名を指定します。この名前は、イベントルールやSSL通知などのさまざまなモジュールでPagerDutyアラートを送信するために使用されます。
   - **統合キー** - 統合キーを指定します。このキーはPagerDutyポータルから取得できます。PagerDutyで統合用のサービスを作成する際は、**Generic Events API Integration**オプションを使用してください。
   - **作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細については、PagerDutyのドキュメントのサービスと統合を参照してください。

### ServiceNowプロファイルの表示

NetScalerイベントのServiceNow通知を有効にするには、ITSMコネクタを使用してNetScaler ConsoleをServiceNowと統合する必要があります。

詳細については、NetScaler ConsoleとServiceNowインスタンスの統合を参照してください。

ServiceNowプロファイルを表示および確認するには、次の手順を実行します。

1. **ServiceNow**では、**Citrix_Workspace_SN**プロファイルがデフォルトで選択されています。
2. **テスト**をクリックしてServiceNowチケットを自動生成し、構成を確認します。

**注:**

NetScalerライセンスのさまざまな種類については、ライセンスの概要を参照してください。

### LASのRBACサポート

ロールベースのアクセス制御 (RBAC) を使用して、以下の制御レベルでLASアプリケーションアクセスを管理できます。

- **機能レベル**: 特定の管理者に対するライセンス機能の可視性を制限します。
- **インスタンスレベル**: 承認された管理者が、選択したNetScalerインスタンスにのみライセンスを適用できるように制限します。

設定の詳細については、ロールベースのアクセス制御を参照してください。

## 手動で管理されるエンタイトルメント (ファイルベースのライセンス)

以下のセクションは、手動で管理されるエンタイトルメント (ファイルベースのライセンス) に適用されます。

### ライセンスファイル

NetScaler Flexedライセンスには、MyCitrixポータルからダウンロードする必要がある以下のファイルが含まれています。現在のNetScalerライセンスの種類からFlexed Licensingへの移行の詳細については、Flexed Licensingへの移行を参照してください。

このセクションでは、NetScalerに存在するライセンスファイルについて説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ファイル名に含まれるもの | 説明 | ダウンロード情報 | ライセンスのアップロード/適用先 |
|---|---|---|---|
| NetScaler Flexed VPX SW インスタンス | VPX/CPX/BLX ソフトウェアインスタンスの使用を許可します。 | NetScaler Console ホスト ID を使用してこのファイルをダウンロードします。 | NetScaler Console 上で |
| NetScaler Flexed MPX SW インスタンス | MPX ソフトウェアインスタンスの使用を許可します。 | NetScaler Console ホスト ID を使用してこのファイルをダウンロードします。 | NetScaler Console 上で |
| NetScaler Flexed SDX SW インスタンス | SDX ソフトウェアインスタンスの使用を許可します。 | NetScaler Console ホスト ID を使用してこのファイルをダウンロードします。 | NetScaler Console 上で |
| ネットスケーラー フレックスド プラチナ BW | Flexed Platinum スループット容量の使用を許可します。 | NetScaler Console ホスト ID を使用してこのファイルをダウンロードします。 | ネットスケーラー コンソールで |
| NetScaler Flexed VPX FIPS SWインスタンス | VPX FIPSソフトウェアインスタンスの利用を許可します | NetScaler ConsoleホストIDを使用してこのファイルをダウンロードします | ネットスケーラー コンソールで |
| ゼロキャパシティ MPX-Zプラットフォームライセンス | NetScaler MPX HW/ NetScaler MPX FIPS HWをFlexedライセンスに参加させることを許可します | このファイルをダウンロードします | NetScaler MPX上 |
| ゼロキャパシティ SDX-Zプラットフォームライセンス | NetScaler SDX HW/ NetScaler SDX FIPS HWをFlexedライセンスに参加させることを許可します | このファイルをダウンロードします | NetScaler SDX上 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 重要な注意事項

1. Pooledライセンスのお客様で、Flexedライセンスに移行し、MPXおよびSDXハードウェアにすでにZ-Cap永続ライセンスがある場合、Flexedで受け取ったZ-Capライセンスを適用する必要はありません。ただし、NetScaler MPX/NetScaler SDXに適用されている現在のZ-Capライセンスが特定の期間有効である場合は、Flexedライセンスで受け取ったZ-Capライセンスを適用する必要があります。Flexedソフトウェアライセンスには、NetScaler Flexed MPX/SDX/VPX/VPX FIPSソフトウェアインスタンスとNetScaler Flexed Platinum帯域幅ライセンスが含まれます。
2. 展開で使用しているNetScalerフォームファクターの NetScaler Consoleに、Flexedライセンスを適用する必要があります。例：

   NetScaler SDXフォームファクターを使用している場合は、次のライセンスを適用します。

   |ライセンスファイル|適用先| |-|-| |NetScaler Flexed SDX SW インスタンス|NetScaler コンソール| |NetScaler Flexed VPX SW インスタンス|NetScaler コンソール| |NetScaler Flexed プラチナム BW|NetScaler コンソール| |ADC Zero Capacity SDX-Z プラットフォーム|NetScaler SDX|

   NetScaler MPXフォームファクターを使用している場合は、次のライセンスを適用します。

   |ライセンスファイル|適用先| |-|-| |NetScaler Flexed MPX SW インスタンス|NetScaler コンソール| |ネットスケーラー フレックスド プラチナ BW|NetScaler コンソール| |ADC Zero Capacity MPX-Z プラットフォーム|NetScaler MPX|

   NetScaler VPX、NetScaler BLX、または NetScaler CPX フォームファクターを使用している場合は、以下のライセンスを適用します。

   |ライセンスファイル|適用先| |-|-| |NetScaler Flexed VPX SW インスタンス|NetScaler コンソール| |NetScaler フレックスド プラチナ BW|NetScaler コンソール|

   NetScaler VPX FIPS フォームファクターを使用している場合は、以下のライセンスを適用します。

   |ライセンスファイル|適用対象| |-|-| |NetScaler Flexed VPX FIPS SW インスタンス|NetScaler コンソール| |NetScaler フレックスド プラチナ BW|NetScaler コンソール|

### ライセンスファイルを適用する

ライセンスの追加、削除、ダウンロードが可能です。ライセンスは使用する前に適用する必要があります。

1. **NetScaler Licensing > License Management**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **License Files**セクションで、**Add License File**をクリックし、次のいずれかのオプションを選択します。

   - **Upload license files from a local computer**: ライセンスファイルがすでにローカルコンピューターにある場合は、NetScaler Consoleにアップロードできます。
   - **Use license access code**: Citrixから購入したライセンスのライセンスアクセスコードを指定します。**Get Licenses**をクリックし、次に**Finish**をクリックします。

3. **Finish**をクリックします。 ライセンスファイルがNetScaler Consoleに追加されます。 **License Expiry Information**セクションには、NetScaler Consoleに存在するライセンス、その数、および有効期限までの残り日数が表示されます。

   次のスクリーンショットは、Flexed NetScaler VPX、NetScaler MPX、NetScaler SDX、およびNetScaler VPX FIPSソフトウェアインスタンスライセンスの数、存在するFlexedプレミアム帯域幅容量、および有効期限までの日数（契約終了日）を示しています。

   Flexed ライセンスの有効期限(/en-us/netscaler-application-delivery-management-software/media/flexed-license-expiry.png)

   次のスクリーンショットは、利用可能なプールされたStandard、Advanced、およびPremium帯域幅、および有効期限までの日数（契約終了日）を示しています。

   

4. ライセンスファイルを選択し、**ライセンスを適用**をクリックします。

#### ライセンスファイルを削除する

ライセンスファイルを削除するには、1つ以上のファイルを選択し、**削除**をクリックします。ライセンスを削除する場合、まずライセンスを追加し、その後で適用できます。

#### ライセンスファイルをダウンロードする

ライセンスファイルをダウンロードするには、ファイルを選択し、**ダウンロード**をクリックします。ライセンスファイルをオフラインでバックアップとして保存できます。

### ライセンスサーバーのポート設定

ポートは、NetScalerインスタンスがライセンスサーバーと通信するために使用されます。**編集**アイコンをクリックし、以下のパラメーターの値を指定します。

- **ライセンスサーバーポート**: NetScalerインスタンスがライセンス割り当てのためにCitrixライセンスポータルにアクセスする際に使用するプロキシサーバーポート。デフォルト値: 27000。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ベンダーデーモンポート**: NetScalerインスタンスがライセンスサーバーと通信するために使用するライセンスサーバーポート。デフォルト値: 7279。
- **プロキシサーバーポート**: NetScaler Consoleは、NetScalerインスタンスがMyCitrix Portalにアクセスして自動ライセンス取得を行うためのフォワードHTTPプロキシとして使用できます。この機能を有効にするには、プロキシがリッスンするTCPポートを指定します。

### ライセンスの有効期限情報

FlexedまたはPooledキャパシティライセンスの有効期限しきい値を設定できるようになりました。しきい値が設定されている場合、ライセンスの有効期限が近づくと、NetScaler Consoleはメールまたは SMSを使用して通知を送信します。ライセンスがNetScaler Consoleで期限切れになった場合も、SNMPトラップと通知が送信されます。

ライセンスの有効期限通知が送信されるとイベントが生成され、このイベントはNetScaler Consoleの**インフラストラクチャ > イベント**から表示できます。

#### ライセンスの有効期限を表示

1. 「**NetScaler Licensing > License Management**」に移動します。
2. **License Settings**ページにある**License Expiry Information**セクションで、期限切れになるライセンスの詳細を確認できます。
   - **機能**: 期限切れになるライセンスの種類。
   - **カウント**: 影響を受ける仮想サーバーまたはインスタンスの数。
   - **有効期限までの日数**: ライセンスの有効期限（契約終了日）までの日数。

**注:**

新しいライセンスをプールに追加すると、NetScalerインスタンスは既存のライセンスの有効期限が切れたときに新しいライセンスを使用します。

### 通知設定

ライセンスの割り当てと有効期限までの日数に関する通知が送信される設定を指定します。

1. **Notification Settings**セクションで、**Edit**アイコンをクリックし、**Notify me on license usage**を選択します。通知を送信するために割り当てられるFlexedまたはPooledライセンス容量の割合としてアラートしきい値を設定します。
2. ライセンスがしきい値に達したとき、または期限切れになる場合に送信する通知の種類を、適切なチェックボックスを選択して選びます。通知の種類は次のとおりです。通知の種類を選択

© 1997–2026 Citrix Systems, Inc. All rights reserved.

し、**Add**をクリックして詳細を追加します。設定を保存する前に、各通知が配信されることをテストすることもできます。

- **メール**: 通知を送信するためのメールプロファイルまたは配布リスト。詳細については、「メール配布リストの作成」を参照してください。
- **SMS**: 通知を送信するためのSMSプロファイルまたは配布リスト。
- **Slack**: 通知を送信するためのSlackプロファイルの詳細。
- **PagerDuty**: 通知を送信するためのPagerDutyプロファイル。
- **ServiceNow**: Citrix ServiceNowプロファイルはデフォルトで指定されており、現在利用可能な唯一のオプションです。 これらのプロファイルの作成に関する詳細については、通知の設定を参照してください。

3. 有効期限までの日数を指定します。これは、ライセンスの有効期限について通知を受けたい日数です。
4. **保存**をクリックします。

### メール配信リストを作成する

メール配信リストを作成するには、次の手順を実行します。

1. **メール**を選択し、**追加**をクリックします。
2. **メール配信リストの作成**で、次の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **メールサーバー** - メール通知を送信するメールサーバーを選択します。メールサーバーを追加するには、をクリックします。サーバー名/IPアドレスとポートを指定します。メールサーバーへのアクセスに認証を必須にするには、を選択します。メールサーバーがSSL認証をサポートしている場合は、を選択します。をクリックします。
   - **差出人** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
   - **宛先** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
   - **Cc** - NetScaler Consoleがメッセージをコピーするメールアドレスを指定します。
   - **Bcc** - NetScaler Consoleがメッセージをブラインドカーボンコピー（メールアドレスを表示しない）するメールアドレスを指定します。
3. **作成**をクリックします。

### SMS配信リストを作成する

SMS通知設定を構成するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **SMS**で、**追加**をクリックします。
2. **SMS配信リストの作成**で、次の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **SMSサーバー** - SMS通知を送信するSMSサーバーを選択します。SMSサーバーを追加するには、**追加**をクリックします。サーバーの詳細を指定し、**作成**をクリックします。
   - **宛先** - NetScaler Consoleがメッセージを送信する電話番号を指定します。
3. **作成**をクリックします。

### Slackプロファイルの作成

Slackプロファイルを作成するには、次の手順を実行します。

1. **Slack**で、**追加**をクリックします。
2. **Slackプロファイルの作成**で、次の詳細を指定します。
   - **プロファイル名** - プロファイル名を指定します。この名前はSlackプロファイルリストに表示されます。
   - **チャネル名** - NetScaler Consoleが通知を送信するSlackチャネル名を指定します。
   - **Webhook URL** - チャネルのWebhook URLを指定します。受信Webhookは、外部ソースからSlackにメッセージを投稿する簡単な方法です。URLはチャネル名に内部的にリンクされています。このURLに送信されるすべてのイベント通知は、指定されたSlackチャネルに投稿されます。Webhookの例は次のとおりです。`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`。

### PagerDutyプロファイルの作成

PagerDutyを使用すると、登録された番号に電子メール、SMS、プッシュ通知、電話で通知を設定できます。NetScaler ConsoleにPagerDutyプロファイルを追加する前に、PagerDutyで必要な設定が完了していることを確認してください。PagerDutyの利用を開始するには、PagerDutyのドキュメントを参照してください。

PagerDutyプロファイルを作成するには、次の手順を実行します。

1. 「**PagerDuty**」で、「**Add**」をクリックします。
2. 「**Create PagerDuty Profile**」で、次の詳細を指定します。
   - **Profile Name** - プロファイル名を指定します。この名前は、イベントルールやSSL通知などのさまざまなモジュールでPagerDutyアラートを送信するために使用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Integration Key** - 統合キーを指定します。このキーはPagerDutyポータルから取得できます。

3. 「**Create**」をクリックします。

詳細については、PagerDutyのドキュメントにある「Services and Integrations」を参照してください。

#### ServiceNowプロファイルの表示

NetScalerイベントおよびNetScaler ConsoleイベントのServiceNow通知を有効にするには、ITSMコネクタを使用してNetScaler ConsoleをServiceNowと統合する必要があります。詳細については、「Integrate NetScaler Console with the ServiceNow instance」を参照してください。

ServiceNowプロファイルを表示および確認するには、次の手順を実行します。

1. 「**ServiceNow**」では、「**Citrix_Workspace_SN**」プロファイルがデフォルトで選択されています。
2. 「**Test**」をクリックしてServiceNowチケットを自動生成し、構成を確認します。

**注:**

さまざまな種類のNetScalerライセンスについては、「Licensing overview」を参照してください。

## FlexedおよびPooledライセンスの最小および最大容量

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexed licenses (CPL/UHMC)、従来のNetScaler Pooled licenses、およびNetScaler Fixed term Bandwidth licensesをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-prem リリース14.1-51.x以降および13.1-60.x以降から非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScaler Flexedライセンスは、ライセンスサーバーとして構成されたNetScaler Consoleを使用して、Flexedライセンス（帯域幅プールライセンスとインスタンスプールライセンス）を管理します。

帯域幅プールとインスタンスプールからライセンスをチェックアウトする際、ゼロキャパシティハードウェア上のNetScalerフォームファクターとハードウェアモデル番号によって、以下が決定されます。

- NetScalerインスタンスが機能する前にチェックアウトする必要がある最小帯域幅とインスタンス数。
- NetScalerがチェックアウトできる最大帯域幅とインスタンス数。
- 各帯域幅チェックアウトの最小帯域幅単位。最小帯域幅単位とは、NetScalerがプールからチェックアウトする必要がある帯域幅の最小単位です。すべてのチェックアウトは、最小帯域幅単位の整数倍である必要があります。たとえば、NetScalerの最小帯域幅単位が1 Gbpsの場合、1000 Mbpsはチェックアウトできますが、200 Mbpsや150.5 Gbpsはチェックアウトでき

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ません。最小帯域幅単位は、最小帯域幅要件とは異なります。NetScalerインスタンスは、少なくとも最小帯域幅でライセンスが付与された後にのみ動作できます。最小帯域幅が満たされると、インスタンスは最小帯域幅単位の倍数でさらに帯域幅をチェックアウトできます。

表1から5は、サポートされているすべてのNetScalerインスタンスの最大帯域幅/インスタンス、最小帯域幅/インスタンス、および最小帯域幅単位をまとめたものです。表6は、サポートされているすべてのNetScalerインスタンスの異なるフォームファクターのライセンス要件をまとめたものです。以下の表はシステム要件を示しています。

**注:**

NetScaler CPX/BLX/VPXの最小帯域幅チェックアウト単位は10 Mbpsです。NetScaler MPX/SDXの最小帯域幅チェックアウト単位は1 Gbpsです。

## 表1. MPXでサポートされるFlexed容量

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小帯域幅単位 |
|---|---|---|---|
| **MPX 5900Z** | 1 | 10 | 1 ギガビーピーエス |
| **MPX 8900Z** | 5 | 30 | 1 ギガビット/秒 |
| **MPX 8900Z FIPS** | 5 | 20 | 1 ギガビット/秒 |
| **MPX 9100Z** | 10 | 95 | 1 ギガビット/秒 |
| **MPX 9200** | 10 | 95 | 1 ギガビット/秒 |
| **MPX 9100Z FIPS** | 10 | 95 | 1 ギガbps |
| **MPX 14000Z** | 20 | 100 | 1 ギガbps |
| **MPX 14000Z-40G** | 20 | 100 | 1 ギガbps |
| **MPX 14000Z-40S** | 40 | 100 | 1 ギガビット/秒 |
| **MPX 14000Z FIPS** | 30 | 80 | 1 ギガビット/秒 |
| **MPX 15000Z** | 20 | 120 | 1 ギガビット/秒 |
| **MPX 15000Z-50G** | 20 | 120 | 1 ギガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小帯域幅単位 |
|---|---|---|---|
| **MPX 15000Z FIPS** | 30 | 120 | 1 ギガビーピーエス |
| **MPX 16000Z** | 30 | 250 | 1 ギガビーピーエス |
| **MPX 22000Z** | 40 | 120 | 1 ギガビーピーエス |
| **MPX 24000Z** | 100 | 150 | 1 ギガビーピーエス |
| **MPX 25000Z** | 100 | 160 | 1 ギガbps |
| **MPX 25000Z-40G** | 100 | 200 | 1 ギガbps |
| **MPX 26000Z** | 100 | 200 | 1 ギガビット/秒 |
| **MPX 26000Z-50S** | 100 | 200 | 1 ギガビット/秒 |
| **MPX 26000Z-100G** | 100 | 200 | 1 ギガビーピーエス |

## 表2A. ビルド13.0-47.xより前のNetScaler SDXバージョンでサポートされるFlexed容量

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小インスタンス | 最大インスタンス | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 8900Z** | 10 | 30 | 2 | 7 | 1 ギガビーピーエス |
| **SDX 14000Z** | 20 | 100 | 5 | 25 | 1 ギガビーピーエス |
| **SDX 14000Z-40G** | 40 | 100 | 20 | 25 | 1 ギガビーピーエス |
| **SDX 15000Z** | 20 | 120 | 5 | 55 | 1 ギガビーピーエス |
| **SDX 15000Z-50G** | 20 | 120 | 5 | 55 | 1 ギガビーピーエス |
| **SDX 22000Z** | 40 | 120 | 80 | 80 | 1 ギガビーピーエス |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小インスタンス | 最大インスタンス | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 24000Z** | 100 | 150 | 80 | 80 | 1 ギガビーピーエス |
| **SDX 25000Z** | 100 | 200 | 20 | 115 | 1 ギガビーピーエス |
| **SDX 25000Z-40G** | 100 | 200 | 20 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z** | 100 | 200 | 20 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z-50S** | 100 | 200 | 20 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z-100G** | 100 | 200 | 20 | 115 | 1 ギガビット/秒 |

## 表2B. NetScaler SDX バージョン13 (ビルド13.0-47.x以降)、バージョン13.1 (ビルド51.xより前)、およびバージョン14.1 (ビルド12.xより前) のサポートされるFlexed容量

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 8900Z** | 5 | 30 | 1 | 7 | 1 ギガビット/秒 |
| **SDX 9100Z** | 10 | 95 | 2 | 7 | 1 ギガビット/秒 |
| **SDX 14000Z** | 10 | 100 | 2 | 25 | 1 ギガbps |
| **SDX 14000Z-40G** | 20 | 100 | 10 | 25 | 1 ギガbps |
| **SDX 15000Z** | 10 | 120 | 2 | 55 | 1 ギガbps |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 15000Z-50G** | 10 | 120 | 2 | 55 | 1 ギガビット/秒 |
| **SDX 16000Z** | 15 | 250 | 10 | 55 | 1 ギガビット/秒 |
| **SDX 22000Z** | 20 | 120 | 40 | 80 | 1 ギガビーピーエス |
| **SDX 24000Z** | 50 | 150 | 40 | 80 | 1 ギガビーピーエス |
| **SDX 25000Z** | 50 | 200 | 10 | 115 | 1 ギガビーピーエス |
| **SDX 25000Z-40G** | 50 | 200 | 10 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z** | 50 | 200 | 10 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z-50S** | 50 | 200 | 10 | 115 | 1 ギガビーピーエス |
| **SDX 26000Z-100G** | 50 | 200 | 10 | 115 | 1 ギガビーピーエス |

## 表 2C. NetScaler SDX バージョン 13.1 (ビルド 51.x 以降) およびバージョン 14.1 (ビルド 12.x 以降) でサポートされるFlexed容量

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 8900Z** | 5 | 30 | 1 | 7 | 1 ギガビーピーエス |
| **SDX 9200Z** | 10 | 95 | 1 | 7 | 1 ギガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最小帯域幅 (GBPS) | 最大帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 9100Z** | 10 | 95 | 1 | 7 | 1ギガbps |
| **SDX 14000Z** | 10 | 100 | 1 | 25 | 1ギガbps |
| **SDX 14000Z-40G** | 20 | 100 | 1 | 25 | 1 ギガビット/秒 |
| **SDX 15000Z** | 10 | 120 | 1 | 55 | 1 ギガビット/秒 |
| **SDX 15000Z-50G** | 10 | 120 | 1 | 55 | 1 ギガビット/秒 |
| **SDX 16000Z** | 30 | 250 | 1 | 55 | 1 ギガビット/秒 |
| **SDX 17000Z** | 30 | 350 | 1 | 55 | 1 ギガビット/秒 |
| **SDX 22000Z** | 20 | 120 | 1 | 80 | 1 ギガビット/秒 |
| **SDX 24000Z** | 50 | 150 | 1 | 80 | 1 ギガビット/秒 |
| **SDX 25000Z** | 50 | 200 | 1 | 115 | 1 ギガビット/秒 |
| **SDX 25000Z-40G** | 50 | 200 | 1 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z** | 50 | 200 | 1 | 115 | 1 ギガビーピーエス |
| **SDX 26000Z-50S** | 50 | 200 | 1 | 115 | 1 ギガビーピーエス |
| **SDX 26000Z-100G** | 50 | 200 | 1 | 115 | 1 ギガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注記:**

- 最小購入数量は、最小システム要件とは異なる場合があります。
- ビルド14.1-12.x以降を実行しているNetScaler SDXでは、Flexedライセンスを使用する場合、最小数のインスタンスライセンスをチェックアウトするという制限が解除されます。つまり、最小1つのインスタンスライセンスをチェックアウトできます。

## 表3. NetScaler CPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **CPX** | 10 | 10 | 1 | 1 | 10 メガビット/秒 |

## 表4. ハイパーバイザーおよびクラウドサービス上のNetScaler VPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス数

| ハイパーバイザー/クラウドサービス | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **シトリックス ハイパーバイザー** | 40 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **ヴイエムウェア ESXI** | 100 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **リナックス KVM** | 100ギガビーピーエス | 10メガビーピーエス | 1 | 1 | 10 メガビット/秒 |
| **Microsoft Hyper-V** (マイクロソフト ハイパーブイ) | 3 ギガbps | 10 メガbps | 1 | 1 | 10 メガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ハイパーバイザー/クラウドサービス | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **AWS** | 30 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **アジュール** | 10ギガビット/秒 | 10メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **グーグル クラウド** | 10 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |

注

最小購入数量は、最小システム要件とは異なります。

## 表5. NetScaler BLXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **BLX** | 100 | 10 | 1 | 1 | 10 メガビット/秒 |

## 表 6. 異なるフォームファクターのゼロキャパシティライセンス要件

| 製品ライン | ゼロキャパシティハードウェア |
|---|---|
| **MPX** | ライセンスが必要 |
| **SDX** | ライセンスが必要 |
| **VPX** | - |
| **CPX** | - |
| **BLX** | - |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Flexed容量ライセンス

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASがNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console オンプレミス のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console オンプレミス リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console オンプレミス リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console オンプレミス 13.1はLASをサポートしていないため、15th April 2026までにConsole オンプレミス リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負う

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScaler Flexedライセンスは、ライセンス管理プロセスを簡素化することを目的とした新しいライセンスフレームワークです。Flexedライセンスには、ソフトウェアインスタンスライセンス（VPX/CPX/BLX、SDX、MPX、およびVPX FIPS）と帯域幅容量ライセンスが含まれます。

**License Activation Service (LAS)** - Cloud Connect展開でLASをアクティベートして、NetScaler Console On-premでFlexedエンタイトルメントを表示できるようにします。その後、NetScaler Console On-premで任意のNetScalerフォームファクターに割り当てます。

**手動で管理されるエンタイトルメント（ファイルベースのライセンス）** - Flexedライセンスを NetScaler Console on-premに直接適用します。また、MPX Z-CapおよびSDX Z-Capライセンスをそれぞれの NetScaler MPXおよびNetScaler SDXハードウェアに適用する必要があります。その後、これらのエンタイトルメントを、クラウドおよびオンプレミス展開の両方で、すべての NetScalerフォームファクターに割り当てることができます。

Flexedライセンスは、無制限の仮想サーバーに対する分析機能も提供します。

プール型ライセンスをお持ちで、新たにFlexedライセンスを購入された場合、Flexedライセンスダッシュボードでライセンスの詳細を確認できます。合計帯域幅とインスタンスは、Flexedライセンスダッシュボードに表示されます。

帯域幅ライセンスには通常、Premiumエディションのみが含まれますが、以前にプール型StandardまたはAdvancedライセンスをお持ちだった場合は、Standard、Advanced、およびPremiumエディションがFlexedライセンスダッシュボードに表示されます。

Flexedおよびプール型帯域幅とインスタンスライセンス(/en-us/netscaler-application-delivery-management-software/media/flexed-pooled-bw-instance-license.png)

詳細については、「Flexedライセンスダッシュボード」を参照してください。

Flexedライセンスを使用すると、インスタンスに必要な帯域幅を、必要以上に割り当てないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられた帯域幅を増減できます。

## ゼロキャパシティハードウェア

NetScaler® Flexedライセンスを通じて管理される場合、MPXおよびSDXインスタンスは「ゼロキャパシティハードウェア」と呼ばれます。これは、これらのインスタンスが帯域幅プールからリソースをチェックアウトするまで機能できないためです。したがって、これらのプラットフォームはMPX-ZおよびSDX-Zアプライアンスとも呼ばれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ゼロキャパシティハードウェアは、共通プールから帯域幅をチェックアウトするためにZ-capライセンスを必要とします。

**注：**

- ゼロキャパシティライセンスのインストールは、他のNetScalerローカルライセンスと同様に機能します。ゼロキャパシティライセンスの取得とインストール方法の詳細については、「NetScalerのライセンスガイド」を参照してください。

### Z-capライセンスの管理とインストール

Z-capライセンスは、ハードウェアのシリアル番号またはライセンスアクセスコードを使用して手動でインストールする必要があります。Z-capライセンスがインストールされると、ハードウェアにロックされ、オンデマンドでNetScalerハードウェアインスタンス間で共有することはできません。ただし、Z-capライセンスを別のNetScalerハードウェアインスタンスに手動で移動することはできます。

NetScalerソフトウェアリリース11.1ビルド54.14以降を実行しているNetScaler MPXインスタンスと、11.1ビルド58.13以降を実行しているNetScaler SDXインスタンスは、NetScaler Flexedライセンスをサポートしています。詳細については、「Flexedおよびプール型ライセンスの最小および最大容量」の表1および表2を参照してください。

**注：**

LASベースのライセンスを使用する場合、Z-Capライセンスを適用する必要はありません。

## スタンドアロンNetScaler VPXインスタンス

NetScalerソフトウェアリリース11.1 Build 54.14以降を実行しているNetScaler VPXインスタンスは、以下のハイパーバイザーでFlexedライセンスをサポートしています。

- ヴイエムウェア ESX 6.0
- シトリックス ハイパーバイザー™
- リナックス KVM

NetScalerソフトウェアリリース12.0 Build 51.24以降を実行しているNetScaler VPXインスタンスは、以下のハイパーバイザーおよびクラウドプラットフォームでFlexedライセンスをサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- マイクロソフト Hyper-V
- AWS
- マイクロソフト Azure
- グーグル クラウド

NetScalerソフトウェアリリース13.0および13.1（すべてのバージョン）を実行しているNetScaler VPXインスタンスは、以下のハイパーバイザーおよびクラウドプラットフォームでFlexedライセンスをサポートしています。

- ヴイエムウェア ESX 6.0
- シトリックス ハイパーバイザー
- リナックス KVM
- マイクロソフト ハイパーV
- AWS
- マイクロソフト アジュール
- グーグル クラウド

**注:**

NetScaler ConsoleとMicrosoft AzureまたはAWS間の通信を有効にするには、IPSECトンネルを構成する必要があります。詳細については、「クラウドに展開されたNetScaler VPXインスタンスをNetScaler Consoleに追加する」を参照してください。ゼロキャパシティハードウェアとは異なり、NetScaler VPXはゼロキャパシティライセンスを必要としません。トラフィックを処理するには、プールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

## スタンドアロンNetScaler CPXインスタンス

Dockerホストに展開されたNetScaler CPXインスタンスは、Flexedライセンスをサポートしています。ゼロキャパシティハードウェアとは異なり、NetScaler CPXはZ-capライセンスを必要としません。最大1 Gbpsのスループットを消費する単一のNetScaler CPXインスタンスは、ライセンスプールから1インスタンスのみをチェックアウトし、帯域幅はチェックアウトしません。たとえば、20 Gbpsの帯域幅プールを持つ20個のNetScaler CPXインスタンスがあるとします。NetScaler CPXインスタンスの1つが500 Mbpsのスループットを消費しても、残りの19個のNetScaler CPXインスタンスの帯域幅プールは20 Gbpsのままです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

同じNetScaler CPXインスタンスが1500 Mbpsのスループットを消費し始めた場合、帯域幅プールは残りの19個のNetScaler CPXインスタンスに対して19.5 Gbpsになります。

Flexedライセンスの場合、帯域幅は10 Mbpsの倍数でのみ追加できます。

## スタンドアロンNetScaler BLXインスタンス

NetScaler BLXインスタンスはFlexedライセンスをサポートしています。NetScaler BLXインスタンスはZ-capライセンスを必要としません。トラフィックを処理するには、NetScaler BLXインスタンスはプールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

## 帯域幅プール

帯域幅プールは、物理および仮想の両方のNetScalerインスタンスで共有できる総帯域幅です。帯域幅プールは、Premiumソフトウェアエディション用のプールで構成されます。PooledライセンスからFlexedライセンスに移行する場合、Standard、Advanced、Premiumソフトウェアエディションが混在している可能性があります。特定のNetScaler MPX/VPX/CPX/BLXインスタンスは、異なるプールから帯域幅を同時にチェックアウトすることはできません。帯域幅をチェックアウトできる帯域幅プールは、ライセンスされているソフトウェアエディションによって異なります。

## インスタンスプール

ソフトウェアインスタンスプールには3つのタイプがあります。

- VPX/CPX/BLX ソフトウェアインスタンス
- MPX ソフトウェアインスタンス（MPX FIPS にも同じプールが適用されます）
- SDX ソフトウェアインスタンス（SDX FIPS にも同じプールが適用されます）
- VPX FIPS ソフトウェアインスタンス

プールからチェックアウトされると、ライセンスはソフトウェアインスタンスのリソース（CPU/PE、SSLコア、1秒あたりのパケット数、帯域幅など）をアンロックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# ライセンスの構成

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026 にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix 製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026 以降、NetScaler インスタンスをアクティベートおよびライセンス供与する唯一の方法は LAS となり、NetScaler Flexed ライセンス (CPL/UHMC)、従来の NetScaler Pooled ライセンス、および NetScaler Fixed term Bandwidth ライセンスをサポートします。サポートを継続するには、NetScaler および NetScaler Console の展開が LAS 互換バージョンである必要があります。

LAS 互換の NetScaler の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console オンプレミスでの LAS サポートは、リリース 14.1-51.x 以降です。ただし、ファイルベースのライセンスは、Console オンプレミスリリース 14.1-51.x 以降および 13.1-60.x 以降では April 15 2026 をもって非推奨となります。Console オンプレミスリリース 14.1-51.x またはリリース 13.1-60.x 以降にアップグレードした場合、15th April 2026 までファイルベースのライセンスを引き続き使用できます。ただし、Console オンプレミス 13.1 は LAS をサポートしていないため、15th April 2026 までに Console オンプレミスリリース 14.1-51.x 以降にアップグレードし、LAS に切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他の従来の NetScaler ライセンスはすべて LAS ではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用している NetScaler インスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LAS ベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrix は、これらの要件を遵守しない場合、Citrix が法律上または衡平法上持つその他の救済措置に加えて、責任を負

© 1997–2026 Citrix Systems, Inc. All rights reserved.

うことなく Citrix Maintenance を制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
続行する前に、以下の注記をお読みください。

**注:**

プールライセンスをお持ちで、Flexed ライセンスを購入して適用した場合、結合されたエンタイトルメントは Flexed ライセンスダッシュボードに表示されます。

NetScaler Flexedライセンスを使用すると、さまざまなNetScalerフォームファクター間で帯域幅またはインスタンスライセンスを共有できます。このFlexed容量は、データセンターまたはパブリッククラウドにあるインスタンスに使用します。インスタンスがリソースを必要としなくなった場合、割り当てられた容量は共通プールに返却されます。解放された容量は、リソースを必要とする他のNetScalerインスタンスで再利用できます。

Flexedライセンスを使用すると、インスタンスに必要な帯域幅を割り当て、必要以上の割り当てを行わないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられた帯域幅を増減できます。

NetScaler Consoleでは、次のタスクを実行できます。

- **LASの場合:**
  a. Cloud Connectを使用してLicense Activation Service (LAS) をアクティブ化します。
  b. Consoleオンプレミスライセンスサーバーにライセンスエンタイトルメントが表示されたら、NetScalerインスタンスのライセンスをチェックアウトします。
  c. ライセンスが各インスタンスの最小および最大容量に基づいていることを確認します。
- **ファイルベースのライセンスの場合:**
  a. 帯域幅とソフトウェアインスタンスプールを含むFlexedライセンスを、NetScaler Console オンプレミスライセンスサーバーにアップロードします。
  b. SDXまたはMPXのゼロ容量ライセンスをそれぞれのハードウェアに直接アップロードします。
  c. 必要に応じて、ライセンスプールからNetScalerインスタンスにライセンスを割り当てます。ライセンスをチェックアウトする際は、インスタンスの最小および最大容量に基づいていることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

帯域幅、インスタンス、ゼロ容量 (Z-cap) ライセンスを含むすべてのFlexedライセンスは、citrix.com Webサイトからダウンロードできます。詳細については、「NetScaler®のライセンスガイド」を参照してください。

## LASベースのライセンス

LASを使用する場合、外部エージェントはオプションです。インスタンスがNetScaler Consoleからライセンスをチェックアウトできるように、ポート443が利用可能であることを確認してください。詳細については、「システム要件」を参照してください。

### ステップ1: LASをアクティブ化し、エンタイトルメントを取得する

1. **Cloud Connect**を使用してLASをアクティブ化します。

   詳細については、「ライセンスアクティベーションサービスをアクティブ化する」を参照してください。

   アクティブ化されると、FlexedおよびPooledライセンスエンタイトルメントが**License Management > LAS**に表示されます。

   。

### ステップ2：NetScaler Console On-premにNetScalerインスタンスを追加する

NetScalerインスタンスがライセンスを受け取れるように、NetScaler Console On-premに追加されていることを確認してください。インスタンスの追加の詳細については、「NetScaler Console On-premにNetScalerインスタンスを追加する」を参照してください。

### ステップ3：NetScalerインスタンスのライセンス供与または移行

1. **Licensing management > LAS**に移動します。
2. **License with LAS or Migrate to LAS**をクリックします。

   詳細については、「ライセンスアクティベーションサービス」を参照してください。

### ステップ4：Flexedスループット容量の編集

インスタンスのライセンス供与後、割り当てられたスループット容量を変更します。

1. **NetScaler Licensing > Flexed Licensing > Dashboard**に移動します。
2. **LAS managed entitlements**タブを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Licensed NetScalers**セクションで、インスタンスを選択し、**Edit Throughput Capacity**をクリックします。
4. 「**Allocate**」列に新しい容量を入力し、「**Submit**」をクリックします。

### ライセンスのないMPXアプライアンスの特別なライセンス

ライセンスのないMPXがNetScaler Consoleオンプレミスに直接、またはエージェントを介して接続されている場合、HTTPS接続はサポートされません。その結果、手順2は実行できません。代わりに、NetScalerに移動して以下の手順を完了してください。

**前提条件:** NetScaler MPXがNetScaler Consoleオンプレミスに直接（つまり、エージェントなしで）接続されている場合は、NetScaler Consoleオンプレミスで基本認証が有効になっていることを確認してください。初期設定後（つまり、NetScaler ConsoleオンプレミスでNetScaler MPXを管理およびライセンス供与した後）、セキュリティ上の理由からこの基本認証設定を無効にすることができます。

1. NetScaler GUIにログインします。
2. **システム > ライセンス > ADCライセンス > ライセンスの管理 > 新しいライセンスの追加** に移動します。
3. **Licenses** ページで、**Use remote licensing** ラジオボタンを選択し、**Remote Licensing Mode** から **LAS** モードを選択します。
4. **Server Name/IP address** フィールドに、NetScaler Console外部エージェントのIPアドレスを入力します。
5. インスタンスをNetScaler Consoleに登録するための資格情報を入力し、**Continue** をクリックします。

   **注**: 検証用のデジタル証明書をお持ちの場合は、Validate Certificateチェックボックスをオンにします。
6. **Device Profile Name** フィールドに、NetScaler Consoleがインスタンスにアクセスするために使用するインスタンスプロファイルを入力します。このプロファイルには、追加するインスタンスのユーザー名とパスワードが保持されます。デフォルトのプロファイルは ns_nsroot_profileです。ただし、デフォルトの管理者資格情報を変更した場合は、カスタムインスタンスプロファイル名を定義するようにしてください。
7. **Allocate licenses** で、ライセンスエディションを選択し、必要な帯域幅を指定します。NetScalerで初めてライセンスを割り当てる場合、後でNetScaler Console GUIから直接割り当てを変更または解放できます。
8. **Get Licenses** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

変更を有効にするには、ライセンスエディションを変更した後、インスタンスのウォームリスタートを実行します。

### ライセンスアクティベーションブロブの動作

NetScalerインスタンスがオンプレミスのConsoleから**License with LAS or Migrate to LAS**の一部として取得するライセンスアクティベーションブロブは、30日間有効です。NetScalerがオンプレミスのConsoleとの接続を失い、その後再確立した場合、ライセンスアクティベーションブロブはすぐに復元されます。

NetScalerが最大24時間オンプレミスのConsoleに再接続できない場合、猶予期間に入ります。 デフォルトでは、ライセンスアクティベーションブロブは8時間ごとに更新されます。24時間以内に8時間ごとの更新試行が3回連続で失敗した場合、NetScalerは猶予期間に入ります。

### ライセンス猶予期間アラート

ライセンス猶予期間アラートのタッチポイントは次のとおりです。

- Flexedダッシュボードに、インスタンスが猶予期間中であり、ライセンスアクティベーションブロブの有効期限が切れるまでの残り日数を示す警告アイコンが表示されます。
- 管理者がNetScalerインスタンスのGUIにログインするたびに、インスタンスが猶予期間中であり、ライセンスアクティベーションブロブの有効期限が切れるまでの残り日数を示すポップアップメッセージが表示されます。
- 設定されたメールアドレスにメール通知が送信されます。詳細については、「メール設定の構成」を参照してください。

**注:** ライセンス関連のメール通知を受信するには、システムイベントカテゴリで**ライセンス**を選択してください。

## 手動で管理されるエンタイトルメント（ファイルベースライセンス）

### はじめる前に

Flexedライセンスを構成する前に、次の前提条件が満たされていることを確認してください。

- ライセンスをチェックアウトするために、NetScalerからNetScaler Consoleへ`27000`および`7279`ポートに到達可能であることを確認してください。「システム要件」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ステップ1 - NetScaler Consoleでライセンスを適用する

1. **NetScaler® Licensing > License Management**に移動します。
2. 「**ライセンスファイル**」セクションで、「**ライセンスファイルの追加**」を選択し、次のいずれかのオプションを選択します。

   - **ローカルコンピューターからライセンスファイルをアップロードします。**ライセンスファイルがすでにローカルコンピューターに存在する場合は、NetScaler Consoleにアップロードできます。
   - **ライセンスアクセスコードを使用します。**Citrixから購入したライセンスのライセンスアクセスコードを指定します。次に、「**ライセンスの取得**」を選択します。その後、「**完了**」を選択します。

   **注:**

   いつでも、「**ライセンス設定**」からNetScaler Consoleにライセンスを追加できます。

3. 「**完了**」をクリックします。

   ライセンスファイルがNetScaler Consoleに追加されます。「**ライセンス有効期限情報**」セクションには、NetScaler Consoleに存在するライセンスと、有効期限までの残り日数が表示されます。

4. 「**ライセンスファイル**」で、適用したいライセンスファイルを選択し、「**ライセンスの適用**」をクリックします。

   このアクションにより、NetScalerインスタンスは選択したライセンスをFlexedライセンスとして使用できるようになります。

### ステップ2 - NetScaler Consoleをライセンスサーバーとして登録し、ライセンスを割り当てる

NetScaler ConsoleをNetScalerインスタンスのライセンスサーバーとして登録できます。

#### GUIを使用してNetScaler Consoleサーバーを登録する

NetScaler Console GUIで、NetScalerインスタンスに関連付けられたNetScaler Consoleサーバーを登録します。

1. NetScaler GUIにログインします。
2. **システム > ライセンス > ライセンスの管理**に移動します。
3. 「**新しいライセンスの追加**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**リモートライセンスの使用**」を選択し、「**リモートライセンスモード**」でリストから「**プールライセンス**」を選択します。
5. 「**サーバー名/IPアドレス**」フィールドに、NetScaler ConsoleサーバーのIPアドレスを指定します。
6. デフォルトのライセンスポートは27000です。
7. NetScaler Consoleサーバーの資格情報を入力してインスタンスをNetScaler Consoleに登録し、「**続行**」をクリックします。NetScaler Consoleでは、いずれかのサーバーがライセンスサーバーになります。

   NetScalerでのライセンス管理(/en-us/netscaler-application-delivery-management-software/media/upgrade-vpx-2.png)

   **注:**

   デジタル証明機関 (CA) 証明書を検証用に持っている場合にのみ、「**証明書の検証**」チェックボックスを選択します。

8. 「**デバイスプロファイル名**」で、NetScaler Consoleがインスタンスへのアクセスに使用できるインスタンスプロファイルを指定します。このインスタンスプロファイルには、NetScaler Consoleに追加するインスタンスのユーザー名とパスワードが含まれています。デフォルトのプロファイルは「**ns_nsroot_profile**」です。インスタンスのデフォルトの管理者資格情報を変更した場合は、カスタムインスタンスプロファイル名を定義できます。
9. 「**ライセンスの割り当て**」で、ライセンスエディションを選択し、必要な帯域幅を指定します。

   初めてNetScalerでライセンスを割り当てます。後でNetScaler Console GUIからライセンスの割り当てを変更または解放できます。

   NetScaler GUIからライセンスを割り当てる(/en-us/netscaler-application-delivery-management-software/media/allocate-licenses-from-adc-gui.png)

   「**ライセンスの取得**」をクリックします。

   **重要**

   ライセンスエディションを変更した場合は、インスタンスをウォーム再起動してください。インスタンスを再起動するまで、構成の変更は有効になりません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CLIを使用してNetScaler Consoleサーバーを追加する

NetScalerインスタンスにGUIがない場合は、以下のCLIコマンドを使用して、インスタンスに関連付けられたNetScaler Consoleサーバーを追加します。

1. NetScalerコンソールにログインします。
2. NetScaler Consoleに登録されている、関連付けられたNetScaler ConsoleサーバーのIPアドレスを追加します。デフォルトのライセンスポートは27000です。

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-license-port-number>
```

3. ライセンスサーバーで利用可能なライセンス帯域幅を表示します。

```
> sh ns licenseserverpool
```

4. 必要なライセンスエディションからライセンス帯域幅を割り当てます。

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth> edition <specify-license-edition>
```

**重要**

ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。

`reboot -w`
インスタンスを再起動するまで、構成の変更は有効になりません。

### ステップ3 - NetScalerインスタンスのFlexedスループット容量を編集する

1. **NetScaler Licensing > Flexed Licensing > Dashboard**に移動します。
2. **Licensed NetScalers**セクションで、インスタンスを選択し、**Edit Throughput Capacity**をクリックします。
3. **Edit Throughput Capacity**ページで、**Allocate**列に数値を入力します。
4. **Submit**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler MPX-Z

MPX-Zは、フレックスキャパシティ対応のNetScaler MPXアプライアンスです。MPX-Zは、Premium Editionライセンスのみの帯域幅プールをサポートしています。

MPX-Zは、ライセンスサーバーに接続する前にライセンスが必要です。MPX-Zライセンスは、次のいずれかの方法でインストールできます。

- ローカルコンピューターからライセンスファイルをアップロードする。
- インスタンスのハードウェアシリアル番号を使用する。
- インスタンスのGUIの**システム** > **ライセンス**セクションにあるライセンスアクセスコード。

MPX-Zライセンスを削除すると、MPXはライセンスなしの状態になります。ライセンスはライセンスサーバーに解放されます。

MPX-Zインスタンスの帯域幅は、再起動なしで動的に変更できます。再起動が必要なのは、ライセンスエディションを変更する場合のみです。

**注：**

インスタンスを再起動すると、構成された容量に必要なフレックスライセンスが自動的にチェックアウトされます。

### NetScaler SDX-Z

SDX-Zは、フレックスキャパシティ対応のNetScaler SDXアプライアンスです。SDX-Zは、Premium Editionライセンスの帯域幅とインスタンスプールをサポートしています。

SDX-Zは、ライセンスサーバーに接続する前にライセンスが必要です。SDX-Zライセンスは、次のいずれかの方法でインストールできます。

- ローカルコンピューターからライセンスファイルをアップロードする。
- インスタンスのハードウェアシリアル番号を使用する。
- インスタンスのGUIの**System** > **Licenses**セクションからのライセンスアクセスコード。

SDX-Zライセンスを削除すると、SDXはライセンスなしの状態になります。ライセンスはライセンスサーバーに解放されます。

再起動せずにSDX-Zインスタンスの帯域幅を動的に変更できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

インスタンスを再起動すると、設定された容量に必要なFlexedライセンスが自動的にチェックアウトされます。

### NetScaler高可用性ペアのライセンス要件（LASとファイルベースライセンスの両方に共通）

開始する前に、NetScaler Consoleサーバーがライセンスサーバーとして構成されていることを確認してください。詳細については、「NetScaler Consoleをライセンスサーバーとして構成する」を参照してください。

NetScaler HAペアに帯域幅を割り当てると、NetScaler Consoleは割り当てられた帯域幅をプライマリインスタンスにチェックアウトします。セカンダリインスタンスに対してもこのプロセスを繰り返す必要があります。

NetScaler HAペアにプールライセンスを割り当てるには、「NetScalerインスタンスにFlexedライセンスを割り当てる」を参照してください。

**Flexed Capacity**ページには、インスタンスとその割り当てられた容量が個別に表示されます。

### NetScaler Flexedライセンスの状態（LASとファイルベースライセンスの両方に共通）

Flexedライセンスの状態は、NetScalerインスタンスのライセンス要件を示します。Flexedライセンスで構成されたNetScalerインスタンスは、次のいずれかの状態を表示します。

- **割り当て済み**: インスタンスは適切なライセンス容量で実行されています。
- **猶予期間**: インスタンスは猶予期間中に実行されています。猶予期間は30日間で、その後インスタンスはライセンスなしの状態になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# フレックスライセンスダッシュボード

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  **注:** ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を負うことなくCitrixメンテナンスを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
続行する前に、以下の注記をお読みください。

**注:**

- 以前にプールライセンスをお持ちで、現在フレックスライセンスを購入して適用した場合、結合されたエンタイトルメントがフレックスライセンスダッシュボードに表示されます。
- プールライセンスのみをお持ちの場合は、プールライセンスダッシュボードを確認してください。
- Flexedライセンスのみをお持ちの場合、またはFlexedライセンスとプールライセンスの両方をお持ちの場合は、Flexedライセンスダッシュボードを確認してください。
- **ライセンス方法に基づく注意点:**
  - LASベースのライセンスを表示するには、**NetScaler® licenses > Flexed Licensing > Dashboard > LAS managed entitlements**タブに移動します。
  - 手動で管理されているエンタイトルメント（ファイルベースのライセンス）を表示するには、**NetScaler® licenses > Flexed Licensing > Dashboard > Manually managed entitlements**タブに移動します。
  - 両方のライセンスメカニズムを使用している場合は、両方のタブを参照してください。 Flexedライセンスダッシュボードでは、購入したスループット容量とインスタンスの包括的なビューが表示されます。

このページには、エディション全体のスループット容量と、MPX、VPX、SDXなどのさまざまなフォームファクターのインスタンスの詳細が表示されます。NetScaler MPXとNetScaler MPX FIPSは同じライセンスファイルを持っています。同様に、NetScaler SDXとNetScaler SDX FIPSも同じライセンスファイルを持っています。ただし、NetScaler VPX FIPSはNetScaler VPXとは異なるファイルを持ち、個別に表示されます。また、NetScaler VPX（SDX上のVPXを含む）、NetScaler BLX、およびNetScaler CPXにはNetScaler VPXライセンスが必要であり、VPXのエンタイトルメントと割り当ての一部です。Flexedライセンスはプレミアムエディションのみをサポートします。ただし、Flexedライセンスを購入し、以前にプールされたStandardまたはAdvanced帯域幅容量を持っていた場合、帯域幅容量（StandardまたはAdvanced）に関連する詳細もFlexedライセンスダッシュボードに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPX（SDX上のVPXを含む）、BLX、およびCPXフォームファクターには、NetScaler Flexed VPX SWインスタンスライセンスファイルが必要です。つまり、これらのフォームファクターは、Flexed VPX SWインスタンスライセンスのエンタイトルメントと割り当ての一部です。

ライセンスされたNetScalerインスタンスに関する詳細は、**Licensed NetScalers**セクションで確認できます。インスタンスを選択し、帯域幅を編集したり、そのインスタンスのライセンスを解放したりできます。

次のパラメータに基づいて結果をフィルタリングできます。

- スループット容量でフィルタリング
  - プレミアム
  - アドバンスト
  - スタンダード
- フォームファクター
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- ライセンスステータス
  - 接続が失われました
  - 猶予
  - 割り当て済み

## NetScalerインスタンスで割り当てられたスループット容量を編集する

1. **NetScaler Licensing > Flexed Licensing > Dashboard**に移動します。
2. **Licensed NetScalers**セクションで、インスタンスを選択し、**Edit Throughput Capacity**をクリックします。
3. **Edit Throughput Capacity**ページで、**Allocate**列に数値を入力します。
4. **Submit**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScalerインスタンスでライセンスを解放する

ライセンスを別のインスタンスに転送するには、現在のインスタンスでライセンスを解放し、新しいインスタンスにライセンスを適用する必要があります。**Release License**を選択すると、次の処理が行われます。

- そのインスタンスでチェックアウトされているすべてのライセンスをライセンスサーバーに解放します。
- そのインスタンス上のライセンスサーバー構成を削除します。

「**はい**」を選択すると、NetScalerインスタンスはライセンスなしの状態になり、トラフィックを処理できなくなります。

## Flexedライセンスレポート

**重要:**

ファイルベースのライセンスシステム (手動で管理されるエンタイトルメントとも呼ばれます) は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了 (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASはNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  **注:** ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしてい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンスは、LASではサポートされません。アクティブなメンテナンスのないperpetualライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
このダッシュボードでは、次の詳細を表示できます。

- ソフトウェアインスタンス (VPX、MPX、SDX、およびVPX FIP) のエンタイトルメントと割り当て
- 帯域幅/スループット容量のエンタイトルメント、割り当て、および実際の使用状況
- 管理対象または選択されたすべてのインスタンスにおけるピークおよび平均割り当て
- 管理対象または選択されたすべてのインスタンスにおけるピークおよび平均使用量

| 機能 (NETSCALER インスタンスの場合) | 説明 |
| --- | --- |
| エンタイトルメント | ソフトウェアインスタンスタイプ (VPX、SDX、MPX) の合計インスタンスエンタイトルメント。 |
| 割り当て | ソフトウェアインスタンスタイプ (VPX、SDX、MPX) の合計インスタンス割り当て。 |

| 機能 (帯域幅/スループット容量の場合) | 説明 |
| --- | --- |
| エンタイトルメント | 管理対象のすべてのNetScalerインスタンスにおける帯域幅/スループット容量の合計エンタイトルメント。合計エンタイトルメントは、ライセンス管理 (**NetScaler Licensing > License Management**) で適用されたライセンスから計算されます。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 機能 (帯域幅/スループット容量の場合) | 説明 |
| --- | --- |
| 割り当て | フレックスライセンスダッシュボード ( **NetScalerライセンス > フレックスライセンス > ダッシュボード** ) で、**ライセンスされた NetScaler** に割り当てられる帯域幅/スループット容量。 |
| 使用量 | NetScalerインスタンスによって消費された総スループット。 |

**注:**

フレックスライセンスはプレミアムエディションのみをサポートします。ただし、フレックスライセンスを購入して適用し、以前に標準またはアドバンストの帯域幅容量をプールしていた場合、帯域幅/スループット容量（標準またはアドバンスト）に関連する詳細も表示されます。たとえば、1000 Gbpsのフレックスライセンス（プレミアム）を適用しており、100 Gbpsのアドバンスト帯域幅の有効なプールライセンスも持っている場合、レポートダッシュボードにはプレミアム1000 Gbpsと100アドバンスト帯域幅の両方が表示されます。

次の例は、ダッシュボードがピーク使用量と平均使用量をどのように表示するかを理解するのに役立ちます。

3つの管理対象NetScalerインスタンス（NetScaler A、NetScaler B、NetScaler C）がフレックスライセンス（プレミアム帯域幅）を使用しており、選択された期間が1日であるとします。計算のために、NetScaler ConsoleはNetScalerインスタンスごとに1時間あたりのデータポイント（Mbps単位）を考慮します。1日あたり、各NetScalerインスタンスには24のデータポイントがあります。したがって、3つのNetScalerインスタンスの場合、(24 * 3)のデータポイントがあります。

- **ピーク使用量** = すべてのNetScalerインスタンスの24時間における最高のデータポイント（Mbps）の合計。たとえば、NetScaler Aの24時間期間における最高のデータポイントが30 Mbps、NetScaler Bが45 Mbps、NetScaler Cが120 Mbpsの場合、ピーク使用量は195 Mbps（30 + 45 + 120）と表示されます。
- **平均使用量** = 各NetScalerインスタンスの24時間すべてのデータポイントの合計を24で割った値。したがって、3つのNetScalerインスタンスの場合、3つのNetScalerインスタンスすべての合計平均を3で割ります。たとえば、NetScaler Aの平均が25 Mbps、NetScaler Bの平均が20 Mbps、NetScaler Cの平均が45 Mbpsの場合、平均使用量は30 Mbps（25 + 20 + 45 を3で割った値）と表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

同様に、ピークおよび平均割り当ての詳細も同じロジックを使用して表示されます。

リストから期間（1時間から1年まで）を選択し、表形式ビューとグラフィカルビューの両方で詳細を表示できます。

次の例は、フレックスライセンス（プレミアム帯域幅）を使用しているインスタンスの表形式ビューを示しています。

フレックスライセンスインスタンスレポート(/en-us/netscaler-application-delivery-management-software/media/flexed-license-instance-reporting.png)

ダッシュボードには次の詳細が表示されます。

- **ピーク使用量** - 選択した期間における最高の使用量（Mbps単位）。
- **平均使用量** - 選択した期間における平均使用量（Mbps単位）。
- **ピーク割り当て** - 選択した期間における最高の割り当て。
- **平均割り当て** - 選択した期間の平均割り当てです。
- **フィルター** - 1つ以上のインスタンスを選択して、特定のインスタンスの使用状況と割り当ての詳細を表示できます。
- **エクスポート** - 詳細をPDF、JPEG、PNG形式でエクスポートできます。

次の例は、Flexedライセンス（プレミアム帯域幅）を使用しているインスタンスのグラフィカルビューを示しています。

## フレックス型ライセンスへの移行

**重要:**

ファイルベースのライセンスシステム (手動で管理されるエンタイトルメントとも呼ばれます) は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了 (EOL) となります。ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS互換の最小要件となるNetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  **注:** ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降で提供されます。ただし、ファイルベースのライセンスは、April 15 2026をもって、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの従来のNetScalerライセンスの他のすべての形式は、LASではサポートされません。アクティブなメンテナンスのないPerpetualライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている場合、お客様は利用できない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
先に進む前に、以下の注記をお読みください。

## LASベースのライセンス

**注:**

NetScaler (ADCおよびSDX) インスタンスがLAS互換バージョンであることを確認してください。

以下のライセンスの移行に関する情報は、License Activation Service の「**既存のライセンスインスタンスの移行**」セクションを参照してください。

- Flexedライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス) へ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プールライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス) へ

以下のライセンスの移行に関する情報は、License Activation Service の「**LASへの移行**」セクションを参照してください。

- プールvCPUライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス) へ
- 固定サブスクリプションまたは永続ライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス) へ
- 固定vCPUライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス) へ
- CICOライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス) へ

## 手動で管理されるエンタイトルメント (ファイルベースライセンス)

**注:**

現在のライセンスの有効期限が切れる前に、Flexedライセンスに切り替える必要があります。移行を計画する際は、以下の手順を念頭に置き、手順にライセンスの再構成またはNetScaler®の再起動が含まれる場合は、メンテナンス期間を計画してください。

### プール帯域幅ライセンスからFlexedライセンスへ

一部の手順はMPX、SDX、VPXに共通です。これらの手順を最初に示し、次にMPX、SDX、またはVPXに固有の手順を示します。

#### VPX/MPX/SDXの共通手順

1. NetScaler Console に Flexed ソフトウェアライセンスをアップロードして適用します。「ライセンスファイル」(/ja-jp/netscaler-application-delivery-management-software/current-release/license-server/license-management.html#license-files)を参照してください。
2. 特定の期間の Z-Cap ソフトウェアライセンスをお持ちの場合は、そのライセンスを NetScaler ハードウェア (MPX/SDX) に適用してください。

#### VPX/MPXの場合

以下の追加手順が必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. プールされたプレミアム (プラチナ) 帯域幅ライセンスをお持ちの場合、古いライセンスの有効期限が切れると、ライセンスは自動的に Flexed に切り替わります。
2. プールされたStandardまたはプールされたAdvanced帯域幅ライセンスをお持ちの場合は、手動でプレミアム帯域幅をチェックアウトし、NetScalerをウォームリブートしてください。

#### SDXの場合

**注:**

現在のライセンスの有効期限が切れる前に、Flexed ライセンスに切り替えてください。

以下の追加手順が必要です。

1. 必要なインスタンスと帯域幅ライセンスをFlexedライセンスからSDXにチェックアウトします。SDXの再起動は不要です。
2. SDX上のすべてのVPXがプレミアムエディションである場合、古いライセンスの有効期限が切れると、ライセンスは自動的にFlexedに切り替わります。
3. StandardまたはAdvancedのすべてのVPX (SDX上) のエディションをPremiumに変更します。これらのVPXインスタンスは自動的に再起動されます。
4. SDX上のStandardおよびAdvanced帯域幅容量をゼロに減らします。

### プールされたvCPUからFlexed帯域幅容量へ

#### VPXの場合

1. NetScaler ConsoleにFlexedソフトウェアライセンスをアップロードして適用します。「ライセンスファイル」を参照してください(/ja-jp/netscaler-application-delivery-management-software/current-release/license-server/license-management.html#license-files)。
2. NetScaler GUIを使用して既存のライセンスサーバーを削除します。すべての手順が完了するまで、NetScalerはライセンスなしの状態になります。
3. Flexed/Pooledオプションでライセンスサーバーを追加します。
4. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
5. NetScalerをウォームリブートします。

#### CPXの場合

1. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。「ライセンスファイル」を参照してください(/ja-jp/netscaler-application-delivery-management-software/current-release/license-server/license-management.html#license-files)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. CPX YAMLまたはHELMマニフェストファイルを帯域幅要件で更新します。「CPX帯域幅ベースのライセンス」を参照してください(/ja-jp/cpx/current-release/cpx-licensing#provision-bandwidth-based-and-vcpu-based-licensing-from-netscaler-adm-service-for-netscaler-cpx)。
3. `kubectl apply -f cpx.yaml` コマンドまたはHELMチャートを使用してCPXインスタンスを展開します。

### 固定サブスクリプションまたは永続ライセンスからFlexedライセンスへ

いくつかの手順はMPX、SDX、VPXに共通です。これらの手順が最初にリストされ、次にMPX、SDX、またはVPXに固有の手順が続きます。

#### VPX/MPX/SDXの共通手順

1. NetScaler Consoleにオンボードします。
2. NetScaler ConsoleにFlexedソフトウェアライセンスをアップロードして適用します。「ライセンスファイル」を参照してください(/ja-jp/netscaler-application-delivery-management-software/current-release/license-server/license-management.html#license-files)。
3. NetScalerハードウェア (MPX/SDX) にZ-Capソフトウェアライセンスを適用します。

#### VPX/MPXの場合

以下の追加手順が必要です。

1. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
2. NetScalerをウォームリブートします。
3. NetScalerの再起動後、固定サブスクリプションライセンスを削除します。

#### SDXの場合

以下の追加手順が必要です。

1. SDX上のFlexedライセンスから、必要なインスタンスおよび帯域幅ライセンスをチェックアウトします。
2. SDX上のすべてのVPXがプレミアムエディションである場合、SDXの再起動は不要です。
3. いずれかのVPXがAdvancedまたはStandardエディションである場合、そのVPXをプレミアムエディションに移行する必要があります。VPXは自動的に再起動します。
4. NetScaler SDXにZ-Capソフトウェアライセンスを適用します。
5. SDX上のFlexedライセンスから、必要なインスタンスおよび帯域幅ライセンスをチェックアウトします。
6. NetScalerの再起動後、固定サブスクリプションライセンスを削除します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CICOからFlexed帯域幅容量へ

#### VPXの場合

1. NetScaler ConsoleにFlexedソフトウェアライセンスをアップロードして適用します。「ライセンスファイル」(/ja-jp/netscaler-application-delivery-management-software/current-release/license-server/license-management.html#license-files)を参照してください。
2. NetScaler GUIを使用して既存のライセンスサーバーを削除します。すべての手順が完了するまで、NetScalerはライセンスなしの状態になります。
3. Flexed/Pooledオプションでライセンスサーバーを追加します。
4. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
5. NetScalerをウォームリブートします。

## FlexedまたはPooledライセンスの有効期限切れと接続性の問題の動作シナリオ

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console オンプレミス の LAS サポートは、リリース 14.1-51.x 以降です。ただし、ファイルベースのライセンスは、Console オンプレミス リリース 14.1-51.x 以降および 13.1-60.x 以

© 1997–2026 Citrix Systems, Inc. All rights reserved.

降では April 15 2026をもって非推奨となります。Console オンプレミス リリース 14.1-51.x またはリリース 13.1-60.x 以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console オンプレミス 13.1 は LAS をサポートしていないため、15th April 2026までに Console オンプレミス リリース 14.1-51.x 以降にアップグレードし、LAS に切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrixメンテナンスを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

## LASベースのライセンス

### 期間満了前

- ライセンスは、期間満了前に更新する必要があります。
- NetScaler Console on-prem (クラウド接続) の場合、ライセンス契約が24時間以内に更新されていれば、ライセンスエンタイトルメントは自動的に更新されます。
- 期間満了前にライセンスが更新された場合、デバイスが稼働している限り、NetScaler は古いライセンスの有効期限が切れた後、新しいライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScaler は手動でのキャパシティ再構成を必要としません。

### 期間満了後

ライセンスが期間満了前に更新されない場合、NetScaler インスタンスは通常の動作を停止します。

- 設定が失われます。
- すべてのトラフィック処理が完全に停止します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 接続の問題の動作シナリオ

NetScaler インスタンスが Console on-prem から **License with LAS** または **Migrate to LAS** プロセスの一部として受け取るライセンスアクティベーションブロブは、30日間有効です。

NetScaler が Console on-prem との接続を失い、その後再接続した場合、遅延なくすぐにライセンスアクティベーションブロブを受け取ります。

NetScaler が Console on-prem に24時間以内に再接続できない場合、猶予期間に入ります。

デフォルトでは、ライセンスアクティベーションブロブは8時間ごとに更新されます。24時間以内に更新試行が3回連続で失敗した場合、NetScaler は猶予期間に入ります。

**猶予期間:**

- NetScaler は30日間の猶予期間に入ります。
- すべてのライセンス機能は引き続き動作します。ただし、31日目には次のようになります。
  - NetScaler VPX、NetScaler CPX、NetScaler BLX、およびNetScaler MPXインスタンスは強制的に再起動され、ライセンスが失効します。
  - NetScaler SDX上のすべてのVPXインスタンスのスループットは1 Mbpsに削減されます。

### ライセンス猶予期間アラート

Flexedダッシュボードには、インスタンスが猶予期間中であり、ライセンスアクティベーションブロブの有効期限が切れるまでの残り日数を示す警告アイコンが表示されます。管理者がNetScalerインスタンスのGUIにログインするたびに、インスタンスが猶予期間中であり、ライセンスアクティベーションブロブの有効期限が切れるまでの残り日数を示すポップアップメッセージが表示されます。

## 手動で管理されるライセンス（ファイルベースのライセンス）

このドキュメントでは、NetScaler MPX、NetScaler SDX、およびNetScaler VPX/NetScaler BLX/NetScaler CPXにおけるライセンスの有効期限切れと接続性の問題のさまざまなシナリオについて説明します。

### Flexedライセンスの種類

- ソフトウェアインスタンス（VPX/BLX/CPX、SDX、MPX、VPX FIPS）
- 帯域幅容量

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## シナリオ：MPXフォームファクター

Flexed/Pooledライセンスを使用しており、ライセンスの有効期限が間もなく切れます。以下のシナリオでは、有効期限の前後でNetScaler Consoleに新しいライセンスがアップロードされた場合、またはライセンスファイルが存在しない場合の動作について説明します。

### 有効期限が切れる前

新しいライセンスが有効期限前にアップロードされ、古いライセンスがまだ有効な場合、2つの異なる容量プール（旧と新）が利用可能です。

- NetScalerが稼働中の場合、古いライセンスの有効期限が切れた後、新しいFlexed/Pooledライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScalerでは、手動でのキャパシティ再構成は不要です。

### 期間の満了後

NetScalerインスタンスは、ライセンスの有効期限が切れると、設定の損失やトラフィック処理の完全なシャットダウンを含め、通常の動作を停止します。

## シナリオ：SDXフォームファクター

Flexed/Pooledライセンスを使用しており、ライセンスの有効期限が間もなく切れます。以下のシナリオでは、期間の満了前と満了後に新しいライセンスがNetScaler Consoleにアップロードされた場合、またはライセンスファイルが存在しない場合の動作について説明します。

### 期間の満了前

新しいライセンスが期間の満了前にアップロードされ、古いライセンスがまだ有効な場合、2つの異なるキャパシティプール（古いものと新しいもの）が利用可能です。

- NetScalerが稼働中の場合、古いライセンスの有効期限が切れた後、新しいFlexed/Pooledライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScalerでは、手動でのキャパシティ再構成は不要です。

### 期間の満了後

NetScalerインスタンスは、ライセンスの有効期限が切れると、設定の損失やトラフィック処理の完全なシャットダウンを含め、通常の動作を停止します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## シナリオ：VPX/BLX/CPXフォームファクター

Flexed/Pooledライセンスを使用しており、ライセンスの有効期限が間もなく切れます。以下のシナリオでは、期間の満了前と満了後に新しいライセンスがNetScaler Consoleにアップロードされた場合、またはライセンスファイルが存在しない場合の動作について説明します。

### 期間満了前

新しいライセンスが期間満了前にアップロードされ、古いライセンスがまだ有効な場合、2つの異なる容量プール（旧と新）が利用可能です。

- NetScalerが稼働中の場合、古いライセンスの有効期限が切れた後、新しいFlexed/Pooledライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScalerは手動での容量再構成を必要としません。

### 期間満了後

ライセンスの有効期限が切れると、NetScalerインスタンスは通常の動作を停止し、設定の損失やトラフィック処理の完全なシャットダウンが発生します。

## 接続の問題の動作シナリオ

NetScalerとNetScaler Consoleオンプレミスサーバー間の接続が切断された場合、動作は次のとおりです。

- NetScalerは30日間猶予期間に入ります。
- この猶予期間中、ライセンス機能は30日目まで引き続き動作します。
- 31日目には、,
    - NetScaler VPX/NetScaler CPX/NetScaler BLXおよびNetScaler MPXは強制的に再起動され、ライセンスなしの状態になります。
    - NetScaler SDX上のすべてのVPXのスループットは1 Mbpsに減少します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとして構成する

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降にNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
管理者は、NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成できます。この構成では、NetScaler ConsoleサーバーはNetScalerインスタンスからライセンスデータのみを受信します。

規制区域からNetScalerインスタンスのデータが流出することを制限する規制上の義務がある場合があります。このような状況では、管理、監視、分析機能を使用するために、規制区域にNetScaler Console on-premサーバーのローカルインスタンスを展開できます。FlexedまたはPooledライセンス機能を使用するために同じアプローチに従う場合、さまざまなNetScaler Consoleライセンスサーバー間でFlexedまたはPooledライセンスを分割する必要があります。このアプローチでは、グローバルに展開されたNetScalerインスタンス全体にFlexedまたはPooledライセンスを柔軟に割り当てることはできません。

したがって、NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成してください。NetScaler Consoleサーバーは、すべてのNetScalerインスタンスからライセンスデータのみを受信します。これにより、規制上の義務を遵守し、グローバルに展開されたNetScalerインスタンス全体にFlexedまたはPooled容量ライセンスを動的に割り当てることができます。

## NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成する方法

開始する前に、NetScaler ConsoleサーバーにNetScalerインスタンスが追加されていないことを確認してください。ステップ4を完了した後にのみ、NetScalerインスタンスを追加してください。

NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成するには、次の手順を実行します。

1. **Settings > Administration** に移動します。
2. **System Configurations** セクションで、**System Deployment** を選択します。
3. **ADM Deployment** で、**NetScaler Console only as a flexed/pooled licensing server** を選択します。

   
4. **OK** をクリックします。

   この操作により、FlexedまたはPooledライセンス機能のみが保持され、以下のNetScaler Console機能が無効になります。

   - NetScaler Consoleのバックアップ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- イベント管理
- SSL証明書管理
- ネットワークレポート
- ネットワーク機能
- 構成監査

**注**

デフォルトでは、NetScaler Consoleの分析機能は無効になっています。この機能を有効にしている場合は、必ず無効にしてください。

確認ボックスで、**はい**をクリックします。

NetScaler Console GUIには、FlexedまたはPooledライセンス機能のみが表示されます。そして、残りの機能は表示されません。

5. ライセンス機能のみにNetScaler Consoleを設定した後、**Infrastructure > Instances**ページでNetScalerインスタンスを追加します。

**注**

- 1つ以上のNetScaler ConsoleサーバーにNetScalerインスタンスを追加できます。そのようなNetScalerインスタンスのパスワードを変更する場合は、インスタンスが検出されたすべてのNetScaler Consoleサーバーでパスワードを更新してください。
- ユーザーは、NetScaler Console GUIで無効になっている機能の一部操作をまだ実行できます。たとえば、イベントポーリングやNetScalerのバックアップなどです。スーパー管理者として、そのような操作を制限したい場合は、適切なアクセスポリシーを使用して他の管理者に対するユーザーアクセスを無効にしてください。詳細については、「NetScaler Consoleでアクセスポリシーを構成する」を参照してください。

NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバー専用として、以下の低い仕様で展開することもできます。

| コンポーネント | 要件 |
| --- | --- |
| RAM | 8 GB |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| コンポーネント | 要件 |
| --- | --- |
| 仮想CPU | 4 |
| ストレージ | 120 GB |

# レガシーライセンス

レガシーライセンスは、NetScalerインスタンス向けの以前のプールされたキャパシティ、チェックインおよびチェックアウト、仮想CPUライセンスモデルを対象としています。以下のトピックは、レガシーライセンスの管理に役立ちます。

- NetScalerプールライセンス
- NetScalerプールされたキャパシティの構成
- NetScaler VPXの永続ライセンスをNetScalerプールされたキャパシティにアップグレード
- NetScaler MPXの永続ライセンスをNetScalerプールされたキャパシティにアップグレード
- NetScaler SDXの永続ライセンスをNetScalerプールされたキャパシティにアップグレード
- クラスターモードのNetScalerインスタンスにおけるNetScalerプールされたキャパシティ
- NetScaler VPXのチェックインおよびチェックアウトライセンス
- NetScaler仮想CPUライセンス
- 問題発生時の予期される動作

## NetScaler プール型キャパシティ

**重要:**

ファイルベースのライセンスシステム (手動で管理されるエンタイトルメントとも呼ばれます) は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了 (EOL) となります。ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScalerプール型ライセンス、およびNetScaler固定期間帯域幅ライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS互換の最小要件NetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  **注:** Consoleオンプレミス向けのLASサポートは、リリース14.1-51.x以降で提供されます。ただし、ファイルベースのライセンスは、April 15 2026をもって、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他の従来のNetScalerライセンスはすべてLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScalerプール型キャパシティを使用すると、異なるNetScalerフォームファクター間で帯域幅またはインスタンスライセンスを共有できます。仮想CPUサブスクリプションベースのインスタンスの場合、インスタンス間で仮想CPUライセンスを共有できます。このプール型キャパシティは、データセンターまたはパブリッククラウドにあるインスタンスに使用します。インスタンスがリソースを必要としなくなると、割り当てられたキャパシティを共通プールに返却します。解放されたキャパシティは、リソースを必要とする他のNetScalerインスタンスに再利用できます。

プール型ライセンスを使用すると、インスタンスに必要な帯域幅を割り当て、必要以上の割り当てを行わないことで、帯域幅の使用率を最大化できます。トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられた帯域幅を増減できます。プール型キャパシティライセンスを使用すると、インスタンスのプロビジョニングを自動化できます。

### NetScalerプール型キャパシティライセンスの仕組み

NetScaler プール型キャパシティには、次のコンポーネントがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler インスタンスは、次のカテゴリに分類できます。
  - ゼロキャパシティハードウェア
  - スタンドアロンのNetScaler VPXインスタンス、NetScaler CPXインスタンス、または NetScaler BLXインスタンス
- 帯域幅プール
- インスタンスプール
- ライセンスサーバーとして構成されたNetScaler Console

### ゼロキャパシティハードウェア

NetScaler プール型キャパシティを介して管理される場合、MPXおよびSDXインスタンスは「ゼロキャパシティハードウェア」と呼ばれます。これは、これらのインスタンスが帯域幅プールとインスタンスプールからリソースをチェックアウトするまで機能できないためです。したがって、これらのプラットフォームはMPX-ZおよびSDX-Zアプライアンスとも呼ばれます。

ゼロキャパシティハードウェアは、共通プールから帯域幅とインスタンスライセンスをチェックアウトできるようにするために、プラットフォームライセンスを必要とします。

**注**

- MPXインスタンスにはインスタンスライセンスのサブスクリプションは必要ありません。MPXおよびSDXインスタンスでサポートされているプール型キャパシティについては、このページの表1を参照してください。さまざまなMPXおよびSDXフォームファクターのライセンス要件については、表5を参照してください。
- ゼロキャパシティライセンスのインストールは、他のNetScalerローカルライセンスと同じように機能します。ゼロキャパシティライセンスの取得とインストール方法の詳細については、NetScalerのライセンスガイドを参照してください。

### プラットフォームライセンスの管理とインストール

プラットフォームライセンスは、ハードウェアのシリアル番号またはライセンスアクセスコードを使用して手動でインストールする必要があります。プラットフォームライセンスがインストールされると、ハードウェアにロックされ、オンデマンドでNetScalerハードウェアインスタンス間で共有することはできません。ただし、プラットフォームライセンスを別のNetScalerハードウェアインスタンスに手動で移動することはできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerソフトウェアリリース11.1ビルド54.14以降を実行しているNetScaler MPXインスタンスと、11.1ビルド58.13以降を実行しているNetScaler SDXインスタンスは、NetScaler Pooled capacityをサポートします。詳細については、「**表1. MPXおよびSDXインスタンスでサポートされるPooled capacity**」を参照してください。

### スタンドアロンNetScaler VPXインスタンス

NetScalerソフトウェアリリース11.1ビルド54.14以降を実行しているNetScaler VPXインスタンスは、次のハイパーバイザーでPooled capacityをサポートします。

- ヴイエムウェア ESX 6.0
- シトリックス ハイパーバイザー™
- リナックス KVM

NetScalerソフトウェアリリース12.0ビルド51.24以降を実行しているNetScaler VPXインスタンスは、次のハイパーバイザーおよびクラウドプラットフォームでPooled capacityをサポートします。

- マイクロソフト Hyper-V
- AWS
- マイクロソフト Azure
- グーグル クラウド

NetScalerソフトウェアリリース13.0および13.1（すべてのバージョン）を実行しているNetScaler VPXインスタンスは、次のハイパーバイザーおよびクラウドプラットフォームでPooled capacityをサポートします。

- ヴイエムウェア ESX 6.0
- シトリックス ハイパーバイザー
- リナックス KVM
- マイクロソフト Hyper-V
- AWS
- マイクロソフト Azure
- グーグル クラウド

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

NetScaler Console と Microsoft Azure または AWS 間の通信を有効にするには、IPSEC トンネルを構成する必要があります。詳細については、「クラウドに展開された NetScaler VPX インスタンスを NetScaler Console に追加する」を参照してください。 ゼロキャパシティハードウェアとは異なり、NetScaler VPX にはプラットフォームライセンスは必要ありません。トラフィックを処理するには、プールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

### スタンドアロン NetScaler CPX インスタンス

Docker ホストに展開された NetScaler CPX インスタンスは、プールされたキャパシティをサポートします。ゼロキャパシティハードウェアとは異なり、NetScaler CPX にはプラットフォームライセンスは必要ありません。最大 1 Gbps のスループットを消費する単一の NetScaler CPX インスタンスは、ライセンスプールから 1 インスタンスのみをチェックアウトし、帯域幅はチェックアウトしません。たとえば、20 Gbps の帯域幅プールを持つ 20 個の NetScaler CPX インスタンスがあるとします。いずれかの NetScaler CPX インスタンスが 500 Mbps のスループットを消費しても、帯域幅プールは残りの 19 個の NetScaler CPX インスタンスに対して 20 Gbps のままです。

同じ NetScaler CPX インスタンスが 1500 Mbps のスループットを消費し始めた場合、帯域幅プールは残りの 19 個の NetScaler CPX インスタンスに対して 19.5 Gbps になります。

プールライセンスの場合、帯域幅は 10 Mbps の倍数でのみ追加できます。

### スタンドアロン NetScaler BLX インスタンス

NetScaler BLX インスタンスは、プールされたキャパシティライセンスをサポートします。NetScaler BLX インスタンスにはプラットフォームライセンスは必要ありません。トラフィックを処理するには、NetScaler BLX インスタンスはプールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

### 帯域幅プール

帯域幅プールは、物理および仮想の両方の NetScaler インスタンスで共有できる合計帯域幅です。帯域幅プールは、各ソフトウェアエディション (Standard、Advanced、Premium) ごとに個別のプールで構成されます。特定の NetScaler インスタンスは、異なるプールから帯域幅を同時にチェックアウトすることはできません。帯域幅をチェックアウトできる帯域幅プールは、ライセンスされているソフトウェアエディションによって異なります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### インスタンスプール

インスタンスプールは、NetScaler Pooled capacity を介して管理できる NetScaler VPX インスタンス、NetScaler CPX インスタンス、または NetScaler BLX インスタンスの数、あるいは SDX-Z インスタンス内の NetScaler VPX インスタンスの数を定義します。

プールからチェックアウトされると、ライセンスは MPX-Z、SDX-Z、VPX、NetScaler CPX、および NetScaler BLX インスタンスのリソース（CPU/PE、SSLコア、1秒あたりのパケット数、帯域幅など）をアンロックします。

**注**

SDX-Z の管理サービスはインスタンスを消費しません。

### NetScaler Console ライセンスサーバー

NetScaler Pooled capacity は、ライセンスサーバーとして構成された NetScaler Console を使用して、帯域幅プールライセンスとインスタンスプールライセンスという Pooled capacity ライセンスを管理します。NetScaler Console ライセンスがなくても、NetScaler Console ソフトウェアを使用して Pooled capacity ライセンスを管理できます。

帯域幅プールとインスタンスプールからライセンスをチェックアウトする際、ゼロキャパシティハードウェア上の NetScaler フォームファクターとハードウェアモデル番号によって、以下が決定されます。

- NetScaler インスタンスが機能する前にチェックアウトする必要がある最小帯域幅とインスタンス数。
- NetScaler がチェックアウトできる最大帯域幅とインスタンス数。
- 各帯域幅チェックアウトの最小帯域幅単位。最小帯域幅単位は、NetScaler がプールからチェックアウトする必要がある帯域幅の最小単位です。すべてのチェックアウトは、最小帯域幅単位の整数倍である必要があります。たとえば、NetScaler の最小帯域幅単位が 1 Gbps の場合、1000 Mbps はチェックアウトできますが、200 Mbps や 150.5 Gbps はチェックアウトできません。最小帯域幅単位は、最小帯域幅要件とは異なります。NetScaler インスタンスは、少なくとも最小帯域幅でライセンスが付与された後にのみ動作できます。最小帯域幅が満たされると、インスタンスは最小帯域幅単位でさらに帯域幅をチェックアウトできます。

表 1、2、3、および 4 は、サポートされているすべての NetScaler インスタンスの最大帯域幅/インスタンス数、最小帯域幅/インスタンス数、および最小帯域幅単位をまとめたものです。表 5 は、サポートされているすべての NetScaler インスタンスのさまざまなフォームファクターのライセンス要件をまとめたものです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**表 1. MPX および SDX インスタンスでサポートされる Pooled capacity**

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **MPX 5900Z** | 10 | 1 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 8900Z** | 30 | 5 | NA | NA | 1 ギガビット/秒 |
| **MPX 9100Z** | 30 | 10 | NA | NA | 1 ギガビーピーエス |
| **MPX 8900Z FIPS** | 33 | 5 | NA | NA | 1 ギガビーピーエス |
| **MPX 14000Z シリーズ** | 100 | 20 | NA | NA | 1 ギガビット/秒 |
| **MPX 14000Z 40G シリーズ** | 100 | 20 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 14000Z FIPS シリーズ** | 100 | 20 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 14000Z 40S シリーズ** | 100 | 20 | 該当なし | 該当なし | 1 ギガビット/秒 |
| **MPX 15000Z シリーズ** | 120 | 20 | 該当なし | 該当なし | 1 ギガビット/秒 |
| **MPX 15000Z FIPS シリーズ** | 120 | 20 | N/A | N/A | 1 ギガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **MPX 15000Z 50G シリーズ** | 120 | 20 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 16000Z シリーズ** | 200 | 30 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 22000Z シリーズ** | 120 | 40 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 24000Z シリーズ** | 150 | 100 | N/A | N/A | 1 ギガビット/秒 |
| **MPX 25000Z 40G** | 200 | 100 | N/A | N/A | 1 ギガビーピーエス |
| **MPX 25000ZA** | 200 | 100 | N/A | N/A | 1 ギガビーピーエス |
| **MPX 26000Z シリーズ** | 200 | 100 | N/A | N/A | 1 ギガビーピーエス |
| **MPX 26000Z 100G シリーズ** | 200 | 100 | N/A | N/A | 1ギガビット/秒 |
| **MPX 26000Z 50S シリーズ** | 200 | 100 | N/A | N/A | 1ギガビット/秒 |
| **SDX 8900Z** | 30 | 10 | 1 | 7 | 1 ギガbps |
| **SDX 9100Z** | 95 | 20 | 1 | 7 | 1 ギガbps |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 14000Z シリーズ** | 100 | 10 | 1 | 25 | 1 ギガbps |
| **SDX 14000Z 40G シリーズ** | 100 | 1 | 2 | 25 | 1 ギガビーピーエス |
| **SDX 14000Z 40S シリーズ** | 100 | 20 | 1 | 25 | 1 ギガビーピーエス |
| **SDX 14000Z FIPS シリーズ** | 100 | 10 | 1 | 25 | 1 ギガビーピーエス |
| **SDX 15000Z 50G** | 120 | 10 | 1 | 55 | 1 ギガビーピーエス |
| **SDX 15000Z** | 120 | 10 | 1 | 55 | 1 ギガビーピーエス |
| **SDX 16000Z シリーズ** | 200 | 15 | 1 | 55 | 1 ギガビーピーエス |
| **SDX 22000Z シリーズ** | 120 | 20 | 1 | 80 | 1 ギガビーピーエス |
| **SDX 25000Z 40G** | 200 | 50 | 1 | 115 | 1 ギガビット/秒 |
| **SDX 25000ZA** | 200 | 50 | 1 | 115 | 1 ギガビット/秒 |
| **SDX 26000Z 100G** | 200 | 50 | 1 | 115 | 1 ギガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (GBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **SDX 26000Z** | 200 | 50 | 1 | 115 | 1ギガbps |
| **SDX 26000Z 50S** | 200 | 50 | 1 | 115 | 1ギガbps |
| **SDX 24000Z シリーズ** | 150 | 50 | 1 | 80 | 1 ギガビット/秒 |

注

最小帯域幅とインスタンスは、以下のリリース以降を実行しているSDXインスタンスに適用されます: 11.1 64.x、12.0 63.x、12.1 54.x、および13.0 41.x。

最小購入数量は、最小システム要件とは異なります。

**表2. NetScaler CPXインスタンスでサポートされるプール容量**

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **CPX** | 10 | 10 | 1 | 1 | 10メガビット/秒 |

**表3. ハイパーバイザーおよびクラウドサービス上のNetScaler VPXインスタンスでサポートされているプール容量**

| ハイパーバイザー/クラウドサービス | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **シトリックス ハイパーバイザー** | 40 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **ヴイエムウェア ESXI** | 100 ギガbps | 10 メガbps | 1 | 1 | 10 メガビット/秒 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ハイパーバイザー/クラウドサービス | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **リナックス KVM** | 100 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **マイクロソフト Hyper-V** | 3 ギガビーピーエス | 10 メガビーピーエス | 1 | 1 | 10 メガビット/秒 |
| **AWS** | 30 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **アジュール** | 10 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |
| **グーグル クラウド** | 10 ギガビット/秒 | 10 メガビット/秒 | 1 | 1 | 10 メガビット/秒 |

注

最小購入数量は、最小システム要件とは異なります。

**表4. NetScaler BLXインスタンスでサポートされるプール容量**

| 製品ライン | 最大帯域幅 (GBPS) | 最小帯域幅 (MBPS) | 最小インスタンス数 | 最大インスタンス数 | 最小帯域幅単位 |
|---|---|---|---|---|---|
| **BLX** | 100 | 10 | 1 | 1 | 10 メガビット/秒 |

**表5. 異なるフォームファクターのライセンス要件**

| 製品ライン | ゼロキャパシティハードウェア購入 | 帯域幅およびエディションサブスクリプション | インスタンスサブスクリプション |
|---|---|---|---|
| **MPX** | 必要なライセンス | ライセンスが必要 | - |
| **SDX** | ライセンスが必要 | ライセンスが必要 | ライセンスが必要 |
| **VPX** | - | ライセンスが必要 | ライセンスが必要 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 製品ライン | ゼロキャパシティハードウェア購入 | 帯域幅およびエディションサブスクリプション | インスタンスサブスクリプション |
|---|---|---|---|
| **CPX** | - | - | ライセンスが必要 |
| **BLX** | - | ライセンスが必要 | ライセンスが必要 |

## NetScaler プール型キャパシティを設定する

**重要:**

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム (手動で管理されるエンタイトルメントとも呼ばれます) は、April 15, 2026にサポート終了 (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体の製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASはNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexed licenses (CPL/UHMC)、従来のNetScaler Pooled licenses、およびNetScaler Fixed term Bandwidth licensesをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換の最小要件となるNetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを継続して使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのないPerpetualライセンスを利用している

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードすると、ライセンスが失効します。
法律または規制によって禁止されている場合、LASベースのライセンスは顧客に提供されないことがあります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScaler プール型キャパシティを使用するには、必要なNetScalerインスタンスのライセンスサーバーとしてNetScaler Consoleを設定します。NetScalerインスタンスは、NetScaler Consoleからライセンスをチェックインおよびチェックアウトします。NetScaler Console GUIで次のタスクを実行できます。

- プール型キャパシティライセンスファイル (帯域幅およびインスタンスプール) をライセンスサーバーにアップロードします。
- ライセンスプールからNetScalerインスタンスに必要に応じてライセンスを割り当てます。
- インスタンスの最小容量と最大容量に基づいて、NetScalerインスタンス (MPX-Z /SDX-Z/VPX/CPX/BLX) からライセンスをチェックアウトします。
- NetScaler FIPSインスタンスのプール容量を構成して、ライセンスをチェックインまたはチェックアウトします。

プールライセンス(/en-us/netscaler-application-delivery-management-software/media/pool-licenses-console.png)

### サポートされているハードウェアおよびソフトウェアのバージョン

プール容量でサポートされているハードウェアおよびソフトウェアのバージョンについては、NetScaler Pooled capacityを参照してください。

### NetScaler プール容量の状態

プール容量の状態は、NetScalerインスタンスのライセンス要件を示します。プール容量で構成されたNetScalerインスタンスは、次のいずれかの状態を表示します。

- **最適**: インスタンスは適切なライセンス容量で稼働しています。
- **容量の不一致**: インスタンスは、ユーザーが構成した容量よりも少ない容量で稼働しています。
- **猶予**: インスタンスは猶予ライセンスで稼働しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **猶予と不一致**: インスタンスは猶予期間中ですが、ユーザーが構成した容量よりも少ない容量で稼働しています。
- **利用不可**: インスタンスが管理のためにNetScaler Consoleに登録されていないか、NetScaler ConsoleからインスタンスへのNITRO通信が機能していません。
- **未割り当て**: インスタンスにライセンスが割り当てられていません。

### ステップ1 - NetScaler Consoleでライセンスを適用する

1. NetScaler Consoleで、**NetScaler Licensing > Pooled Licensing**に移動します。
2. 「**ライセンスファイル**」セクションで、「**ライセンスファイルの追加**」を選択し、次のいずれかのオプションを選択します。

   - **ローカルコンピューターからライセンスファイルをアップロードします。**ライセンスファイルがすでにローカルコンピューターに存在する場合は、NetScaler Consoleにアップロードできます。
   - **ライセンスアクセスコードを使用します。**Citrixから購入したライセンスのライセンスアクセスコードを指定します。次に、「**ライセンスの取得**」を選択します。その後、「**完了**」を選択します。

   **注**

   いつでも、「**ライセンス設定**」からNetScaler Consoleにライセンスを追加できます。

3. 「**完了**」をクリックします。

   ライセンスファイルがNetScaler Consoleに追加されます。「**ライセンス有効期限情報**」タブには、NetScaler Consoleに存在するライセンスと有効期限までの残り日数が表示されます。

4. 「**ライセンスファイル**」で、適用するライセンスファイルを選択し、「**ライセンスの適用**」をクリックします。

   このアクションにより、NetScalerインスタンスは選択したライセンスをプールされたキャパシティとして使用できるようになります。

### ステップ2 - NetScaler Consoleをライセンスサーバーとして登録する

NetScaler ConsoleをNetScalerインスタンスのライセンスサーバーとして登録するには、次のいずれかの手順に従います。

- GUIを使用する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CLIを使用する

### GUIを使用してNetScaler Consoleをライセンスサーバーとして登録する

NetScaler GUIで、NetScaler Consoleサーバーをライセンスサーバーとして登録します。

1. NetScaler GUIにログインします。
2. **System** > **Licenses** > **Manage Licenses** に移動します。
3. **Add New License** をクリックします。
4. **Use remote licensing** を選択し、**Remote Licensing Mode** でリストから **Pooled Licensing** を選択します。
5. **Server Name/IP address** フィールドに、NetScaler ConsoleサーバーのIPアドレスを指定します。

   HA展開の場合は、フローティングIPを使用します。構成の詳細については、Configure High Availability Deployment を参照してください。

   > スタンドアロンのNetScaler ConsoleまたはエージェントをNetScaler Consoleを使用する展開については、Licensing overview を参照してください。

6. デフォルトのライセンスポートは27000です。
7. NetScaler Consoleにインスタンスを登録するために、NetScaler Consoleサーバーの資格情報を入力し、**Continue** をクリックします。NetScaler Consoleでは、いずれかのサーバーがライセンスサーバーになります。

   **注記:**

   - NetScaler Consoleに有効なデジタル証明書が認証局 (CA) によって発行されている場合のみ (**Settings > Administration > SSL Settings** の下)、**Validate Certificate** チェックボックスを選択します。
   - NetScalerがNAT IP経由でのみ到達可能な場合、デバイス登録が失敗する可能性があります。ライセンスは引き続きチェックアウトできますが、NetScaler Consoleはそれらの NetScalerインスタンスを管理対象外インスタンスとして表示します。

8. **Device Profile Name** で、NetScaler Consoleがインスタンスにアクセスするために使用できるインスタンスプロファイルを指定します。このインスタンスプロファイルには、NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Consoleに追加するインスタンスのユーザー名とパスワードが含まれています。デフォルトのプロファイルは **ns_nsroot_profile** です。インスタンスのデフォルトの管理者資格情報を変更した場合は、カスタムインスタンスプロファイル名を定義できます。

9. **Allocate licenses** で、ライセンスエディションを選択し、必要な帯域幅を指定します。

   初めて、NetScalerでライセンスを割り当てます。後で、NetScaler Console GUIからライセンスの割り当てを変更または解放できます。

   a. をクリックします。

   **重要:**

   ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。インスタンスを再起動するまで、構成の変更は有効になりません。

### CLIを使用してNetScaler Consoleをライセンスサーバーとして追加する

NetScalerインスタンスにGUIがない場合は、以下のCLIコマンドを使用してNetScaler Consoleサーバーをライセンスサーバーとして追加します。

1. NetScalerコンソールにログインします。
2. NetScaler ConsoleサーバーのIPアドレスを追加します。

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
```

   詳細については、ライセンスの概要を参照してください。

3. ライセンスサーバーで利用可能なライセンス帯域幅を表示します。

```
> sh ns licenseserverpool
```

   このコマンドは、ライセンスサーバーの追加時に指定されたライセンスモードに基づいてライセンスを一覧表示します。

   **例-1：**

   指定されたライセンスモードが `CICO` の場合、出力にはCICOライセンスのみが含まれます。

   **例-2：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指定されたライセンスモードが `Pooled` の場合、出力にはプール容量ライセンスのみが含まれます。

**例-3**:

指定されたライセンスモードが `vCPU` の場合、出力には仮想CPUライセンスのみが含まれます。

すべてのライセンスをまとめて表示するには、次のコマンドを実行します。

```
> sh ns licenseserverpool -getallLicenses
```

**出力例**:

4. 必要なライセンスエディションからライセンス帯域幅を割り当てます。

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify-
amount-license-bandwidth> -edition <specify-license-edition>
```

ライセンスエディションは、**Standard**、**Enterprise**、または**Platinum**です。

**重要**

ライセンスエディションを変更した場合は、インスタンスをウォーム再起動します。

`reboot -w`

インスタンスを再起動するまで、構成の変更は有効になりません。

### ステップ3 - NetScalerインスタンスにプールライセンスを割り当てる

NetScaler Console GUIからプールされた容量ライセンスを割り当てるには:

1. NetScaler Consoleにログインします。
2. **インフラストラクチャ > ライセンス > 帯域幅ライセンス > プール容量** に移動します。

   FIPSインスタンス容量は、FIPSインスタンスライセンスをNetScaler Consoleにアップロードした場合にのみ表示されます。
3. 管理したいライセンスプールをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注**
>
> **Allocated Capacity** フィールドは、変更された帯域幅をすぐに反映しません。帯域幅の変更は、NetScalerのウォームリスタート後に有効になります。

**Allocation Details** では、インスタンスの帯域幅割り当てを変更すると、**Requested** および **Applied** フィールドが更新されます。

4. **>** ボタンをクリックして、利用可能なインスタンスのリストからNetScalerインスタンスを選択します。

   NetScaler Consoleのプールされたインスタンス(/en-us/netscaler-application-delivery-management-software/media/pooled-licenses-manage-licenses-3.png)

   **LICENSE STATUS** 列には、対応するライセンス割り当てステータスメッセージが表示されます。

   > **注:**
   >
   > **Unmanaged Instances** タブには、検出されたがNetScaler Consoleで管理されていないインスタンスが表示されます。

   管理されていないインスタンス(/en-us/netscaler-application-delivery-management-software/media/unmanaged-instances.png)

5. ライセンス割り当てを変更するには、**Change allocation** または **Release allocation** をクリックします。
6. ライセンスサーバーで利用可能なライセンスを含むポップアップウィンドウが表示されます。
7. **Allocate** リストオプションを設定することで、インスタンスへの帯域幅またはインスタンスの割り当てを選択できます。選択後、**Allocate** をクリックします。
8. **Change License Allocation window** のリストオプションから、割り当てられたライセンスエディションを変更することもできます。

   > **注**
   >
   > ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

帯域幅の割り当てを変更する方法の詳細については、関連ビデオを参照してください。

<iframe src="https://www.youtube.com/embed/AMaHr-ska8s" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

### NetScalerインスタンスでプールされたキャパシティを構成する

以下のNetScalerインスタンスでプールされたキャパシティライセンスを構成できます。

- NetScalerインスタンス
- NetScaler VPX™インスタンス
- NetScaler高可用性ペア

#### NetScaler MPX™インスタンス

MPX-Zは、プールされたキャパシティが有効なNetScaler MPXアプライアンスです。MPX-Zは、Premium、Advanced、またはStandardエディションライセンスの帯域幅プーリングをサポートします。

MPX-Zは、ライセンスサーバーに接続する前にプラットフォームライセンスを必要とします。MPX-Zプラットフォームライセンスは、以下のいずれかの方法でインストールできます。

- ローカルコンピューターからライセンスファイルをアップロードする。
- インスタンスのハードウェアシリアル番号を使用する。
- インスタンスのGUIの**System** > **Licenses**セクションにあるライセンスアクセスコード。

MPX-Zプラットフォームライセンスを削除すると、プール容量機能は無効になります。インスタンスライセンスはライセンスサーバーに解放されます。

再起動せずにMPX-Zインスタンスの帯域幅を動的に変更できます。再起動が必要なのは、ライセンスエディションを変更する場合のみです。

**注：**

インスタンスを再起動すると、構成された容量に必要なプールライセンスが自動的にチェックアウトされます。

#### NetScaler VPXインスタンス

プール容量が有効なNetScaler VPXインスタンスは、帯域幅プール（Premium/Advanced/Standardエディション）からライセンスをチェックアウトできます。NetScaler GUIを使用して、ライセンスサーバーからライセンスをチェックアウトできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

再起動せずにVPXインスタンスの帯域幅を動的に変更できます。再起動が必要なのは、ライセンスエディションを変更する場合のみです。

**注：**

インスタンスを再起動すると、構成されたプール容量ライセンスがNetScaler Consoleサーバーから自動的にチェックアウトされます。

### NetScaler高可用性ペア

開始する前に、NetScaler Consoleサーバーがライセンスサーバーとして構成されていることを確認してください。詳細については、「NetScaler Consoleをライセンスサーバーとして構成する」を参照してください。

高可用性モードで構成されたNetScalerインスタンスの場合、高可用性ペアの各ノードでプール容量を構成する必要があります。プライマリノードとセカンダリノードの両方で、同じ容量のライセンスを割り当てる必要があります。たとえば、HAペアの各インスタンスから1 Gbpsの容量が必要な場合、共通プールから2倍の容量（2 Gbps）が必要になります。その後、各ノードに1 Gbpsの容量を割り当てることができます。

ペアの各ノードにプールライセンスを割り当てるには、NetScalerインスタンスにプールライセンスを割り当てるに記載されている手順に従ってください。まず最初のノードにライセンスを割り当て、次に同じ手順を繰り返して2番目のノードにライセンスを割り当てます。

## NetScaler VPX の永続ライセンスを NetScaler Pooled capacity にアップグレードする

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-prem のLASサポートはリリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-prem リリース14.1-51.x以降および13.1-60.x以降から非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを継続して使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つ可能性のあるその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
永続ライセンスを持つNetScaler VPXインスタンスは、NetScaler Pooled capacityライセンスにアップグレードできます。Pooled capacityライセンスにアップグレードすると、ライセンスプールからVPXインスタンスにオンデマンドでライセンスを割り当てることができます。高可用性モードで構成されたNetScalerインスタンスに対してPooled capacityライセンスを構成することもできます。高可用性モードのVPXインスタンスにPooled capacityライセンスを構成するには、「NetScaler VPX高可用性ペアの永続ライセンスをNetScaler Pooled Capacityにアップグレードする」を参照してください。

### 前提条件

**NetScaler Pooled capacityにアップグレードするには:**

1. Webブラウザで、VPXインスタンスのIPアドレス (例: `<http://192.168.100.1>`) を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。
3. **ようこそ**ページで、**続行**をクリックします。
4. **構成**タブで、**システム > ライセンス**に移動し、**ライセンスの管理**をクリックします。
5. **ライセンス**ページで、**新しいライセンスの追加**をクリックします。
6. **ライセンス**ページで、**リモートライセンスの使用**を選択し、次の操作を行います。

   a. **リモートライセンスモード**ドロップダウンリストで、**プールライセンス**を選択します。
   b. **サーバー名/IPアドレス**フィールドに、ライセンスサーバーの詳細を入力します。
   c. **続行**をクリックします。

7. **ライセンスの割り当て**で、次の操作を行います。

   a. ドロップダウンリストからライセンスエディションを選択します。

   b. **割り当て**メニューからNetScalerアプライアンスに帯域幅を割り当て、**ライセンスの取得**をクリックします。

8. プロンプトが表示されたら、**Reboot**をクリックしてアプライアンスを再起動します。

   NetScalerインスタンスを再起動します(/en-us/netscaler-application-delivery-management-software/media/upgrade-license5.jpg)

9. 確認ダイアログボックスで、**Yes**をクリックします。
10. VPXインスタンスが再起動したら、インスタンスにログオンします。**Welcome**ページで、**Continue**をクリックします。

    **Licenses**ページには、NetScaler VPXアプライアンスでライセンスされているすべての機能が表示されます。**X**をクリックします。

11. **System > Licenses**に移動し、**Manage Licenses**をクリックします。

    **Manage Licenses**ページで、ライセンスサーバー、ライセンスエディション、および割り当てられた帯域幅の詳細を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler VPX高可用性ペアの永続ライセンスをNetScalerプール容量にアップグレードする

高可用性モードで構成されたVPXインスタンスの場合、HAペアのプライマリインスタンスとセカンダリインスタンスの両方でプール容量を構成する必要があります。プライマリインスタンスとセカンダリインスタンスの両方に、同じ容量のライセンスを割り当てる必要があります。たとえば、HAペアの各インスタンスから1 Gbpsの容量が必要な場合、共通プールから2倍の容量（2 Gbps）が必要になります。その後、HAペアのプライマリインスタンスとセカンダリインスタンスにそれぞれ1 Gbpsの容量を割り当てることができます。

**既存のNetScaler VPX HAセットアップをNetScalerプール容量にアップグレードするには：**

1. セカンダリVPX（ノード2）インスタンスにログオンします。Webブラウザで、NetScalerアプライアンスのIPアドレス（例: `http://192.168.100.1`）を入力します。
2. **User Name**と**Password**に、管理者資格情報を入力します。
3. **Welcome**ページで、**Continue**をクリックします。
4. Configurationタブで、**System > Licenses**に移動し、**Manage Licenses**をクリックします。
5. **Licenses**ページで、**Add New License**をクリックします。
6. 「**リモートライセンスの使用**」を選択し、次の操作を行います。

   「リモートライセンスの使用」(/en-us/netscaler-application-delivery-management-software/media/upgrade-vpx-2.png)

   a. 「**リモートライセンスモード**」ドロップダウンリストで、「**プールライセンス**」を選択します。
   b. 「**サーバー名/IPアドレス**」フィールドに、ライセンスサーバーの詳細を入力します。
   c. インスタンスのプールライセンスをNetScaler Console経由で管理する場合は、「**NetScaler Consoleに登録**」チェックボックスが選択されていることを確認し、NetScaler Consoleの資格情報を入力します。
   d. 「**続行**」をクリックします。
7. 「**ライセンスの割り当て**」で、次の操作を行います。

   a. ドロップダウンリストからライセンスエディションを選択します。

      「ライセンスエディションの選択」(/en-us/netscaler-application-delivery-management-software/media/upgrade-vpx-3.jpg)

   b. 「**割り当て**」メニューからNetScalerアプライアンスに帯域幅を割り当て、「**ライセンスの取得**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「ライセンスの割り当て」(/en-us/netscaler-application-delivery-management-software/media/upgrade-vpx-4.jpg)

c. プロンプトが表示されたら、「**再起動**」をクリックしてインスタンスをウォーム再起動します。

「インスタンスをウォーム再起動する」(/en-us/netscaler-application-delivery-management-software/media/upgrade-license5.jpg)

8. 「**確認**」ダイアログボックスで、「**はい**」をクリックします。

VPXインスタンスが再起動します。

プロンプトが表示されたら、**Reboot** をクリックしてアプライアンスを再起動します。アプライアンスが新しいライセンスで稼働したら、`force ha failover` と入力してフェイルオーバーを強制実行します。このフェイルオーバーにより、HAペアが正常な状態であることが保証されます。

9. フェイルオーバー後、新しいセカンダリVPXインスタンス（ノード1）にログオンし、新しいセカンダリをプールに追加するために同じプロセスを繰り返します。

HAペアのプライマリインスタンスとセカンダリインスタンスを元のHAペア構成に変更したい場合は、フェイルオーバーを強制実行します。HAペア内の任意のインスタンスで次のコマンドを実行します。

```
> force ha failover
```

10. VPXインスタンスがプール容量ライセンスにアップグレードされたことを確認するには、プライマリインスタンスとセカンダリインスタンスにログオンし、次の手順を完了します。

a. **Welcome** ページで、**Continue** をクリックします。

b. Configurationタブで、**System > Licenses** に移動し、**Manage Licenses** をクリックします。**Manage Licenses** ページで、ライセンスサーバー、ライセンスエディション、および割り当てられた帯域幅の詳細を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScaler MPX の永続ライセンスを NetScaler Pooled Capacity にアップグレードする

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026 にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix 製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026 以降、NetScaler インスタンスをアクティベートしてライセンスを付与する唯一の方法は LAS になり、NetScaler Flexed ライセンス (CPL/UHMC)、従来の NetScaler Pooled ライセンス、および NetScaler Fixed term Bandwidth ライセンスをサポートします。サポートを継続するには、NetScaler および NetScaler Console の展開が LAS 互換バージョンである必要があります。

LAS 互換の NetScaler の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス：14.1-51.x

  **注:** Console on-prem の LAS サポートは、リリース 14.1-51.x 以降です。ただし、ファイルベースのライセンスは、April 15 2026 をもって、Console on-prem リリース 14.1-51.x 以降および 13.1-60.x 以降では非推奨となります。Console on-prem リリース 14.1-51.x またはリリース 13.1-60.x 以降にアップグレードした場合、15th April 2026 までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1 は LAS をサポートしていないため、15th April 2026 までに Console on-prem リリース 14.1-51.x 以降にアップグレードし、LAS に切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来の NetScaler ライセンス形式は LAS ではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用している NetScaler インスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LAS ベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrix は、これらの要件を遵守しない場合、Citrix が法律または衡平法上持つその他の救済措置に加えて、責任を負う

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ことなく Citrix Maintenance を制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
続行する前に、以下の注記をお読みください。

永続ライセンスを持つ NetScaler MPX は、NetScaler Pooled Capacity ライセンスにアップグレードできます。NetScaler Pooled Capacity ライセンスにアップグレードすると、ライセンスプールから NetScaler アプライアンスにオンデマンドでライセンスを割り当てることができます。高可用性モードで構成された NetScaler インスタンスに対して、NetScaler Pooled Capacity ライセンスを構成することもできます。高可用性モードの NetScaler MPX インスタンスに NetScaler Pooled Capacity ライセンスを構成する方法については、「NetScaler MPX 高可用性ペアの永続ライセンスを NetScaler Pooled Capacity にアップグレードする」を参照してください。

**注**

永続ライセンスからプール容量ライセンスへの変換は、ライセンスエンタイトルメントにとって一方通行のプロセスです。プール容量ライセンスを永続ライセンスに戻すことはできません。 **重要**

NetScaler MPXをNetScalerプール容量ライセンスにアップグレードするには、MPX-Zライセンスをアプライアンスにアップロードする必要があります。
**NetScalerプール容量にアップグレードするには：**

1. Webブラウザで、NetScalerのIPアドレス（例：`<http://192.168.100.1>`）を入力します。
2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。
3. **ようこそ**ページで、**続行**をクリックします。
4. ゼロ容量ライセンス（MPX-Zライセンス）をアップロードします。構成タブで、**システム** \> **ライセンス**に移動します。
5. 詳細ペインで、**ライセンスの管理**をクリックし、**新しいライセンス**の追加をクリックします。
6. **ライセンス**ページで、**ライセンスファイルのアップロード**を選択し、**参照**をクリックしてローカルマシンからゼロ容量ライセンスを選択します。
7. ライセンスがアップロードされたら、**再起動**をクリックしてアプライアンスを再起動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**警告**

MPX-Zライセンスを適用すると、アプライアンス上のSSLオフロードを含む機能はライセンスなしの状態になります。アプライアンスはHTTPSリクエストの処理を停止します。

アップグレード前にアプライアンスで**セキュアアクセスのみ**オプションが有効になっている場合、HTTPSを使用してNetScaler Console GUI経由でアプライアンスに接続することはできません。

8. **確認**ページで、**はい**をクリックします。
9. アプライアンスが再起動したら、アプライアンスにログオンします。
10. 「ようこそ」ページで、「**ライセンス**」セクションをクリックします。

    設定を保存して再起動(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-4-welcome.jpg)

11. 「**ライセンスサーバー**」セクションで、次の操作を行います。

    ライセンスサーバーを構成(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-5.jpg)

    a. 「**サーバー名/IPアドレス**」フィールドに、ライセンスサーバーの詳細を入力します。
    b. 「**ライセンスポート**」フィールドに、ライセンスサーバーのポートを入力します。デフォルト値: 27000。
    c. NetScaler Console を介してインスタンスのプールライセンスを管理する場合は、「**管理のためにライセンスサーバーに登録**」チェックボックスをオンにし、NetScaler Console の資格情報を入力します。
    d. 「**続行**」をクリックします。

12. 「**ライセンスの割り当て**」で、次の操作を行います。

    a. ドロップダウンリストからライセンスエディションを選択します。

       ライセンスを割り当てる(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-6.jpg)

    b. 「**割り当て**」メニューからNetScalerに帯域幅を割り当て、「**ライセンスの取得**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスを取得(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-7.jpg)

c. プロンプトが表示されたら、「**再起動**」をクリックしてアプライアンスを再起動します。

13. NetScaler MPX が再起動したら、NetScaler MPX にログオンします。「**ようこそ**」ページで、「**続行**」をクリックします。

「**ライセンス**」ページには、すべてのライセンス機能が一覧表示されます。

14. **システム > ライセンス**に移動し、**ライセンスの管理**をクリックします。

**ライセンスの管理**ページで、ライセンスサーバー、ライセンスエディション、および割り当てられた帯域幅の詳細を表示できます。

ライセンスサーバーのライセンス詳細(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-10.jpg)

### NetScaler MPX高可用性ペアにおける永続ライセンスのNetScalerプール容量へのアップグレード

高可用性モードで構成されたMPXアプライアンスの場合、HAペアのプライマリおよびセカンダリNetScalerインスタンスの両方でプール容量を構成する必要があります。HAペアのプライマリおよびセカンダリNetScalerインスタンスの両方に、同じ容量のライセンスを割り当てます。たとえば、HAペアの各インスタンスから1 Gbpsの容量が必要な場合、共通プールから2 Gbpsの容量を割り当てる必要があります。2 Gbpsの容量があれば、HAペアのプライマリおよびセカンダリNetScalerインスタンスにそれぞれ1 Gbpsを割り当てることができます。

**重要**

NetScaler MPXをNetScalerプール容量ライセンスを使用するようにアップグレードするには、MPX-Zをアプライアンスにアップロードする必要があります。

#### 前提条件

HAペアのプライマリおよびセカンダリインスタンスの両方にMPX-Zライセンスをアップロードしていることを確認してください。

#### HAペアのNetScaler MPXインスタンスにMPX-Zライセンスをアップロードするには：

1. Webブラウザで、アプライアンスのIPアドレスを入力します。例：`<http://192.168.100.1>`.
2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **ようこそ**ページで、**続行**をクリックします。
4. ゼロ容量ライセンス（MPX-Zライセンス）をアップロードします。**構成**タブで、**システム \> ライセンス**に移動します。
5. 詳細ペインで、**ライセンスの管理**をクリックし、**新しいライセンスの追加**をクリックします。
6. **ライセンス**ページで、**ライセンスファイルのアップロード**を選択し、**参照**をクリックしてローカルマシンからゼロキャパシティライセンスを選択します。

   ライセンスがアップロードされると、アプライアンスの再起動を促されます。
7. **再起動**をクリックしてアプライアンスを再起動します。
8. **確認**ページで、**はい**をクリックします。

**既存のHAセットアップをNetScalerプールキャパシティにアップグレードするには：**

1. セカンダリNetScaler MPXインスタンスにログオンします。Webブラウザで、NetScalerのIPアドレス（例: `<http://192.168.100.1>`）を入力します。
2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。
3. **ようこそ**ページで、**ライセンス**セクションをクリックします。

   高可用性セットアップへようこそ(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-4-welcome.jpg)
4. **ライセンスサーバー**セクションで、次の操作を行います。

   ライセンスサーバー(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-5.jpg)

   a. **サーバー名/IPアドレス**フィールドに、ライセンスサーバーの詳細を入力します。
   b. **ライセンスポート**フィールドに、ライセンスサーバーポートを入力します。デフォルト値: 27000。
   c. NetScaler Consoleを介してインスタンスのプールライセンスを管理したい場合は、**管理のためにライセンスサーバーに登録**チェックボックスを選択し、NetScaler Consoleの資格情報を入力します。
   d. 「**続行**」をクリックします。
5. 「**ライセンスの割り当て**」で、次の操作を行います。

   a. ドロップダウンリストからライセンスエディションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 「**割り当て**」メニューからNetScalerに帯域幅を割り当て、「**ライセンスの取得**」をクリックします。



c. プロンプトが表示されたら、「**再起動**」をクリックしてアプライアンスを再起動します。アプライアンスが新しいライセンスで稼働したら、`force ha failover`と入力してフェールオーバーを強制実行します。このフェールオーバーにより、HAペアが正常な状態であることが保証されます。

6. 既存のプライマリNetScaler MPXにログオンし、アプライアンスを再起動します。次の操作を実行します。

a. Webブラウザで、NetScalerのIPアドレス（例: `<http://192.168.100.1>`）を入力します。

b. 「**ユーザー名**」と「**パスワード**」に管理者資格情報を入力します。

c. 「**ようこそ**」ページで、「**続行**」をクリックします。

d. 「**構成**」タブで、「**システム**」をクリックします。

e. 「**システム**」ページで、「**再起動**」をクリックします。

f. 「**再起動**」ページで、「**ウォーム再起動**」を選択し、「**OK**」をクリックします。



プライマリ NetScaler MPX が再起動すると、HA ペアのセカンダリ NetScaler MPX になります。HA ペアのプライマリおよびセカンダリインスタンスを元の HA ペア構成に戻したい場合は、フェイルオーバーを強制実行します。HA ペアのいずれかのインスタンスで次のコマンドを実行します。

```
> force ha failover
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScaler SDXの永続ライセンスをNetScalerプール容量にアップグレードする

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降にNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScalerプールライセンス、およびNetScaler固定期間帯域幅ライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開は、LAS互換バージョンである必要があります。

LAS互換の最小要件のNetScalerバージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードすると、ライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている場合、お客様には利用できない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負う

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ことなくCitrixメンテナンスを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
永続ライセンスを持つNetScaler SDXは、NetScalerプール容量ライセンスにアップグレードできます。NetScalerプール容量ライセンスにアップグレードすると、ライセンスプールからNetScalerにオンデマンドでライセンスを割り当てることができます。高可用性モードで構成されたNetScalerインスタンスに対して、NetScalerプール容量ライセンスを構成することもできます。

**重要**

永続ライセンスからプール容量ライセンスへの変換は、一方向のライセンスエンタイトルメントプロセスです。プール容量ライセンスを永続ライセンスに戻すことはできません。

- NetScaler SDXをNetScaler Pooled Capacityライセンスにアップグレードするには、SDX-Zライセンスをアプライアンスにアップロードする必要があります。
- NetScaler ConsoleでNetScalerインスタンスを追加する権限があることを確認してください。
- 現在のライセンスへの影響がないことを確認するために、お客様は永続ライセンスの一部として利用可能なインスタンスと帯域幅の数を同じだけ割り当てる必要があります。

**NetScaler Pooled Capacityにアップグレードするには：**

1. Webブラウザで、`<http://192.168.100.1>`のようにNetScaler SDXのIPアドレスを入力します。
2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。
3. **ようこそ**ページで、**続行**をクリックします。
4. ゼロキャパシティライセンスをアップロードします。構成タブで、**システム** > **ライセンス**に移動します。
5. **ライセンスの管理**ページで、**ライセンスファイルの追加**をクリックします。
6. **ライセンス**ページで、**ローカルコンピューターからライセンスファイルをアップロード**を選択し、**参照**をクリックしてローカルマシンからゼロキャパシティライセンスを選択します。次に、**完了**をクリックします。

   ゼロキャパシティライセンスが正常に適用されると、**ライセンス**ページに**プールされたライセンス**セクションが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

古いライセンスファイルを削除するためにNetScaler SDXを再起動する必要がないため、ダウンタイムを回避できます。詳細については、NetScalerサポートにお問い合わせください。

7. **プールされたライセンス**セクションで、次の操作を行います。

   a. 「**ライセンスサーバー名またはIPアドレス**」フィールドに、ライセンスサーバーの詳細を入力します。NetScaler Consoleサーバーをライセンスサーバーとして構成する場合は、NetScaler ConsoleサーバーのIPアドレスを指定します。

   b. 「**ポート番号**」フィールドに、ライセンスサーバーのポートを入力します。デフォルト値: 27000。

   c. ライセンスサーバーの**ユーザー名**と**パスワード**を指定します。

      - NetScaler Consoleサーバーの場合は、管理者資格情報を入力します。
      - NetScaler Consoleエージェントの場合は、エージェント資格情報を入力します。

   d. 「**ライセンスの取得**」をクリックします。

8. 「**ライセンスの割り当て**」ウィンドウで、必要なインスタンスと帯域幅を指定し、「**割り当て**」をクリックします。

   「**ライセンスの管理**」ページで、ライセンスサーバー、ライセンスエディション、およびプールから割り当てられたインスタンスと帯域幅の詳細を表示できます。

**注**

永続ライセンスをプール容量にアップグレードしても、SDXアプライアンスの再起動は必要ありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# クラスターモードのNetScalerインスタンスにおけるNetScalerプール容量

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  **注:** ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負う

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ことなくCitrixメンテナンスを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
クラスターとして構成されたNetScalerインスタンスで、NetScalerプール容量を構成できます。クラスターモードのNetScalerインスタンスでプール容量を構成するための前提条件は次のとおりです。

- インスタンスは、クラスターを形成するために個別にプール容量ライセンスモードで実行されている必要があります。
- すべてのインスタンスは同じ帯域幅で実行されている必要があります。
- All the instances checked out the Pooled capacity from the same NetScaler Console.
- New instances cannot be added to an existing NetScaler cluster unless their capacity and NetScaler Console configurations are the same as those of the existing instances in the cluster.

NetScalerクラスターからの容量チェックアウトは、すべてのクラスターノードに同じ容量を割り当て、チェックアウト帯域幅 = 提供された帯域幅 * ノード数となります。

例えば、NetScalerクラスターから50 Mbpsの帯域幅をチェックアウトし、クラスターに12個のインスタンスが含まれている場合、各インスタンスは自動的に50 Mbpsを受け取ります。そして、プールから600 Mbpsがチェックアウトされます。

**注**

クラスター内の1つ以上のインスタンスが応答しなくなった場合でも、クラスターは残りのインスタンスの容量でトラフィックの処理を続行します。

### NetScalerクラスターにNetScaler Pooled capacityを割り当てる

各クラスターノードにライセンスを個別に割り当てます。これは、クラスターノード間でライセンスを伝播および同期するコマンドが無効になっているためです。

各クラスターノードで次の手順を繰り返します。

1. Webブラウザーで、NetScaler IPアドレス (NSIP) を入力します。例: `http://192.168.100.1`。
2. 「**ユーザー名**」フィールドと「**パスワード**」フィールドに、管理者資格情報を入力します。
3. 「**Configuration**」タブで、「**System > Licenses > Manage Licenses**」の順に移動します。「**Add New License,**」をクリックし、「**Use Pooled Licensing**」を選択します。
4. 「**Server Name/IP Address**」フィールドに、ライセンスサーバーの名前またはアドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. インスタンスのプールライセンスをNetScaler Console経由で管理する場合は、「**Register with NetScaler Console for manageability**」チェックボックスをオンにして、NetScaler Consoleの資格情報を入力します。
6. ライセンスエディションと必要な帯域幅を選択し、**Get Licenses** をクリックします。



7. ライセンスの割り当てを変更または解放するには、**割り当ての変更**または**割り当ての解放**を選択します。



8. **割り当ての変更**をクリックすると、ライセンスサーバーで利用可能なライセンスを示すポップアップウィンドウが表示されます。

> **注**
>
> 帯域幅の割り当ては、対応するフォームファクターの最小帯域幅単位の整数倍である必要があります。



9. **割り当て**ドロップダウンリストから、NetScalerインスタンスに帯域幅またはインスタンスを割り当てることができます。次に、**ライセンスの取得**をクリックします。
10. ポップアップウィンドウのドロップダウンリストから、ライセンスエディションと必要な帯域幅を選択できます。

> **注**
>
> 帯域幅の割り当てを変更しても再起動は不要ですが、ライセンスエディションを変更する場合はウォーム再起動が必要です。

### CLIを使用してNetScalerクラスターにNetScalerプール容量を割り当てる

各クラスターノードに個別にライセンスを割り当てます。クラスターノード間でライセンスを伝播および同期するコマンドは無効になっているためです。

各クラスターノードで次の手順を繰り返します。

1. SSHクライアントで、NetScaler IPアドレス（NSIP）を入力し、管理者資格情報を使用してログインします。
2. ライセンスサーバーを追加するには、次のコマンドを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port
number >]
```

3. ライセンスサーバーで利用可能なライセンスを表示するには、次のコマンドを入力します。

```
sh licenseserverpool
```

4. NetScaler VPXアプライアンスにライセンスを割り当てるには、次のコマンドを入力します。

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

## NetScaler VPXおよびNetScaler BLXライセンスのチェックインとチェックアウト

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASはNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:** ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScaler ConsoleからオンデマンドでNetScaler VPXおよびNetScaler BLXライセンスをNetScalerインスタンスに割り当てることができます。NetScaler Consoleソフトウェアはライセンスを保存および管理し、スケーラブルで自動化されたライセンスプロビジョニングを提供するライセンスフレームワークを備えています。インスタンスは、プロビジョニング時にNetScaler Consoleからライセンスをチェックアウトできます。インスタンスが削除または破棄されると、そのインスタンスはライセンスをNetScaler Consoleソフトウェアにチェックインし直します。

### 前提条件

次の前提条件が満たされていることを確認してください。

- ソフトウェアバージョン12.0を実行しているNetScaler VPXイメージを使用しています。例: NSVPX-ESX-12.0-xx.xx_nc.zip
- バージョン12.0を実行しているNetScaler Consoleをインストール済みです。例: MAS-ESX-12.0-xx.xx.zip

**注**

NetScaler Consoleで既存のNetScaler VPXライセンスを管理するには、ライセンスをNetScaler Consoleに再ホストする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Consoleでのライセンスのインストール

**注**

ライセンスをインストールする前に、ソフトウェアエディションまたは帯域幅を変更した場合は、NetScaler Console仮想アプライアンスを再起動してください。

**NetScaler Consoleにライセンスファイルをインストールするには:**

1. Webブラウザで、NetScaler ConsoleのIPアドレスを入力します（例: `<http://192.168.100.1>`）。
2. とに、管理者資格情報を入力します。
3. **インフラストラクチャ > プールされたライセンス**に移動します。
4. **ライセンスファイル**セクションで、次のいずれかのオプションを選択します。

   - **ローカルコンピューターからライセンスファイルをアップロード** - ライセンスファイルがすでにローカルコンピューターにある場合は、NetScaler Consoleにアップロードできます。ライセンスファイルを追加するには、**参照**をクリックして追加するライセンスファイル（.lic）を選択します。次に、**完了**をクリックします。
   - **ライセンスアクセスコードを使用** - Citrixは、購入したライセンスのライセンスアクセスコードをメールで送信します。ライセンスファイルを追加するには、テキストボックスにライセンスアクセスコードを入力し、**ライセンスの取得**をクリックします。

   **注**

   ライセンスをインストールするためにライセンスアクセスコードを使用する前に、インターネットに接続していることを確認してください。

   いつでも、**ライセンス設定**ページからNetScaler Consoleにライセンスを追加できます。

### 確認

NetScaler Console GUIで、利用可能なライセンスと割り当て済みのライセンスを表示できます。

**ライセンスを表示するには：**

1. Webブラウザで、NetScaler ConsoleのIPアドレス（例：`<http://192.168.100.1>`）を入力します。
2. **ユーザー名**と**パスワード**に、管理者資格情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Configurationタブで、**Infrastructure > Pooled Licensing > VPX Licenses**に移動します。



4. 利用可能なライセンスセクションの下のテーブルで、割り当て済みのライセンスを表示できます。

### NetScaler GUIを使用して、NetScaler VPXおよびNetScaler BLXライセンスをNetScalerインスタンスに割り当てる

1. Webブラウザで、NetScalerインスタンスのIPアドレス（例：`<http://192.168.100.1>`）を入力します。
2. **ユーザー名**と**パスワード**フィールドに、管理者資格情報を入力します。
3. Configurationタブで、**Settings > Licenses > Manage Licenses**に移動し、**Add New License**をクリックして、**Use Remote Licensing > CICO Licensing**を選択します。
4. **サーバー名/IPアドレスフィールド**に、ライセンスサーバーの詳細を入力します。
5. 「**ユーザー名**」と「**パスワード**」にNetScaler Consoleの資格情報を入力し、「**続行**」をクリックします。



6. 必要な帯域幅のライセンスエディションを選択し、「**ライセンスの取得**」をクリックします。



7. 「**再起動**」をクリックすると、NetScalerインスタンスが再起動します。
8. **システム > ライセンス > ライセンスの管理**に移動し、「**割り当ての変更**」または「**割り当ての解放**」を選選択することで、ライセンスの割り当てを変更または解放できます。



9. 「**割り当ての変更**」をクリックすると、ライセンスサーバーで利用可能なライセンスを示すポップアップウィンドウが表示されます。必要なライセンスを選択し、「**ライセンスの取得**」をクリックします。



### NetScaler CLIを使用してNetScalerインスタンスにNetScaler VPXおよびNetScaler BLXライセンスを割り当てる

1. SSHクライアントで、NetScalerインスタンスのIPアドレスを入力し、管理者資格情報を使用してログオンします。
2. ライセンスサーバーを追加するには、次のコマンドを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port
number >]
```

3. ライセンスサーバーで利用可能なライセンスを表示するには、次のコマンドを入力します。

```
sh licenseserverpool
```

4. NetScaler にライセンスを割り当てるには、次のコマンドを入力します。

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

### API を使用して NetScaler VPX および NetScaler BLX ライセンスを NetScaler インスタンスに割り当てる

Web ブラウザまたは API クライアントで、管理者資格情報を使用して NetScaler インスタンスにログオンします。

**ライセンスサーバーを追加するには:**

1. リクエストタイプを **Post** に設定します。
2. パスを /nitro/v1/config/nslicensingserver に設定します。
3. ペイロードを次のように設定します。

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

object= {“params”;{warning”:”yes”},”nslicensing server”;
{servername”:”\<NetScaler Console IP\>”, “port”:”27000”}}\\r\\n
```

NetScaler Console はリクエストに応答します。次の応答例は成功を示しています。

**ライセンスサーバーで利用可能なライセンスを表示するには:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. リクエストタイプを **Get** に設定します。
2. パスを /nitro/v1/config/nslicenseserverpool に設定します。

   NetScaler Console がリクエストに応答します。以下のサンプル応答は、成功とライセンスサーバーで利用可能なライセンスのリストを示しています。

**NetScaler にライセンスを割り当てるには:**

1. リクエストタイプを **Post** に設定します。
2. パスを /nitro/v1/config/nscapacity に設定します。
3. ペイロードを次のように設定します。

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

{“nscapacity:{“platform”:”VE8000”}}\\r\\n
```

   NetScaler Console がリクエストに応答します。以下のサンプル応答は、成功を示しています。

### ライセンスサーバーの IP アドレスを更新する

インスタンス上の割り当てられたライセンス帯域幅やデータ損失に影響を与えることなく、NetScaler VPX および NetScaler BLX インスタンスのライセンスサーバー IP アドレスを更新できます。

**CLI を使用して更新**: CLI を使用してライセンスサーバーの IP アドレスを更新するには、インスタンスで次のコマンドを入力します。

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

このコマンドは新しいサーバーに接続し、以前のライセンスサーバーに関連付けられていたリソースを解放します。

**GUI を使用して更新**: GUI を使用してライセンスサーバーの IP アドレスを更新するには、**System > Licenses > Manage Licenses** に移動し、**Add New License** をクリックします。詳細について

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、NetScaler GUI を使用して NetScaler インスタンスに NetScaler VPX および NetScaler BLX ライセンスを割り当てる を参照してください。

### NetScaler VPX および NetScaler BLX のチェックイン/チェックアウトライセンスの有効期限チェックを設定する

NetScaler VPX および NetScaler BLX ライセンスの有効期限しきい値を設定できるようになりました。しきい値を設定すると、ライセンスの有効期限が近づいたときに NetScaler Console がメールまたは SMS で通知を送信します。ライセンスが NetScaler Console で期限切れになった場合も、SNMP トラップと通知が送信されます。

ライセンスの有効期限通知が送信されるとイベントが生成され、このイベントは NetScaler Console で表示できます。

**ライセンスの有効期限チェックを設定するには:**

1. **Infrastructure > Pooled Licensing** に移動します。
2. **License Settings** ページの **License Expiry Information** セクションで、有効期限が近づいているライセンスの詳細を確認できます。
   - **Feature**: 有効期限が近づいているライセンスの種類。
   - **Count**: 影響を受ける仮想サーバーまたはインスタンスの数。
   - **Days to expiry**: ライセンスの有効期限までの日数。
3. **Notification Settings** セクションで、**Edit** アイコンをクリックし、アラートしきい値を指定します。管理者に通知するために使用するプールライセンス容量の割合を設定できます。
4. 適切なチェックボックスを選択して、送信する通知の種類を選択します。通知の種類は次のとおりです。
   a. **Email Profile**: メールサーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくとメールがトリガーされます。
   b. **SMS Profile**: ショートメッセージサービス (SMS) サーバーとプロファイルの詳細を指定します。ライセンスの有効期限が近づくと SMS メッセージがトリガーされます。
5. 次に、ライセンスの有効期限までの日数で、いつ通知を送信するかを指定します。
6. **Save** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScaler仮想CPUライセンス

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026 にEnd of Life (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026 以降、LASがNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexed licenses (CPL/UHMC)、従来のNetScaler Pooled licenses、およびNetScaler Fixed term Bandwidth licensesをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-prem リリース14.1-51.x以降および13.1-60.x以降では April 15 2026 をもって非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026 までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026 までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンスは、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先に進む前に、以下の注記をお読みください。

**注:**

vCPUライセンスは購入できなくなりました。詳細については、ライセンスを参照してください。

お客様のようなデータセンター管理者は、ネットワーク機能を簡素化し、コストを削減し、拡張性を高める新しいテクノロジーに移行しています。新しいデータセンターアーキテクチャには、少なくとも以下の機能が含まれている必要があります。

- ソフトウェア定義ネットワーク (SDN)
- ネットワーク機能仮想化 (NFV)
- ネットワーク仮想化 (NV)
- マイクロサービス

このような動きには、絶えず変化するビジネスニーズに対応するために、ソフトウェア要件が動的で、柔軟で、俊敏であることも必要です。ライセンスも、使用状況を完全に可視化できる中央管理ツールによって管理されることが期待されています。

### NetScaler VPX の仮想 CPU ライセンス

以前は、NetScaler VPX ライセンスはインスタンスによる帯域幅消費に基づいて割り当てられていました。NetScaler VPX は、バインドされているライセンスエディションに基づいて、特定の帯域幅とその他のパフォーマンスメトリックを使用するように制限されています。利用可能な帯域幅を増やすには、より多くの帯域幅を提供するライセンスエディションにアップグレードする必要があります。特定のシナリオでは、帯域幅の要件は少ないかもしれませんが、SSL TPS や圧縮スループットなどの他の L7 パフォーマンスの要件は高くなります。このような場合、NetScaler VPX ライセンスのアップグレードは適切ではないかもしれません。しかし、CPU を多用する処理に必要なシステムリソースを解放するために、大容量の帯域幅を持つライセンスを購入する必要があるかもしれません。NetScaler Console は、仮想 CPU 要件に基づいて NetScaler インスタンスにライセンスを割り当てることをサポートするようになりました。

仮想 CPU 使用量ベースのライセンス機能では、ライセンスは特定の NetScaler VPX が使用できる CPU の数を指定します。そのため、NetScaler VPX は、ライセンスサーバーから、自身で実行されている仮想 CPU の数にのみライセンスをチェックアウトできます。NetScaler VPX は、システムで実行されている CPU の数に応じてライセンスをチェックアウトします。NetScaler VPX は、ライセンスをチェックアウトする際にアイドル状態の CPU を考慮しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プールされたライセンス容量および CICO ライセンス機能と同様に、NetScaler Console ライセンスサーバーは、仮想 CPU ライセンスの個別のセットを管理します。ここでも、仮想 CPU ライセンス用に管理される3つのエディションは、Standard、Advanced、Premium です。これらのエディションは、帯域幅ライセンスのエディションによってアンロックされる機能と同じ機能セットをアンロックします。

仮想 CPU の数に変更があった場合、またはライセンスエディションに変更があった場合は、新しいライセンスセットのリクエストを開始する前に、必ずインスタンスをシャットダウンする必要があります。ライセンスをチェックアウトした後、NetScaler VPX を再起動してください。

**GUI を使用して NetScaler VPX でライセンスサーバーを構成するには:**

1. NetScaler VPX で、**System > Licenses** に移動し、**Manage Licenses** をクリックします。
2. **License** ページで、**Add New License** をクリックします。
3. **Licenses** ページで、**Use remote licensing** オプションを選択します。
4. **Remote Licensing Mode**リストから**CPU licensing**を選択します。
5. ライセンスサーバーのIPアドレスとポート番号を入力します。
6. **Continue**をクリックします。

   

   **注**

   NetScaler VPXインスタンスは常にNetScaler Consoleに登録する必要があります。まだ登録していない場合は、**Register with NetScaler Console**を有効にし、NetScaler Consoleのログイン資格情報を入力します。

7. **Allocate licenses**ウィンドウで、ライセンスの種類を選択します。ウィンドウには、合計および利用可能な仮想CPUと、割り当て可能なCPUが表示されます。**Get Licenses**をクリックします。
8. ライセンスを適用するには、次のページで**Reboot**をクリックします。

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

現在のライセンスを解放し、別のエディションからチェックアウトすることもできます。たとえば、インスタンスでStandardエディションのライセンスがすでに実行されている場合、そのライセンスを解放してからAdvancedエディションからチェックアウトできます。

### CLIを使用してNetScaler VPXライセンスでライセンスサーバーを構成する

NetScaler VPXコンソールで、次の2つのタスクに対して次のコマンドを入力します。

1. ライセンスサーバーをNetScaler VPXに追加するには:

```
add licenseserver <IP address of the license server>
```

2. ライセンスを適用するには:

```
set capacity -vcpu - edition premium
```

プロンプトが表示されたら、次のコマンドを入力してインスタンスを再起動します。

```
reboot -w
```

### ライセンスサーバーのIPアドレスを更新する

NetScaler VPXインスタンスのライセンスサーバーIPアドレスは、インスタンスに割り当てられたライセンス帯域幅やデータ損失に影響を与えることなく更新できます。ライセンスサーバーIPアドレスを更新するには、NetScaler VPXインスタンスで次のコマンドを入力します。

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

このコマンドは新しいサーバーに接続し、以前のライセンスサーバーに関連付けられていたリソースを解放します。

### NetScaler Consoleでの仮想CPUライセンスの管理

1. NetScaler Consoleで、**インフラストラクチャ > プールライセンス > プールVCPU** に移動します。
2. このページには、各ライセンスエディションタイプに割り当てられたライセンスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 各ドーナツ内の数字をクリックすると、このライセンスを使用しているNetScalerインスタンスが表示されます。



### NetScaler CPXの仮想CPUライセンス

NetScaler CPXインスタンスをプロビジョニングする際に、インスタンスのCPU使用率に応じてライセンスサーバーからライセンスをチェックアウトするようにNetScaler CPXインスタンスを設定できます。

NetScaler CPXは、NetScaler Consoleで実行されているライセンスサーバーに依存してライセンスを管理します。NetScaler CPXは起動時にライセンスサーバーからライセンスをチェックアウトします。NetScaler CPXがシャットダウンすると、ライセンスはライセンスサーバーにチェックインされます。

'docker pull' コマンドを使用して、QuayコンテナレジストリからNetScaler CPXイメージをダウンロードし、環境に展開できます。

NetScaler CPXライセンスには、次の3種類のライセンスタイプがあります。

1. NetScaler CPXおよびVPXでサポートされている仮想CPUサブスクリプションライセンス
2. プールされたキャパシティライセンス
3. NetScaler CPXのみでシングルから複数のvCPUをサポートするCP1000ライセンス

**NetScaler CPXインスタンスのプロビジョニング中にvCPUサブスクリプションライセンスを構成するには：**

NetScaler CPXインスタンスが使用するvCPUライセンスの数を指定します。

- この値は、Docker、Kubernetes、またはMesos/Marathonを介して環境変数として入力されます。
- ターゲット変数は「CPX_CORES」です。NetScaler CPXは1から16コアをサポートできます。

2コアを指定するには、docker runコマンドを次のように実行します。

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2
```

NetScaler CPXインスタンスをプロビジョニングする際に、NetScalerライセンスサーバーを**docker run**コマンドで環境変数として次のように定義します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT>
cpx:11.1
```

ここで、,

- \<*LS*_*IP*_*ADDRESS*\> はNetScalerライセンスサーバーのIPアドレスです。
- \<*LS*_*PORT*\> はNetScalerライセンスサーバーのポートです。デフォルトでは、ポートは27000です。

**注**

デフォルトでは、NetScaler CPXインスタンスはvCPUサブスクリプションプールからライセンスをチェックアウトします。インスタンスが「n」個のCPUで実行されている場合、NetScaler CPXインスタンスは「n」個のライセンスをチェックアウトします。

**NetScaler CPXインスタンスのプロビジョニング中にNetScalerプールされたキャパシティまたはCP1000ライセンスを構成するには：**

プールライセンス (帯域幅ベース) または NetScaler CPX プライベートプール (CP1000 またはプライベートプールベース) を使用して NetScaler CPX インスタンスのライセンスをチェックアウトする場合は、それに応じて環境変数を指定する必要があります。

次に例を示します。

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e
PLATFORM=CP1000 cpx:11.1
```

**CP1000**。このコマンドは、CP1000 プール (NetScaler CPX プライベートプール) からのチェックアウトをトリガーします。NetScaler CPX インスタンスは、CPX_CORES に指定された「n」個のコアに対して「n」個のインスタンスを取得します。最も一般的なユースケースは、単一インスタンスのチェックアウトのために n = 1 を指定することです。マルチコア NetScaler CPX のユースケースでは、「n」個の vCPU (「n」は 1 から 7) をチェックアウトします。

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e
BANDWIDTH=2000 cpx:11.1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**プール容量**。このコマンドは、インスタンスプールから1つのライセンスをチェックアウトし、プレミアム帯域幅プールから1000 Mbpsの帯域幅を消費しますが、NetScaler CPXは最大2000 Mbpsで実行できます。プールライセンスでは、最初の1000 Mbpsは課金されません。

**注**

帯域幅プールからチェックアウトする際は、次の表に示すように、目的のターゲット帯域幅に対応するvCPUの数を指定してください。

| コア数 (VCPU) | 最大帯域幅 |
|---|---|
| 1 | 1000 メガビット毎秒 |
| 2 | 2000 メガビット毎秒 |
| 3 | 3500 メガビット毎秒 |
| 4 | 5000 Mbpsです |
| 5 | 6500 メガビット/秒 |
| 6 | 8000 メガビット/秒 |
| 7 | 9300 メガビット/秒 |

## 問題発生時の予期される動作

以下は、記載されている問題が発生した場合のライセンスサーバーとNetScalerインスタンスの予期される動作です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ライセンスサーバーが応答を停止する

**重要:**

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にEnd of Life (EOL) となります。ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASは、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScalerプールライセンス、およびNetScaler固定期間帯域幅ライセンスをサポートし、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となります。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換の最小要件となるNetScaler®バージョンは次のとおりです。

- ネットスケーラー ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  **注:** Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、April 15 2026までファイルベースライセンスを継続して使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、April 15 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

プール型vCPU、CICO、永続などの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスがない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、Customer Careにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先に進む前に、以下の注記をお読みください。

**警告**

ライセンスサーバーが応答していません。NetScaler は現在の容量で30日間動作し続けます。30日後もライセンスサーバーへの接続が復元されない場合、NetScaler は現在の容量を失い、トラフィックの処理を停止します。30日以内に接続が復元された場合、NetScaler は現在の容量で動作し続け、トラフィックの処理を続行します。

### NetScaler プールインスタンスが応答を停止します

NetScaler プールインスタンスが応答を停止し、ライセンスサーバーが正常な状態である場合、ライセンスサーバーは10分後にすべてのNetScalerインスタンスのライセンスをチェックインします。インスタンスが再起動すると、ライセンスサーバーからすべてのライセンスをチェックアウトする要求を送信します。

### ライセンスサーバーとNetScaler プールインスタンスの両方が応答を停止します

ライセンスサーバーとNetScaler プールインスタンスの両方が再起動して接続を再確立した場合、ライセンスサーバーは10分後にすべてのライセンスをチェックインし、再起動が完了すると、NetScaler プールインスタンスは自動的にライセンスをチェックアウトします。

### NetScaler プールインスタンスがグレースフルシャットダウンします

グレースフルシャットダウン中に、ライセンスをチェックインするか、グレースフルシャットダウン前に割り当てられたライセンスを保持するかを選択できます。ライセンスをチェックインすることを選択した場合、NetScaler プールインスタンスは再起動後にライセンスなしになります。ライセンスを保持することを選択した場合、インスタンスがシャットダウンするときにライセンスサーバーにチェックインされます。インスタンスが再起動した後、ライセンスサーバーとの接続を再確立し、保存された構成で指定されたライセンスをチェックアウトします。

システムが再起動し、プールに利用可能な容量がないためにチェックアウトが失敗した場合、NetScaler は NetScaler Console プールライセンスのインベントリを確認し、利用可能な容量をチェックアウトします。構成に従って NetScaler がフル容量で稼働していない場合、この状態をユーザーに通知するために SNMP アラームが発行されます。帯域幅プールに容量がない場合、プールインスタンスはライセンスなしになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ネットワーク接続の問題

**エラーメッセージ (SYSLOG)**

ライセンスサーバーが応答していません。

ライセンスサーバーとNetScaler プールインスタンスが正常な状態であっても、ネットワーク接続が失われた場合、インスタンスは30日間、現在の容量で動作し続けます。30日後、ライセンスサーバーへの接続が復元されない場合、インスタンスは容量を失い、トラフィックの処理を停止し、ライセンスサーバーはすべてのライセンスをチェックインします。ライセンスサーバーがNetScaler インスタンスとの接続を再確立した後、インスタンスは再度ライセンスをチェックアウトします。

### 猶予期間

NetScaler プールインスタンスが正常な状態であり、ライセンスサーバーが応答を停止した場合、インスタンスは30日間、現在の容量で動作し続けます。30日後にライセンスサーバーへの接続が復元されない場合、インスタンスは容量を失い、トラフィックの処理を停止します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# システム設定の管理

以下の表に、**設定** > **管理** で利用可能なオプションのリストを示します。

## ネットワーク構成

| ネットワーク構成 | オプション | 説明 |
|---|---|---|
| IPアドレス、セカンダリNIC、ホスト名、プロキシサーバー | IPアドレス | NetScaler Consoleの展開に使用されるNetScaler Consoleネットワーク構成IPアドレスの詳細を表示します |
| | セカンダリNIC | NetScaler Consoleの管理アクセスを分離するために、セカンダリNICを構成できます。詳細については、「NetScaler Consoleにアクセスするためのデュアルの構成」を参照してください。 |
| | ホスト名 | NetScaler Consoleにホスト名を割り当てることができます。詳細については、「NetScaler Consoleサーバーにホスト名を割り当てる」を参照してください。 |
| | プロキシサーバー | NetScaler Consoleをプロキシサーバーとして構成できます。詳細については、「API プロキシサーバーとしてのNetScaler Console」を参照してください。 |
| 静的ルート | | NetScaler ConsoleとNetScaler VPXインスタンス |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ネットワーク構成 | オプション | 説明 |
| --- | --- | --- |
| | | 間の接続を確立するための静的ルートを設定できます。 |
| NTPサーバー | | NetScaler Consoleのクロックが、ネットワーク上の他のサーバーと同じ日付と時刻設定を持つようにします。詳細については、「NTPサーバーの構成」(/ja-jp/netscaler-application-delivery-management-software/current-release/configure/configure-ntp-server.html)を参照してください。 |
| NetScaler Consoleポート情報 | | NetScaler ConsoleとNetScalerインスタンス間の通信のためにどのポートを開く必要があるかを理解できます。詳細については、「サポートされているポート」(/ja-jp/netscaler-application-delivery-management-software/current-release/system-requirements.html#supported-ports)を参照してください。 |

# システム構成

| システム構成 | オプション | 説明 |
| --- | --- | --- |
| システム、タイムゾーン、許可されたURL、および今日のメッセージ | 基本設定 | `nsrecover`ログインの有効化、セッションタイムアウトの有効化など、システム設定を変更できます。 |
| | タイムゾーン | NetScaler Consoleで使用するタイムゾーンを変更できま |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| システム構成 | オプション | 説明 |
| --- | --- | --- |
| | | す。デフォルトのタイムゾーンはUTCです。 |
| | 許可されたURLリスト | NetScaler Consoleに中断のないリクエストを送信するためのURLを設定できます。追加するURLがない場合は、「none」という値で設定できます。 |
| | 今日のメッセージ | NetScaler Consoleでウェルカムメッセージを作成できます。この機能を使用して、自分自身またはNetScaler Consoleにログオンするユーザーへのリマインダーメッセージを設定できます。**メッセージを有効にする**をクリックし、メッセージボックスにメッセージを入力して、**保存**をクリックします。 |
| NetScaler Consoleのフィンガープリントを表示 | | サービスグラフを開始するために、一意のNetScaler Consoleフィンガープリント IDをコピーできます。 |
| 顧客IDの構成 | | 認証された顧客またはユーザーのみがネットワークにアクセスできるようにすることで、ネットワークリソースを保護できます。詳細については、データガバナンスを参照してください。 |
| CUXIP設定 | | このチェックボックスを選択すると、GUIの改善のみを目的として使用統計が収集されます。受信したデータはCitrixエンジニアのみが使用し、誰とも共有されません。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# システムメンテナンス

| システムメンテナンス | 説明 |
| --- | --- |
| NetScaler Consoleのアップグレード | GUIを介してNetScaler Consoleをアップグレードできます。詳細については、アップグレードを参照してください。 |
| NetScaler Console の再起動 | NetScaler Console を再起動できます。 |
| NetScaler Console のシャットダウン | NetScaler Console をシャットダウンできます。 |
| ディザスタリカバリ | ディザスタリカバリノード情報を表示できます。詳細については、「ディザスタリカバリの構成」を参照してください。 |

# データプルーニング

| データプルーニング | オプション | 説明 |
| --- | --- | --- |
| システムおよびインスタンスデータのプルーニング | システム | NetScaler Console サーバーデータベースに保存されるレポートデータの量を制限できます。詳細については、「システムプルーニング設定の構成」を参照してください。 |
| | インスタンスイベント | NetScaler Console に保存されるイベントメッセージレポートデータを制限できます。 |
| | インスタンス Syslog | データベースに保存されるsyslogデータの量を制限できます。詳細については、「インスタンスsyslogのパージ設定の構成」(/ja-jp/netscaler-application-delivery-management-software/current-release/configure/configure-system-settings-for- |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| データプルーニング | オプション | 説明 |
| --- | --- | --- |
| | | optimal-netscaler-mas-performance.html#configure-instance-syslog-prune-settings)を参照してください。 |
| | ネットワークレポート | NetScaler Consoleに保存されるネットワークレポートデータの量を制限できます |

# バックアップ

| バックアップ | オプション | 説明 |
| --- | --- | --- |
| システムおよびインスタンスのバックアップを構成する | システム | システムバックアップを実行する前に、初期バックアップ設定を構成できます。詳細については、「システムバックアップ設定」(/ja-jp/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-system-backup-settings.html)を参照してください。 |
| | インスタンス | NetScaler Consoleで、選択したNetScalerインスタンスまたは複数のインスタンスをバックアップするための設定を構成できます。詳細については、「インスタンスバックアップ設定の構成」(/ja-jp/netscaler-application-delivery-management-software/current-release/networks/instance-management/backup-restore-netscaler-instances.html#configure- |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| バックアップ | オプション | 説明 |
| --- | --- | --- |
| | | instance-backup-settings)を参照してください。 |

## イベント通知

| イベント通知 | オプション | 説明 |
| --- | --- | --- |
| イベント通知とダイジェストの設定 | イベント通知 | システム関連のいくつかの機能について、選択したユーザーグループに通知を送信できます。これらのシステム機能は、SystemReboot、StatusPoll、SystemStateなどのイベントカテゴリに分類されます。NetScaler Consoleを設定して、電子メール、SMS、またはSlackのいずれかを介して通知を送信できます。これにより、データストレージの超過やバックアップの失敗など、システムレベルのアクティビティが通知されます。 |
| | イベントダイジェスト | 重要なシステムイベントと機能イベントの統合レポートを取得できます |

## SSL設定

| SSL設定 | 説明 |
| --- | --- |
| SSL証明書のインストール | SSL証明書とSSLキーファイルをインストールできます |
| SSL証明書の表示 | SSL証明書の詳細を表示できます |
| SSL設定の構成 | 詳細については、SSL設定の構成を参照してください。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| SSL設定 | 説明 |
| --- | --- |
| SSL証明書 | SSL証明書またはSSLキーファイルのアップロード、ダウンロード、削除を可能にします |
| 暗号グループ | 詳細については、暗号グループの構成を参照してください。 |

## 機能の構成

| 機能の構成 | 説明 |
| --- | --- |
| 機能の無効化または有効化 | NetScaler Consoleで機能を有効または無効にできます。詳細については、NetScaler Console機能の有効化または無効化を参照してください。 |

## システムバックアップ設定を構成する

NetScaler Console をバックアップおよび復元する必要がある前に、初期のシステムバックアップ設定を行います。

1. **設定 > 管理** に移動します。**バックアップ** の下にある **システムとインスタンスのバックアップを構成** をクリックします。
2. **バックアップ > システム** ページで、以下を指定します。
   - 保持する以前のバックアップ。最大10個のバックアップのみを保持できます。
   - バックアップファイルを暗号化するには、**バックアップファイルを暗号化** を選択します。
   - バックアップファイルのコピーを別のシステムに転送するには、**外部転送を有効にする** を選択します。構成を復元する場合は、まずファイルをNetScaler Consoleサーバーにアップロードしてから、復元操作を実行する必要があります。サーバー、ユーザー名とパスワード、ポート、使用する転送プロトコル、およびディレクトリパスを指定します。外部転送の詳細については、「NetScaler Consoleバックアップファイルを外部システムに転送する」を参照してください。
3. **OK** をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

# プロキシサーバー設定の構成

NetScaler Console® を使用すると、アウトバウンド接続用のプロキシサーバーを構成できます。また、SSL インスペクションプロキシがアウトバウンドトラフィックを傍受する NetScaler Console 展開用に、その CA 証明書をアップロードすることもできます。NetScaler Console は、CA 証明書がアップロードされている場合にのみプロキシの証明書を信頼します。この機能により、NetScaler Console からのすべての外部通信が、保護され制御されたプロキシサーバーを介して行われることが保証されます。

この機能には、次の利点があります。

- プロキシが SSL インターセプトを実行する際の通信のセキュリティを確保します。
- テレメトリのアップロードと Cloud Connect 通信における接続の問題を防ぎます。

プロキシサーバーを構成するには、 **>** に移動し、 をクリックします。



## 注意点

- プロキシサーバーが、指定された IP/ポートを介して NetScaler Console から到達可能であることを確認してください。
- SSL インターセプトが有効になっている場合は、接続障害を回避するために、プロキシの CA 証明書を NetScaler Console にインポートしてください。
- プロキシ構成の変更は、新しい詳細が追加されるまで、自動テレメトリのアップロードまたは Cloud Connect に影響を与える可能性があります。

## プロキシサーバーの構成

タブを使用して、プロキシの詳細と資格情報を追加できます。

前提条件

- `adm.cloud.com` を許可リストに追加します。

すべての送信トラフィックをルーティングするためのプロキシサーバーを追加するには、次の手順を実行します。

1. **Settings > Administration** に移動し、**Proxy Server** をクリックします。
2. **Proxy Server Configuration** タブで、**Enable Proxy Server** を選択します。
3. プロキシサーバーの **IP Address/Hostname** とそのリスニング **Port** を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注:**

- 14.1 リリースビルド 56.x 以降、NetScaler Console はプロキシ構成に IP アドレスに加えて DNS ホスト名 (FQDN) の使用をサポートしています。
- ホスト名の使用は、次のような環境で役立ちます。
  - DNS ベースの冗長性 (例: GSLB) を使用して、複数のプロキシサーバー間でトラフィックをルーティングする。
  - ロードバランサーがないが、高可用性とフェイルオーバーを管理するために DNS に依存している。
  - データセンター全体でスケーラブルで回復力のあるプロキシ構成を必要とする。

  DNS ホスト名を使用するサポートにより、NetScaler Console は最適なプロキシエンドポイントを動的に解決し、信頼性を向上させ、管理を簡素化できます。

4. プロキシに資格情報が必要な場合は、**Username** と対応する **Password** を入力します。

**注:**

NetScaler Console は現在、プロキシの基本認証をサポートしています。

5. **Save** をクリックします。

## CA証明書の管理

プロキシサーバーがSSLインスペクションを実行する場合、**CA証明書の管理**タブを使用してプロキシサーバーのCA証明書をアップロードします。必要に応じて、証明書を追加または削除できます。

プロキシサーバーのCA証明書をアップロードするには、次の手順を実行します。

1. **設定 > 管理**に移動し、**プロキシサーバー**をクリックします。
2. **証明書のアップロード**をクリックします。

プロキシサーバーのCA証明書を削除するには、次の手順を実行します。

1. **設定 > 管理**に移動し、**プロキシサーバー**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 削除する証明書を選択します。
3. **証明書の削除**をクリックします。



## プロキシ構成のサポート

NetScaler Consoleは、さまざまなエンタープライズネットワークアーキテクチャに対応するために、次のプロキシ展開モデルをサポートしています。環境とセキュリティ要件に基づいて、次のサポートされているプロキシ構成のいずれかを選択できます。

- プロキシなし
- 明示的なフォワードプロキシ
- 明示的SSLインターセプトプロキシ(#explicit-sslintercepting-proxy)
- 透過的SSLインターセプトプロキシ(#transparent-sslintercepting-proxy)

**重要**

- 明示的SSLインターセプトプロキシおよび透過的SSLインターセプトプロキシの展開では、プロキシCA証明書のアップロードが必須です。プロキシCA証明書がアップロードされていない場合、NetScaler Consoleからのアウトバウンドトラフィックは失敗します。
- 透過的SSLインターセプトプロキシを使用している場合、NetScaler Console on-premでプロキシを構成しないでください。

### プロキシなし (直接インターネットアクセス)

この展開モデルでは、NetScaler Console on-premはプロキシを使用せずにCitrix Cloudに直接接続します。

- 通信はアウトバウンドHTTPSトラフィックのみを使用します。
- NetScaler Console on-premではプロキシ構成は不要です。

### 明示的フォワードプロキシ (非インターセプト)

明示的フォワードプロキシ設定では、NetScaler Console on-premからのアウトバウンドトラフィックはプロキシサーバーを介して明示的にルーティングされます。

- NetScaler Consoleトラフィックは、構成されたフォワードプロキシを介して送信されます。
- プロキシはSSL/TLSを復号化せずにHTTPSトラフィックを転送します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 必須: NetScaler Console on-premでプロキシの詳細を構成する必要があります。
- オプション: 認証はオプションです。ユーザーは、プロキシ構成を提供する際に、認証のためにユーザー名とパスワードを提供できます。基本認証のみがサポートされています。

### 明示的なSSLインターセプトプロキシ

この展開モデルでは、プロキシはSSL/TLS接続を終端して再暗号化することにより、暗号化されたトラフィックを検査します。

- プロキシはSSL復号化と再暗号化を実行します。
- 必須: NetScaler Consoleでプロキシ設定が必要です。
- 必須: プロキシCA証明書をNetScaler Consoleにアップロードする必要があります。詳細については、CA証明書の管理を参照してください。
- オプション: 認証はオプションです。ユーザーは、プロキシ設定を提供する際に、ユーザー名とパスワードを入力して認証できます。基本認証のみがサポートされています。

### 透過的なSSLインターセプトプロキシ

透過型プロキシのセットアップでは、クライアント側で明示的なプロキシ設定なしに、トラフィックはネットワークレベルでインターセプトされます。

- NetScaler Consoleでのプロキシ設定なしに、SSL検査は透過的に行われます。
- ネットワークデバイスはトラフィックをプロキシに自動的にリダイレクトします。
- 必須: SSL検証のために、プロキシCA証明書をNetScaler Consoleにアップロードする必要があります。詳細については、CA証明書の管理を参照してください。
- NetScaler Consoleでプロキシ設定は不要です。

## NTPサーバーを構成する

NetScaler Consoleでネットワークタイムプロトコル (NTP) サーバーを構成して、そのクロックをNTPサーバーと同期させることができます。NTPサーバーを構成すると、NetScaler Consoleのクロックがネットワーク上の他のサーバーと同じ日付と時刻設定を持つことが保証されます。

**NetScaler ConsoleでNTPサーバーを構成するには：**

1. **Settings > NTP Servers**に移動し、**Add**をクリックします。
2. **Create NTP Server**ページで、次の詳細を入力します。
   - **サーバー名/IPアドレス** – NTPサーバーのドメイン名またはIPアドレスを入力します。NTPサーバーを追加した後は、名前またはIPアドレスを変更できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **最小ポーリング間隔** – 送信されるNTPメッセージ間の間隔の最小値を、2の累乗で秒単位で指定します。たとえば、最小ポーリング間隔を64秒（2\^6と表現できる）にする場合は、「6」と入力します。
- **最大ポーリング間隔** – 送信されるNTPメッセージ間の間隔の最大値を、2の累乗で秒単位で指定します。たとえば、最大ポーリング間隔を256秒（2\^8と表現できる）にする場合は、「8」と入力します。
- **キー識別子** - NTPサーバーとの対称鍵認証に使用できるキー識別子を入力します。Autokeyを選択する場合は、キー識別子を追加しないでください。
- **Autokey** - NTPサーバーとの公開鍵認証を使用する場合は、**Autokey**を選択します。キー識別子を追加する場合は選択しないでください。
- **優先** – このNTPサーバーをクロック同期の優先サーバーとして指定する場合は、このオプションを選択します。これは、複数のサーバーが構成されている場合にのみ適用されます。

3. **Create**をクリックします。

   NTPサーバー(/en-us/netscaler-application-delivery-management-software/media/ntp-server.png)

**NetScaler ConsoleでNTP同期を有効にするには：**

1. **Settings > NTP Servers**に移動します。
2. 「**NTP Synchronization**」をクリックし、「**NTP Synchronizationを有効にする**」チェックボックスを選択します。
3. 「**OK**」をクリックします。

   NTPを同期(/en-us/netscaler-application-delivery-management-software/media/ntp1.png)

注

NTPログメッセージは、/var/logディレクトリ内の`/var/log/ntpd.log`ファイルにあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# NetScaler Console のアップグレード

**重要:**

ファイルベースのライセンスは、April 15, 2026をもってEOLとなります。すべてのNetScaler (ADC, SVM) インスタンスは、この日付までにLAS準拠バージョンにアップグレードされ、LASベースのライセンスを使用するように移行する必要があります。 LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1–51.80、13.1-60.29、13.1-37.247 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1–51.83、13.1-60.30

April 15, 2026以降、NetScaler ADCおよびSVMリリース14.1-66.x以降では、NetScalerのアップグレード前にアップグレード関連のチェックがトリガーされます。このチェックは、NetScaler (ADC, SVM) がファイルベースのライセンスをまだ使用しているかどうかを検証し、使用している場合は「NetScaler Upgrade Blocked: File-based licensing in use」というエラーでアップグレードがブロックされます。この予防措置により、NetScalerインスタンスがアップグレードを続行し、April 15, 2026以降にライセンスなしになることを防ぎます。 アップグレードのブロックを解除する方法とそれに伴うリスクを理解するには、CitrixサポートまたはATS担当者にお問い合わせください。

## アップグレード前のチェック

NetScaler Consoleからアップグレードをトリガーする前に、システムは自動的にアップグレード前チェックを実行し、システムの準備状況とアップグレードイメージの整合性を検証します。このチェックにより、アップグレードがスムーズに進行し、アップグレードプロセス中に障害が発生する可能性が低減されます。

**注:**

アップグレード前チェック機能は、NetScaler Console 14.1リリースビルド56.x以降で利用できます。このチェックは、オンプレミスのNetScaler Consoleを通じて開始されるすべてのアップグレードの前に自動的に実行されます。

チェックで問題が検出された場合、NetScaler Consoleは不一致に関する詳細情報を表示し、アップグレードを続行する前にそれらに対処するよう促します。

アップグレード前チェックには、次の検証が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- メモリ可用性チェック – NetScaler Consoleが安全にアップグレードを実行するのに十分な利用可能なRAMがあることを確認します。
- ディスク容量チェック – アップグレードイメージの抽出とインストールに必要な空きディスク容量が利用可能であることを確認します。
- イメージファイル要件チェック – アップグレードに必要なすべての必須イメージファイルが利用可能であることを確認します。
- イメージファイルの整合性チェック – アップグレードイメージのチェックサムを検証し、ファイルが完全で破損していないことを確認します。
- LAS移行チェック - NetScaler Consoleが、April 15, 2026以降もプール型またはフレックス型ライセンスタイプに対してファイルベースのライセンスを使用しているかどうかを確認します。

  **注:**

  LAS移行チェックはApril 15, 2026に有効になり、プール型およびフレックス型ライセンスタイプに適用されます。この日付以降、ファイルベースのライセンスがまだ使用されている状態でNetScaler Console 14.1-66.x以降にアップグレードしようとすると、アップグレードは許可されません。このチェックは、April 15, 2026以降にオンプレミスのNetScaler Consoleがアップグレードを進めること、およびアップグレード後にNetScalerインスタンスがライセンスなしの状態になることを避けるために行われます。この制限に遭遇した場合は、CitrixサポートまたはATS担当者に連絡してガイダンスを求める必要があります。

  LASアップグレード前チェックが失敗した場合、次のエラーが表示されます。



リソースとファイルの検証に加えて、NetScaler Consoleはシステムの健全性と接続性を検証し、安全なアップグレードを保証します。検証には次のチェックが含まれます。

- データベース整合性チェック – 不足または破損したデータベースファイルを検出し、アップグレードの失敗を防ぎます。
- データベースストリーミングチャネルステータス – ストリーミングチャネルがアクティブで動作していることを確認します。
- セカンダリノード接続 – 冗長性のためにセカンダリノードとの適切な通信を確保します。
- パスワードなしSSH検証 – セカンダリノードへのパスワードなしSSHログインが機能していることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレード前チェック機能は次の利点を提供します。

- アップグレード前にこれらの検証を実行することで、リソース不足または破損したイメージファイルによって引き起こされる失敗を防ぐのに役立ちます。
- 潜在的な問題を事前に特定することで、アップグレード前チェックはアップグレードの信頼性を向上させ、回復または再インストールの作業によるダウンタイムを最小限に抑えます。

**NetScaler Consoleをアップグレードするには：**

1. 「**設定 > 管理**」に移動します。「**システムメンテナンス**」の下にある「**NetScaler Consoleのアップグレード**」をクリックします。
2. 「NetScaler Consoleのアップグレード」ページで、「**ローカル**」（お使いのローカルコンピューター）または「**アプライアンス**」のいずれかを選択して、新しいイメージファイルをアップロードします。

   「

   **注**

   」

   「**アプライアンス**」を選択した場合、NetScaler Consoleの`/var/mps/mps_images`にアップグレードイメージがあることを確認してください。

   デフォルトでは、アップグレードが正常に完了した後、ソフトウェアイメージはクリーンアップされます。
3. 「**OK**」をクリックします。

   「コンソールのアップグレード」(/en-us/netscaler-application-delivery-management-software/media/mas-upgrade-new.png)

### LASのアップグレード前チェックが失敗した場合のNetScaler Consoleアップグレードのブロック解除

このオプションは、NetScaler Consoleのアップグレードを直ちに続行する必要があり、以下に説明するライセンスへの影響を理解し、受け入れる場合にのみ使用してください。アップグレード後もライセンスを維持することが目標である場合は、CitrixサポートまたはATS担当者にお問い合わせください。

「**前提条件:**」NetScaler ConsoleまたはVMへのシェルアクセスと、`/var/tmp`の下にファイルを作成する十分な権限が必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレードのブロックを解除するには:

1. NetScaler Consoleシェルにログインします。
2. バイパスフラグファイルを作成します。

   ```
   touch /var/tmp/skip_las_checks
   ```

3. アップグレードを再実行します。NetScaler Consoleは`skip_las_checks`フラグを検出し、LAS検証をスキップして、アップグレードワークフローの続行を許可します。

**重要:**

ファイルベースのプール型またはフレックス型ライセンスがまだ使用されている状態でLASアップグレード前チェックをバイパスして続行すると、NetScaler Consoleのアップグレード後、管理対象のすべてのNetScalerインスタンスはライセンスなしの状態になると予想されます。

NetScaler Consoleオンプレミスアップグレード後、プール型またはフレックス型ライセンスのLAS移行を完了し、各NetScalerインスタンスが正しくライセンスされていることを確認します。

代替アプローチまたは移行シーケンスに関する支援が必要な場合は、CitrixサポートまたはATS担当者にお問い合わせください。

# NetScaler Console のパスワードをリセットする方法

NetScaler Console のパスワードをリセットする手順は、ホストされているハイパーバイザーによって異なる場合があります。デフォルトのパスワードを変更し、デフォルトのパスワードにリセットしたい場合は、NetScaler Console ノードを再起動することでパスワードをリセットできます。

**XenCenter を使用した Citrix Hypervisor™**:

1. XenCenter を使用して Citrix Hypervisor にログオンします。
2. NetScaler Console ノードを選択し、右クリックして **Reboot** を選択します。
3. **Console** タブで、**CTL + C** を押して起動シーケンスを中断します。

   

4. OK プロンプトで **boot -s** コマンドを実行します。

   

   NetScaler Console が再起動し、次のメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **Enter** を押して /u@ プロンプトを表示します。

6. 次のコマンドを使用してフラッシュパーティションをマウントします。

   ```
   mount /dev/ada0s1a /flash
   ```

7. 次のコマンドを使用してファイルを作成します。

   ```
   touch /flash/mpsconfig/.recover
   ```

   パスワードがデフォルトのパスワードにリセットされました。

8. **Reboot** コマンドを実行して NetScaler Console を再起動します。

9. NetScaler Console GUI にアクセスし、再起動が完了するまで待ちます。

   これで、GUI からログオンするには *nsroot/nsroot* 資格情報を使用し、ハイパーバイザーからログオンするには *nsrecover/nsroot* を使用できます。

   注

   再起動後、パスワードがデフォルトのパスワードにリセットされていない場合は、同じ手順（ステップ1からステップ7）を繰り返します。その後、次のコマンドを実行して NetScaler Console を再起動します。

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

**vSphere を使用した Esx**:

1. vSphere を使用して ESX にログオンします。
2. NetScaler Consoleノードを選択し、右クリックして、**Reboot**を選択します。
3. **Console**タブで、**CTL + C**を押して起動シーケンスを中断します。

4. OKプロンプトで**boot -s**コマンドを実行します。

   NetScaler Consoleが再起動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **Enter**を押して/u@プロンプトを表示します。
6. 次のコマンドを使用してフラッシュパーティションをマウントします。

   ```
   mount dev/da0s1a /flash
   ```

7. 次のコマンドを使用してファイルを作成します。

   ```
   touch /flash/mpsconfig/.recover
   ```

   パスワードがデフォルトのパスワードにリセットされました。
8. **Reboot**コマンドを実行してNetScaler Consoleを再起動します。
9. NetScaler Console GUIにアクセスし、再起動が完了するまで待ちます。

   これで、GUIからログオンするには*nsroot/nsroot*資格情報を使用し、ESXサーバーからログオンするには*nsrecover/nsroot*を使用できます。

   注

   再起動後、パスワードがデフォルトパスワードにリセットされていない場合は、同じ手順（ステップ1からステップ7）を繰り返します。その後、次のコマンドを実行してNetScaler Consoleを再起動します。

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

**Hyper-v マネージャーを使用した Hyper-v**:

1. Hyper-v マネージャーを使用して Hyper-v にログオンします。
2. NetScaler Consoleノードを選択し、右クリックして、**再起動**を選択します。
3. **コンソール**タブで、**CTL + C**を押して起動シーケンスを中断します。
4. OKプロンプトで**boot -s**コマンドを実行します。

   NetScaler Consoleが再起動します。
5. **Enter**キーを押して/u@プロンプトを表示します。
6. 次のコマンドを使用してフラッシュパーティションをマウントします。

   ```
   mount dev/ad0s1a /flash
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 次のコマンドを使用してファイルを作成します。

   ```
   touch /flash/mpsconfig/.recover
   ```

   パスワードがデフォルトパスワードにリセットされました。
8. **Reboot**コマンドを実行して、NetScaler Consoleを再起動します。
9. NetScaler Console GUIにアクセスし、再起動が完了するまで待ちます。

   これで、GUIからログオンするには*nsroot/nsroot*の資格情報を使用し、Hyper-Vマネージャーからログオンするには*nsrecover/nsroot*を使用できます。

   注

   再起動後、パスワードがデフォルトパスワードにリセットされていない場合は、同じ手順（ステップ1からステップ7）を繰り返します。その後、以下のコマンドを実行してNetScaler Consoleを再起動します。

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

**Linux KVMサーバー（任意のSSHクライアントを使用してKVMサーバーにSSH接続）**：

1. SSHクライアントを使用してKVMサーバーからNetScaler Consoleにログオンします。
2. NetScaler Consoleを再起動します。
3. **Loading /boot/defaults/loader.conf**メッセージが表示された直後に、**CTL + C**を押して起動シーケンスを中断します。
4. OKプロンプトで、次のコマンドを実行します。

   ```
   set console='comconsole,vidconsole'
   ```
5. 「**boot -s**」コマンドを実行して、NetScaler Consoleを再起動します。
6. 「**シェルへのフルパスを入力するか、/bin/shの場合はRETURNを押してください:**」というメッセージが表示された後、**Enter**キーを押して/u@プロンプトを取得します。
7. 次のコマンドを使用してフラッシュパーティションをマウントします。

   ```
   mount dev/vtbd0s1a /flash
   ```
8. 次のコマンドを使用してファイルを作成します。

   ```
   touch /flash/mpsconfig/.recover
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パスワードがデフォルトのパスワードにリセットされました。

9. 「**Reboot**」コマンドを実行して、NetScaler Consoleを再起動します。
10. NetScaler Console GUIにアクセスし、再起動が完了するまで待ちます。

これで、*nsroot/nsroot*資格情報を使用してGUIからログオンし、*nsrecover/nsroot*を使用してSSHコンソールからログオンできます。

注

再起動後、パスワードがデフォルトのパスワードにリセットされていない場合は、同じ手順（ステップ1〜7）を繰り返します。その後、次のコマンドを実行し、NetScaler Consoleを再起動します。

- `rm /flash/mpsconfig/master.passwd`
- `rm –rf /etc/passwd`

# NetScaler Consoleにアクセスするためのセカンダリ NICを構成する

NetScaler Consoleへの管理アクセスを分離するために、セカンダリNICを構成できます。このセカンダリNIC機能を使用すると、要件に応じて、NetScaler Consoleを介して送受信されるトラフィックをどのように分離するかを選択できます。

トラフィックを分離したいシナリオを考えてみましょう。

- NetScaler Consoleとその管理対象NetScalerインスタンス間のすべての通信を1つのネットワークに配置する。
- NetScaler Consoleへの管理アクセスを別のネットワークに配置する。

このシナリオでは、管理者として、次のことができます。

- NetScaler Consoleとその管理対象NetScalerインスタンス間のトラフィック用に1つのIPアドレスを構成する。
- NetScaler Consoleソフトウェアを管理し、ソフトウェア内のすべての管理タスクを実行するために、別のIPアドレスを構成する。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

NetScaler ConsoleがHAペアとして構成されている場合、セカンダリNICに構成された管理IPアドレスはプライマリノードに関連付けられます。

## 前提条件

- ハイパーバイザー (Citrix Hypervisor、Microsoft Hyper-V、Linux KVM、またはVMware ESXi) に **NetScaler Console 13.0 Build 47.x 以降** が展開および構成されていることを確認してください。
- ハイパーバイザー (Citrix Hypervisor™、Microsoft Hyper-V、Linux KVM、またはVMware ESXi) にセカンダリNICが追加されていることを確認してください。

Citrix HypervisorでNICにIPアドレスを割り当て、セカンダリインターフェイスを作成するには、「NICにIPアドレスを割り当てる」を参照してください。

## NetScaler Consoleでセカンダリ NICを構成する

1. NetScaler Console GUIにログオンします。
2. **Settings > Administration** に移動します。
3. **Network Configuration** の下にある **IP Address, Second NIC, Host Name and Proxy Server** をクリックします。

   NIC構成(/en-us/netscaler-application-delivery-management-software/media/nic-configuration.png)

   **Network Configuration** ページが表示されます。
4. Second NIC タブをクリックし、次のパラメータを設定します。

   a. **Application Delivery Management IP Address** – NetScaler Consoleにアクセスするための有効なIPアドレスを入力します。既存の管理IPアドレスとは別に、このIPアドレスを使用してNetScaler Consoleにアクセスできます。

   b. **Netmask** – ネットワークホストを指定するためのネットマスクアドレスを入力します。デフォルトアドレスは255.255.255.0です。

   c. **Network Address** – NetScaler Consoleのルートエントリを追加するためのIPアドレスを入力します。**+** をクリックしてIPアドレスを追加します。このフィールドはオプションです。

   d. **Save** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NICの構成(/en-us/netscaler-application-delivery-management-software/media/configure-nic.png)

# NetScaler® エージェントにアクセスするためのセカンダリNIC の構成

エージェントに2つのNICを構成できます。デュアルNICアーキテクチャを使用すると、エージェントは次のことができるようになります。

- エージェントとNetScalerインスタンス間の通信を確立する - 最初のNICを使用して、NetScaler Consoleを介して送受信されるトラフィックを分離し、NetScaler Consoleと別のネットワークにある管理対象NetScalerインスタンス間の通信を行うことができます。
- エージェントとNetScaler Console間の通信を確立する - 2番目のNICを使用して、ネットワーク上にあるNetScaler Consoleを管理し、管理タスクを実行できます。

**注**

両方のNICの機能と構成を入れ替えることはできません。

デュアルNICインフラストラクチャのブロック図(/en-us/netscaler-application-delivery-management-software/media/dual_nic_support_agent-console.png)

このシナリオでは、管理者として次のことができます。

- NetScaler Consoleとその管理対象NetScalerインスタンス間のトラフィックのIPアドレスを構成します。
- ソフトウェア内のすべての管理タスクを実行するために、NetScaler Consoleソフトウェアを管理するためのIPアドレスを構成します。

**注**

エージェントにデュアルNICを構成することは必須ではありません。これはオプションであり、エージェント、NetScaler Console、およびNetScalerインスタンス間のトラフィックを分離する必要がある場合にのみ必要です。

## CLIを使用してIPV4 NICネットワークアドレスを変更する

1. PuTTYなどのSSHクライアントを使用して、NetScalerエージェントコンソールへのSSH接続を開きます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **nsrecover/nsroot** 資格情報を使用してログインし、シェルプロンプトに切り替えます。
3. 「**ifconfig**」コマンドを実行します。設定した2つのNICの詳細が表示されます。

   - NIC 1 – エージェントとNetScaler間の通信用
   - NIC 2 – エージェントとNetScaler Console間の通信用

   コードブロック ifconfig(/en-us/netscaler-application-delivery-management-software/media/code_block_ifconfig.png)
4. 「**networkconfig**」コマンドを実行します。IPv4ネットワークアドレスを設定または変更できるメニューが表示されます。

   コードブロック networkconfig(/en-us/netscaler-application-delivery-management-software/media/code_block_networkconfig.png)

   **注**

   2番目のNICのネットワークアドレスは、複数のIP値を持つことができます。
5. 変更するメニュー項目を選択します。設定を保存して終了します。

## Syslogパージ間隔の設定

Syslogは、ログ記録のための標準プロトコルです。これには2つのコンポーネントがあります。Citrix NetScalerインスタンスで実行されるSyslog監査モジュールと、NetScalerインスタンスの基盤となるFreeBSDオペレーティングシステム（OS）上またはリモートシステム上で実行できるSyslogサーバーです。SYSLOGは、データ転送にUser Datagram Protocol (UDP)を使用します。

Syslogを使用すると、情報を生成するシステムと情報を保存するシステムを分離できます。ログ情報を統合し、収集されたデータから洞察を得ることができます。また、さまざまな種類のイベントをログに記録するようにSyslogを設定することもできます。

データベースに保存されるSyslogデータの量を制限するには、Syslogデータをパージする間隔を指定できます。NetScaler Consoleから以下のSyslogデータが削除されるまでの日数を指定できます。

- 一般Syslogデータ
- AppFirewallデータ
- NetScaler Gatewayデータ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SyslogタイプごとにNetScaler Gatewayのパージ間隔を設定することもできます。このパージ間隔は、NetScaler Gatewayデータを保持するために設定されたパージ間隔よりも優先されます。

**NetScaler ConsoleのSyslogパージ間隔設定を構成するには：**

1. **Settings > Data Storage > Data Retention Policy**の順に移動します。**データパージ**のページが表示されます。**Instance Syslog**をクリックします。
2. **Configure Instance Syslog Prune Settings**ページで、**Retain Syslog Generic Data(days)**を指定します。NetScaler Consoleが一般的なSyslogメッセージを保持する日数を入力します。

# システムのパージ設定とイベントのパージ設定を構成する

NetScaler Consoleソフトウェアデータベースに保存されるレポートデータの量を制限するために、データをパージできます。NetScaler Consoleがネットワークレポートデータ、イベント、監査ログ、タスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと（00:00）にパージされます。

**注**

指定する値は、30日を超えることも、15日未満にすることもできません。

**パフォーマンスレポートのシステムのパージ設定を構成するには：**

1. **設定** > **管理** に移動します。**データパージ** の下にある **システムおよびインスタンスデータのパージ** をクリックします。
2. **システムのパージ設定の構成** ページで、以下を指定します。
   - データを保持する日数
   - ディスク領域の割合（パージしきい値）
3. **OK** をクリックします。

   システムのパージ設定を構成する(/en-us/netscaler-application-delivery-management-software/media/configure-sys-prune-settings.png)

**自動データパージを有効にする** チェックボックスをオンにすると、自動パージを有効にできます。ディスク使用量が構成済みの **データパージしきい値** を超えると、アラームがトリガーされ、メールが送信されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

以下のいずれかの条件が満たされると、パージが開始されます。データパージしきい値、または保持するデータ（日数）です。最初に満たされた条件が、もう一方よりも優先されます。

**アラーム設定を構成して有効にするには：**

1. 「**Settings** > **SNMP**」に移動します。右上の「**Alarms**」をクリックします。
2. 設定するアラーム（例: diskUtilizationHigh）を選択し、「**Edit**」をクリックします。
3. 「**Configure Alarm**」ページで、以下を指定します。

- **Severity**—重大度レベルを選択します。
- **Alarm Threshold**—イベントの重大度が計算される値を入力します。
- **Time**—アラームをトリガーするまでの時間（分）を入力します。



## NetScaler Console を使用してイベントのパージ設定を構成する

NetScaler Console データベースに保存されるイベントメッセージデータの量を制限するために、NetScaler Console がネットワークレポートデータ、イベント、監査ログ、タスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと（00:00時）にパージされます。

1. 「**Settings > Administration > Data Pruning**」に移動し、「**System and Instance Data Pruning**」をクリックします。「**Instance Events**」をクリックします。
2. NetScaler Console サーバーにデータを保持する期間を日数で入力し、「**Save**」をクリックします。

# 非デフォルトユーザーのシェルアクセスを有効にする

NetScaler Consoleで非デフォルトユーザーのシェルアクセスを有効にできます。この機能を使用して、インスタンスとの通信モードを有効にし、設定できます。

**注**

デフォルトでは、非デフォルトユーザーのシェルアクセスは無効になっています。

**NetScaler Consoleで非デフォルトユーザーのシェルアクセスを有効にするには：**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**Settings > Administration**に移動します。
2. 「**システム構成**」で、「**システム、タイムゾーン、許可されたURL、およびエージェント設定**」をクリックします。
3. **System Configurations**ページで、次のパラメータを設定します。
   - **Communication with instances** - 通信プロトコルを選択します。
   - **Secure Access** - NetScaler Consoleのセキュアアクセスを有効にします。
   - **Enable Session Timeout** - 非アクティブなセッションを保持する期間を指定します。
   - **Allow Basic Authentication** - 管理サービスが基本認証プロトコルを使用して提供された資格情報を受け入れることを許可します。
   - **Enable nsrecover Login** - 管理サービスでの`nsrecover`ログインを有効にします。
   - **Enable Certificate Download** - 追加されたNetScalerから証明書をダウンロードできるようにします。
   - **Enable Shell access for non-nsroot User** - NetScaler Consoleで非デフォルトユーザーのシェルアクセスを有効にします。
   - **インスタンスログインのユーザー資格情報を要求** - NetScaler Consoleからインスタンスにログインする際に、ユーザーがユーザー資格情報を入力できるようにします。
     - **StyleBook操作の資格情報を要求** - NetScalerインスタンスでStyleBookおよびconfig pack操作を使用する際に、ユーザーがユーザー資格情報を入力できるようにします。

   **注：**

   **インスタンスログインの資格情報を要求**が選択され、**StyleBook操作の資格情報を要求**がクリアされている場合、ユーザーはNetScalerインスタンスでのStyleBookおよびconfig pack操作のために資格情報の入力を求められません。
4. **OK**をクリックします。

# アクセスできないNetScaler Consoleサーバーを回復する

NetScaler Consoleは、システムデータベースのクリーンアップを実行するためのデータベースメンテナンスツールを提供するようになりました。ファイルシステムに接続し、いくつかのコンポーネントを削除してデータベースにアクセスできるようにするために、NetScaler Consoleユーティリティツールを起動できるようになりました。NetScaler Consoleリカバリスクリプトは、古くなったデータベーステーブルや未使用のデータベーステーブルおよびファイルをクリアすること

© 1997–2026 Citrix Systems, Inc. All rights reserved.

で、ファイルシステムの領域を回復するのに役立つツールです。このツールは、連続した手順でデータベーステーブルとファイルをナビゲートするのに役立ち、それぞれの項目がファイルシステム上で占める現在の領域を表示します。削除するデータベーステーブルとファイルを選択すると、ツールは確認後にそれらをファイルシステムから削除します。

## NetScaler Consoleスタンドアロン展開でNetScaler Consoleデータベースリカバリスクリプトを使用する方法

シングルサーバーのNetScaler Console展開で次の手順を使用して、ファイルシステムに接続し、いくつかのコンポーネントを削除してデータベースにアクセスできるようにし、リカバリ操作を実行します。

1. SSHクライアントまたはハイパーバイザーのコンソールを使用して、NetScaler Consoleにログオンし、次のコマンドを入力します。

   

2. 画面にいくつかのNetScaler Consoleプロセスを停止するための警告メッセージが表示されたら、「y」と入力し、**Enter**キーを押します。

   システムが、システムのコアファイルに影響を与えることなく削除できるデータベースのコンポーネントを判別している間、次の画面が表示されます。

   

3. 画面にデータベース内のファイルリストが表示されます。「y」と入力し、Enterキーを押してクリーンアッププロセスを開始します。

   

4. クリーンアップが必要な特定のデータベースコンポーネントを選択し、対応する番号を入力できます。**Enter**キーを押します。

   例えば、システムカタログのクリーンアップを実行するには、**DBコンポーネント**選択メニューでオプション8を選択し、「y」と入力し、**Enter**キーを押してシステムカタログのクリーンアップを続行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

NetScaler Consoleには、システムカタログとして知られるユーザーテーブルが含まれています。システムカタログは、リレーショナルデータベース管理システムがテーブルや列に関する情報、内部レコードなどのスキーマメタデータを保存するNetScaler Consoleデータベース内の場所です。システムカタログ内のテーブルは、時間の経過とともに肥大化したり、不要な行が蓄積したりする通常のテーブルと同様であり、最適なパフォーマンスのために定期的なクリーンアップが必要です。これらのテーブルを定期的にメンテナンスすることは良い習慣です。この活動は、ディスク領域を解放するだけでなく、データベース全体のパフォーマンス、ひいてはNetScaler Consoleのパフォーマンスも向上させます。

クリーンアップユーティリティには、データベースコンポーネントとファイルコンポーネントをクリーンアップするオプションがあります。「1」から「9」の間の数字を入力してファイルコンポーネントを選択するか、「11」と入力してEnterキーを押し、データベースコンポーネントをクリーンアップできます。

**注**

「11」は、クリーンアップするファイルコンポーネントを選択せず、以前に選択したデータベースコンポーネントのクリーンアップに進むことを示します。この例では、「システムカタログ」です。

5. 最終確認画面で「y」と入力し、もう一度**Enter**キーを押します。

   システムカタログがクリーンアップされます。これには、システムカタログ内のテーブルのサイズに応じて時間がかかる場合があります。プロセスが完了すると、概要画面が表示されます。

6. 「y」と入力し、**Enter**キーを押してNetScaler Consoleを再起動します。

   システムクリーンアップ後、NetScaler Consoleを再起動してください。NetScaler Consoleの再起動後、内部データベース操作が完了するまで約30分間待ちます。その後、NetScaler Consoleデータベースに接続できるはずです。接続できない場合は、リカバリスクリプトを再

© 1997–2026 Citrix Systems, Inc. All rights reserved.

度実行して、さらにスペースを解放してください。NetScaler Consoleが稼働していれば、期待どおりに動作するはずです。

**注**

クリーンアップ後も、システムカタログテーブルの現在のサイズが「Zero」になることはありません。これは、空の行のみがテーブルから削除され、クリーンアップ後もテーブルに有効なエントリが残っている可能性があるためです。

### NetScaler Console高可用性展開でNetScaler Consoleデータベースリカバリスクリプトを使用する方法

高可用性展開におけるNetScaler Consoleサーバーのデータベースシステムは、継続的な同期モードにあります。新しいデータベースリカバリツールを使用する場合、両方のNetScaler Consoleサーバーで手順を繰り返す必要はありません。

1. SSHクライアントまたはハイパーバイザーのコンソールを使用して、プライマリノードにログオンします。
2. 次のコマンドを実行します。

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. NetScaler Consoleスタンドアロン展開リカバリスクリプトに記載されている手順2から、その手順に従ってください。

## NetScaler Consoleサーバーにホスト名を割り当てる

NetScaler Consoleサーバーを識別するために、サーバーにホスト名を割り当てることができます。

**NetScaler Consoleサーバーにホスト名を割り当てるには：**

1. NetScaler Consoleで、**設定 > 管理**に移動します。
2. **ネットワーク構成**で、**IPアドレス、セカンドNIC、ホスト名、およびプロキシサーバー**をクリックします。
3. **ホスト名**を選択し、ホスト名とハイパーバイザーホスト名を入力して、**保存**をクリックします。

   ホスト名の割り当て(/en-us/netscaler-application-delivery-management-software/media/hostname.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注：**

ハイパーバイザーで`networkconfig`コマンドを使用してホスト名を変更することもできます。

# NetScaler Consoleサーバーをバックアップおよび復元する

NetScaler Consoleサーバーの定期的なバックアップを作成できます。構成ファイル、インスタンスの詳細、システムデータなどをバックアップおよび復元できます。

**重要**

Citrixでは、同じバージョンのバックアップを使用してNetScaler Consoleサーバーを復元することをお勧めします。たとえば、NetScaler Consoleのバージョンが13.0の場合、13.0のNetScaler Consoleバックアップを使用してサーバーを復元します。

NetScaler Consoleサーバーのバックアップと復元に対するユーザーアクセスは制限されています。**設定 > バックアップファイル**ページは、すべてのNetScaler Console機能にアクセスできるユーザーにのみ表示されます。ユーザーは、アクセスポリシーにすべての権限がある場合にのみ、このページにアクセスできます。通常、スーパーユーザーはすべてのNetScaler Console機能にアクセスできます。

詳細については、「アクセスポリシーの構成」を参照してください。
アップグレードする前に、予防措置としてNetScaler Consoleサーバーの構成ファイルをバックアップしてください。

バックアップには、次のコンポーネントが含まれます。

- NetScaler Console構成ファイル:
  - SNMP
  - Syslogサーバー構成ファイル
  - NTPファイル
  - SSL証明書
  - Control Centerファイル
- NetScaler Consoleサーバーが管理するNetScalerインスタンスのバックアップ。
- 構成監査テンプレート。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- データベースに保存されているシステムデータ:
  - 作成されたテナントとユーザーのリスト。
  - 外部認証サーバーの構成 (LDAP、RADIUS、その他)。
  - 作成された構成ジョブとジョブテンプレート。
- データベースに保存されているインフラストラクチャおよびアプリケーションデータ:
  - 追加および管理されたNetScalerインスタンスからのデータ。
  - インスタンスプロファイルの詳細、バージョン詳細、インスタンスグループ詳細など。
  - 管理者が作成した静的アプリケーション (仮想サーバーのグループ)。
- SNMP設定。

**注**

分析データ、イベント、NetScaler Consoleライセンス、およびsyslogメッセージはバックアップから除外されます。

## NetScaler Consoleの構成をバックアップする

デフォルトでは、NetScaler Consoleサーバーは24時間ごと (00:30) に構成をバックアップします。バックアップの時間をスケジュールして選択することもできます。さらに、バックアップされたファイルのコピーを別のシステムに移動することもできます。

バックアップは、暗号化も可能な圧縮TARファイルとして保存されます。デフォルトでは、3つのバックアップファイルがサーバーに保持されます。ディスク容量不足の問題を避けるため、NetScaler Consoleサーバーには最大10個のバックアップファイルを保存できます。ただし、予防措置として、バックアップファイルの一部をサーバーに保存するか、(#transfer-a-citrix-adm-backup-file-to-an-external-system)ことをお勧めします。

**NetScaler Consoleの構成をバックアップするには：**

1. **Settings > Backup Files** に移動し、**Back Up** をクリックします。
2. バックアップファイルを暗号化するには、**Password Protect file** チェックボックスをオンにし、ファイルを暗号化するためのパスワードを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler Consoleのバックアップファイルを外部システムに転送する

予防措置として、バックアップファイルのコピーを別のシステムに転送できます。構成を復元したい場合は、まずファイルをNetScaler Consoleサーバーにアップロードし、その後(#restore-the-citrix-adm-configuration-from-a-backup-file)を実行します。

**NetScaler Consoleのバックアップファイルを転送するには：**

1. **Settings > Backup Files** に移動します。
2. 別のシステムに移動したいバックアップファイルを選択し、**Transfer** をクリックします。
3. **Backup Files** ページで、次のパラメーターを指定します。
   - **Server** - バックアップファイルを転送するシステムのIPアドレス。
   - **User Name and Password** - バックアップファイルがコピーされる新しいシステムのユーザー認証情報。
   - **Port** - ファイルが転送されるシステムのポート番号。
   - **Transfer Protocol** - バックアップファイルの転送に使用されるプロトコル。バックアップファイルを転送するには、SCP、SFTP、またはFTPプロトコルを選択できます。
   - **ディレクトリパス** - 新しいシステムにバックアップファイルが転送される場所。
4. 転送後、**転送後にApplication Delivery Managementからファイルを削除**チェックボックスを選択すると、NetScaler Consoleからバックアップファイルを削除できます。
5. 転送を実行するには、**OK**をクリックします。

> **注**
>
> バックアップファイルのコピーをローカルシステムに保存するには、**設定 > バックアップファイル**に移動し、コピーするファイルを選択し、**ダウンロード**をクリックします。

## バックアップファイルからNetScaler Consoleの構成を復元する

以前にバックアップされたファイルからNetScaler Consoleの構成を復元すると、復元操作はバックアップファイルを解凍し、構成を復元します。復元操作は既存の構成を削除し、バックアップファイル内の構成に置き換えます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

- バックアップファイルの名前が変更されたり、バックアップファイルの内容が変更されたりすると、復元操作は失敗します。
- NetScaler Consoleで復元を開始する前に、ライセンスファイルを`/mpsconfig/license/`ディレクトリにコピーします。ターゲットデバイスのホストIDは、コピーされたライセンスファイルに存在するホストIDと一致する必要があります。

**バックアップファイルからNetScaler Consoleの構成を復元するには：**

1. **設定 > バックアップファイル**に移動します。
2. 復元するバックアップファイルを選択し、**復元**をクリックします。



3. 確認ダイアログボックスで、「**はい**」をクリックします。

**注**

外部システムに保存されているバックアップファイルから構成を復元するには、復元操作を実行する前に、バックアップファイルをNetScaler Consoleサーバーにアップロードします。ファイルをアップロードするには、**Settings > Backup Files**に移動し、「**Upload**」をクリックします。

# 高可用性展開におけるNetScaler ConsoleのVMスナップショット

アップグレードを開始する前に、HA展開のNetScaler Consoleサーバーのスナップショットを取得できます。スナップショットは、取得した時点の仮想マシン全体の状態をキャプチャします。

## NetScaler Consoleサーバーのスナップショットを取得する

NetScaler Consoleサーバーのスナップショットを取得するには、次の順序を使用します。

1. NetScaler Consoleセカンダリサーバー
2. NetScaler Consoleプライマリサーバー

**NetScaler Consoleサーバーのスナップショットを取得するには:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ハイパーバイザーで、仮想マシンの一覧からNetScaler Consoleセカンダリサーバーを選択します。
2. VMスナップショットを取得します。

   **注:**

   スナップショットの取得中に、**VMメモリの取得**を選択することをお勧めします。

3. スナップショットにわかりやすい名前を付け、必要に応じて説明を入力します。

   スナップショットはデフォルトのVMディレクトリに保存されます。
4. プライマリサーバーに対しても同じ手順を繰り返します。

**注:**

スナップショットの取得中にVMの電源をオフにする必要はありません。

### NetScaler Consoleサーバーのスナップショットを復元する

スナップショットを復元すると、仮想マシンのメモリ、設定、および仮想マシンディスクの状態が、スナップショットを取得した時点の状態に戻ります。

NetScaler Consoleサーバーのスナップショットを復元するには、次の順序を使用します。

1. NetScaler Consoleプライマリサーバー
2. NetScaler Consoleセカンダリサーバー

**NetScaler Consoleサーバーのスナップショットを復元するには：**

1. ハイパーバイザーで、仮想マシンのリストからNetScaler Consoleプライマリサーバーを選択します。
2. VMを右クリックし、スナップショットを元に戻します。

   仮想マシンは最新のスナップショットの状態に戻ります。
3. NetScaler Consoleセカンダリサーバーについても、同じ手順を繰り返します。

## 監査情報の表示

監査ログには、ユーザーの詳細、操作、実行されたアクションなど、特定の期間の情報が記録されています。以下のシナリオ例のsyslogメッセージを表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler® Console が HA ペアであり、プライマリノードとセカンダリノード間のデータベースレプリケーションに遅延の問題がある場合、その詳細をイベントとして表示できます。
- 無効なログイン試行（ユーザー名またはパスワードのエラー）や正常なログインがあった場合、その詳細をイベントとして表示できます。

管理者は、これらのログをセキュリティの維持や失われたトランザクションの回復に利用できます。

**NetScaler Console で syslog サーバーを構成するには:**

1. **設定 > 監査ログメッセージ > Syslogサーバー** に移動します。
2. **Syslog Server** ページで、**Add** をクリックします。
3. **Create Syslog Server** ページで、次の値を入力します。
    - **Name** - syslog サーバーの名前。
    - **IP Address** - syslog サーバーの IP アドレス。
    - **Port** - syslog サーバーのポート。
4. ログレベル（すべて、なし、またはカスタム）を選択します。
5. **Create** をクリックします。

**NetScaler Console で syslog の日付と時刻の形式を構成するには:**

1. 「**設定 > 監査ログメッセージ > Syslogサーバー**」に移動します。
2. **Syslogサーバー**ページで、Syslogサーバーを選択し、**Syslogパラメータ**をクリックします。
3. **Syslogパラメータの構成**ページで、日付と時刻の形式を指定します。
4. **OK**をクリックします。

**NetScaler ConsoleでSyslogメッセージを表示するには：**

「**設定 > 監査ログメッセージ**」に移動します。

以下のフィルターからフィルターを適用して、システムログメッセージを表示することもできます。

- イベント
- メッセージ
- モジュール
- 重大度

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ソース

詳細については、Syslogメッセージリファレンスを参照してください。

## SSL設定を構成する

SSL (Secure Socket Layer) と TLS (Transport Layer Security) は、ユーザーとサーバー間の暗号化された通信を提供する、一般的に使用されるセキュリティネットワークプロトコルです。NetScaler Console で SSL 設定を構成し、システムに接続するクライアントの種類を指定できます。

**NetScaler Console の SSL 設定を構成するには:**

1. **Settings > Administration** に移動します。**SSL Settings** の下にある **Configure SSL Settings** をクリックします。
2. **SSL Settings** ページで、現在のプロトコル設定とシステムに適用されている暗号スイートを確認します。
3. プロトコル設定を変更するには、**Edit Settings** の下にある **Protocol Settings** の **+** アイコンをクリックし、必要な変更を行います。
4. 適用されている暗号スイートを変更するには、**Edit Settings** の下にある **Cipher Suites** の **+** アイコンをクリックし、必要な変更を行います。
5. **OK** をクリックし、次に **Close** をクリックします。

## CPU、メモリ、ディスク使用量を監視する

ログと統計に保持されている情報を使用できます。この情報は、NetScaler Console の構成と保守に役立つレポートにも表示されます。

CPU、メモリ、ディスク使用量を監視するには、,

- **スタンドアロン展開。 System \> Statistics** に移動します。リアルタイムの CPU、メモリ、ディスク使用率チャートを表示できます。

  

- **高可用性展開。 Settings > Deployment** に移動します。メモリ、CPU、ディスク領域、および管理対象インスタンスの統計は、次の図に示すように数値で表示されます。

  

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 通知設定の構成

次の機能の通知を受信するための通知タイプを選択できます。

- **イベント** – NetScalerインスタンス用に生成されるイベントのリスト。詳細については、「イベントルールアクションの追加」を参照してください。
- **ライセンス** – 現在アクティブなライセンス、期限切れ間近のライセンスなどのリスト。詳細については、「NetScaler Consoleライセンスの有効期限」を参照してください。
- **SSL証明書** – NetScalerインスタンスに追加されたSSL証明書のリスト。詳細については、「SSL証明書の有効期限」を参照してください。

NetScaler Consoleは、次の通知タイプをサポートしています。

- メール
- SMS
- スラック
- PagerDuty
- ServiceNow

通知タイプごとに、NetScaler Console GUIには構成済みの配布リストまたはプロファイルが表示されます。NetScaler Consoleは、選択した配布リストまたはプロファイルに通知を送信します。

## メール配布リストの作成

NetScaler Console機能のメール通知を受信するには、メールサーバーと配布リストを追加する必要があります。

メール配布リストを作成するには、次の手順を実行します。

1. 「**Settings > Notifications**」に移動します。
2. 「**Email**」で、「**Add**」をクリックします。
3. 「**Create Email Distribution List**」で、次の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **メールサーバー** - メール通知を送信するメールサーバーを選択します。メールサーバーを追加する場合は、「**Add**」をクリックします。
   - **差出人** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
   - **宛先** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Cc** - NetScaler Consoleがメッセージのコピーを送信するメールアドレスを指定します。
- **Bcc** - NetScaler Consoleがアドレスを表示せずにメッセージのコピーを送信するメールアドレスを指定します。

メールを追加(/en-us/netscaler-application-delivery-management-software/media/config-jobs-maintenance-6.png)

4. 「**Create**」をクリックします。

複数のメール配信リストを作成するには、この手順を繰り返します。「**Email**」タブには、NetScaler Consoleに存在するすべてのメール配信リストが表示されます。

## SMS配信リストを作成する

NetScaler Console機能のSMS通知を受信するには、SMSサーバーと電話番号を追加する必要があります。

SMS通知設定を構成するには、次の手順を実行します。

1. 「**Settings > Notifications**」に移動します。
2. 「**SMS**」で、「**Add**」をクリックします。
3. 「**Create SMS Distribution List**」で、次の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **SMSサーバー** - SMS通知を送信するSMSサーバーを選択します。
   - **宛先** - NetScaler Consoleがメッセージを送信する電話番号を指定します。
4. 「**Create**」をクリックします。

複数のSMS配信リストを作成するには、この手順を繰り返します。「**SMS**」タブには、NetScaler Consoleに存在するすべてのSMS配信リストが表示されます。

## Slackプロファイルの作成

NetScaler Console機能のSlack通知を受信するには、Slackプロファイルを作成する必要があります。

Slackプロファイルを作成するには、次の手順を実行します。

1. 「**Settings > Notifications**」に移動します。
2. 「**Slack**」で、「**Add**」をクリックします。
3. 「**Create Slack Profile**」で、次の詳細を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **プロファイル名** - プロファイル名を指定します。この名前はSlackプロファイルリストに表示されます。
- **チャネル名** - NetScaler Consoleが通知を送信するSlackチャネル名を指定します。
- **Webhook URL** - チャネルのWebhook URLを指定します。受信Webhookは、外部ソースからSlackにメッセージを投稿する簡単な方法です。URLはチャネル名に内部的にリンクされています。このURLに送信されるすべてのイベント通知は、指定されたSlackチャネルに投稿されます。Webhookの例を次に示します。`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

Slackチャネルを追加(/en-us/netscaler-application-delivery-management-software/media/upgrade-slack.png)

4. 「**作成**」をクリックします。

複数のSlackプロファイルを作成するには、この手順を繰り返します。**Slack**タブには、NetScaler Consoleに存在するすべてのSlackプロファイルが表示されます。

## PagerDutyプロファイルの作成

PagerDutyの設定に基づいてインシデント通知を監視するために、PagerDutyプロファイルを追加できます。PagerDutyを使用すると、登録済みの番号に電子メール、SMS、プッシュ通知、電話で通知を設定できます。

NetScaler ConsoleにPagerDutyプロファイルを追加する前に、PagerDutyで必要な設定を完了していることを確認してください。PagerDutyの使用を開始するには、PagerDutyドキュメントを参照してください。

PagerDutyプロファイルを作成するには、次の手順を実行します。

1. **設定 > 通知**に移動します。
2. **PagerDuty**で、**追加**をクリックします。
3. **PagerDutyプロファイルの作成**で、次の詳細を指定します。
   - **プロファイル名** - 任意のプロファイル名を指定します。
   - **統合キー** - 統合キーを指定します。このキーはPagerDutyポータルから取得できます。PagerDutyで統合用のサービスを作成する際は、**Generic Events API Integration**オプションを使用してください。
4. 「**作成**」をクリックします。

詳細については、PagerDuty ドキュメントの Services and Integrations を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

複数の PagerDuty プロファイルを作成するには、この手順を繰り返します。**PagerDuty** タブには、NetScaler Console に存在するすべての PagerDuty プロファイルが表示されます。

### ServiceNow プロファイルの表示

NetScaler イベントおよび NetScaler Console イベントの ServiceNow 通知を有効にするには、ITSM コネクタを使用して NetScaler Console を ServiceNow と統合する必要があります。詳細については、NetScaler Console を ServiceNow インスタンスと統合する を参照してください。

ServiceNow プロファイルを表示および検証するには、次の手順を実行します。

1. **Settings > Notifications** に移動します。
2. **ServiceNow** で、リストから **Citrix_Workspace_SN** プロファイルを選択します。
3. **Test** をクリックして ServiceNow チケットを自動生成し、構成を検証します。

   NetScaler Console GUI で ServiceNow チケットを表示する場合は、**ServiceNow Tickets** を選択します。

## テックサポートファイルを生成する

問題のデバッグのためにテクニカルサポートに連絡する前に、NetScaler Consoleのデータと統計のアーカイブを生成することをお勧めします。このアーカイブは、テクニカルサポートチームに送信できるTARファイルです。

**注**

高可用性モードのNetScaler Consoleサーバーの場合、どちらかのサーバーからテクニカルサポートファイルを生成できます。Citrixは、テクニカルサポートファイルを生成するために負荷分散仮想サーバーIPアドレスを使用しないことを推奨しています。

**NetScaler Consoleからテクニカルサポートファイルを設定して送信するには：**

1. **設定** \> **診断** \> **テクニカルサポート** に移動し、**テクニカルサポートファイルの生成** をクリックします。
2. **サポートファイルの生成** ページで、次のオプションを選択します。

- **デバッグログの収集** – このオプションを選択して、`afdecoder` ログを収集します。
- **期間** – デバッグログを収集する必要がある期間を入力します。このオプションは、**デバッグログの収集** オプションを有効にした場合にのみ表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **データ分散の収集** – このオプションを選択して、データベースから個別の多様なログを収集します。

```
 The archive file is created as a TAR file.



 For example, the archive file that is created might be named as
follows:
Citrix_ADM_&lt;ADM_IP_address>_&lt;DDMMYY>_&lt;time_stamp>.tar.gz
```

1. テクニカルサポートファイルをサポートチームに送信する方法は2つあります。

   a. NetScaler Console GUIからファイルをローカルストレージにダウンロードし、Webブラウザを使用してCitrix Insight Services(CIS)にアップロードできます。

   b. また、Consoleでスクリプトを実行して、テクニカルサポートファイルをCISウェブサイトにアップロードすることもできます。

      i. SSHを使用して、Consoleにログオンします。

      ii. シェルプロンプトに切り替えて、次のように入力します。

      */mps/collector_upload.pl*

提供する必要がある属性を含む完全なコマンドを以下に示します。

```
/mps/collector_upload.pl [-proxy
[<proxy_user>:<proxy_password>@]<proxy_host>:<proxy_port>] [-user <user>]
[-password <password>] [-sr <sr>] [-description <description>] [-debug]
<file>
```

Perlスクリプトを実行する利点は、テクニカルサポートファイルをNetScaler Consoleからローカルシステムにダウンロードしてアップロードする必要がないことです。オプションとして、Consoleからプロキシを使用してファイルをCISに直接アップロードできます。

CISにアカウントがあることを確認してください。Citrixアカウントの資格情報を使用して、ファイルをCISにアップロードできます。

プロキシサーバーがない場合はどうなりますか？または、SSLフォワードプロキシで問題が発生している場合はどうなりますか？（これは、Perlスクリプトがプロキシサーバーのルート証明書を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

信頼しない場合に発生する可能性があります。） NetScaler ConsoleシェルからCISにファイルを直接アップロードすることもできます。

**注**

NetScaler ConsoleがコンソールからCISにファイルをアップロードできない状況では、ファイルをダウンロードしてCitrixテクニカルサポートチームにメールで送信することもできます。または、NetScaler Consoleからローカルストレージにファイルをダウンロードし、Webブラウザを使用してCISにアップロードすることもできます。

# 暗号グループを構成する

暗号グループは、Citrix NetScalerインスタンス上のSSL仮想サーバー、サービス、またはサービスグループにバインドする暗号スイートのセットです。暗号スイートは、プロトコル、鍵交換 (`Kx`) アルゴリズム、認証 (`Au`) アルゴリズム、暗号化 (`Enc`) アルゴリズム、およびメッセージ認証コード (`Mac`) アルゴリズムで構成されます。

**NetScaler Consoleで暗号グループを追加するには：**

1. **設定 > 管理**に移動します
2. **SSL設定**で、**暗号グループ**をクリックします
3. **追加**をクリックします
4. **暗号グループの作成**ページで、次の詳細を入力します。
   - **グループ名** - 暗号グループの名前。
   - **暗号グループの説明** – 暗号グループの説明を入力します。
   - **暗号スイート** – 「追加」をクリックして、使用可能なリストから暗号スイートを選択し、選択した（またはすべての）暗号スイートを構成済みリストに移動します。
5. **作成**をクリックします。

   暗号グループ(/en-us/netscaler-application-delivery-management-software/media/014_ciphergroups.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# SNMPトラップ宛先、マネージャーコミュニティ、およびユーザーを作成する

NetScaler Consoleで異常な状態が発生すると、SNMPトラップが生成されます。トラップは、トラップ宛先サーバーまたは *SNMP トラップ宛先* と呼ばれるリモートデバイスに送信されます。ここでは、NetScaler Consoleがトラップ宛先として構成されています。*SNMP マネージャー* と呼ばれるリモートデバイスから、システム固有の情報についてSNMPエージェントにクエリを実行できます。エージェントは、要求されたデータについて管理情報ベース (MIB) を検索し、そのデータをSNMPマネージャーに送信します。

**NetScaler ConsoleでSNMPトラップ宛先を作成するには：**

1. **System** \> **SNMP** \> **Trap Destinations** に移動します。
2. **SNMP Traps** で、**Add** をクリックしてSNMPトラップを作成し、次の詳細を指定します。
   - **バージョン。** 使用するSNMPバージョンを選択します。
   - **宛先サーバー。** トラップ宛先の名前またはIPアドレス。
   - **ポート。** トラップ宛先のポートを入力します。ポートはデフォルトで162に設定されています。
   - **コミュニティ。** トラップリスナーにトラップを送信するときに使用するコミュニティ文字列を指定します。
3. **Create** をクリックします。

> **注**
>
> SNMP v3トラップ宛先を作成する場合は、トラップをバインドするSNMPユーザー資格情報を指定します。SNMPユーザー資格情報を追加するには、**Insert** をクリックし、利用可能なSNMPユーザーのリストからユーザーを追加します。

**SNMPマネージャーコミュニティを作成するには：**

1. **System** \> **SNMP** \> **Managers** に移動します。
2. **SNMP Manager** で、**Add** をクリックしてSNMPマネージャーコミュニティを作成し、次の詳細を指定します。
   - 「**SNMPマネージャー**」SNMPマネージャーの名前またはIPアドレスを入力します。
   - 「**コミュニティ**」トラップリスナーにトラップを送信するときに使用するコミュニティ文字列を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. オプションで、**管理ネットワークを有効にする**チェックボックスを選択して、SNMPマネージャーネットワークのサブネットマスクである**ネットマスク**を指定できます。
4. **作成**をクリックします。

**SNMPユーザーを作成するには：**

1. **システム** \> **SNMP** \> **ユーザー**に移動します。
2. **SNMPユーザー**で、**追加**をクリックします。
3. ユーザー名を入力し、メニューからユーザーにセキュリティレベルを割り当てます。
4. ユーザーに割り当てたセキュリティレベルに基づいて、認証プロトコル、プライバシーパスワードなどの追加の認証プロトコルを提供し、SNMPビューを割り当てます。

# システムアラームの設定と表示

NetScaler Consoleサーバーの健全性を監視するために、一連のアラームを有効にして設定できます。重大なシステム問題や主要なシステム問題に確実に気づくために、システムアラームを設定する必要があります。たとえば、CPU使用率が高い場合や、サーバーへのログイン失敗が複数回発生した場合に通知を受けたい場合があります。cpuUsageHighやmemoryUsageHighなどの一部のアラームカテゴリでは、しきい値を設定し、それぞれの重大度（CriticalやMajorなど）を定義できます。inventoryFailedやloginFailureなどの一部のカテゴリでは、重大度のみを定義できます。アラームカテゴリのしきい値を超えた場合（例：memoryUsageHigh）、またはアラームカテゴリに対応するイベントが発生した場合（例：**loginFailure**）、メッセージがシステムに記録され、そのメッセージをsyslogメッセージとして表示できます。さらに、アラーム設定に応じて電子メールまたはSMSを受信する通知を設定できます。

アラームの重大度を割り当てたり変更したりできます。割り当て可能な重大度レベルは、Critical、Major、Minor、Warning、Informationalです。

バックアップの試行が失敗するたびに監視したいシナリオを考えてみましょう。backupFailedアラームを有効にし、Majorなどの重大度を割り当てることができます。NetScaler Consoleがシステムファイルのバックアップを試行し、その試行が失敗するたびにアラームがトリガーされます。このメッセージはNetScaler Consoleで表示するか、電子メールまたはSMSで通知を受け取ることができます。

アラームを設定するには、backupFailedアラームを選択し、重大度レベルをMajorとして指定する必要があります。このアラームはデフォルトで有効になっています。

**NetScaler Consoleを使用してシステムアラームを設定および表示するには：**

1. **Settings > SNMP**に移動します。右上の**Alarms**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 設定したいアラーム（例：backupFailed）を選択し、**Edit**をクリックして設定を変更します。
3. アラームはデフォルトで有効になっています。重大度レベル（例：Major）を割り当ててから、**OK**をクリックします。

**注**

一部のアラームでは、しきい値を設定できません。 アラームがトリガーされると、生成されたイベントをsyslogメッセージとして表示できます。

**NetScaler Consoleを使用してbackupFailedアラームによって生成されたイベントを表示するには：**

1. **System** > **Auditing**に移動します。
2. **Auditing**ページで、**Audit Messages**の下にある**Syslog Messages**を選択します。
3. 検索フィールドに、アラームの名前を入力します。この例では、バックアップの試行が失敗したイベントが生成されたことがわかります。

   バックアップ失敗アラーム(/en-us/netscaler-application-delivery-management-software/media/backup-failure-message.png)

   アラームがトリガーされたときに、電子メールまたはSMS（ショートメッセージサービス）テキストを送信するように通知を設定することもできます。システム通知の構成方法については、「NetScaler Consoleのシステム通知設定を構成する方法」を参照してください。

## ディスク使用率アラームにしきい値制限を追加する

ディスク使用率アラームは、NetScaler Consoleサーバーで使用されているディスク容量が事前定義されたしきい値を超えたときにトリガーされます。

管理者として、アラートを受信したときに、不要なデータを削除するか、追加のストレージリソースを割り当てて、サービスの中断やパフォーマンスの低下を防ぐことができます。

リリース14.1-25.x以降、ディスク使用率アラームに下位レベルのしきい値を追加することもできます。このしきい値を使用すると、上位のしきい値制限に達する前にアラートを受信する下位レベルの制限を設定できます。

下位レベルのしきい値を構成するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **設定 > SNMP > アラーム**に移動し、検索フィールドに「diskUtilizationHigh」と入力して、ディスク使用率アラームを表示します。
2. アラームを選択し、**編集**をクリックします。
3. **アラームの構成**ページで、**下位レベルのしきい値を構成**を選択します。下位レベルのしきい値制限を入力します。

   バックアップ失敗アラーム(/en-us/netscaler-application-delivery-management-software/media/snmp-alarms-lower-threshold.png)

たとえば、ディスク使用率の下位しきい値を60、上位しきい値を80に設定した場合、ディスク使用量がディスク容量の60%を超えるとアラートを受信します。この設定により、ディスク使用率が80%に達する前に是正措置を講じることができます。

# NetScalerエージェントのSNMPマネージャーとユーザーを作成する

SNMPマネージャーと呼ばれるリモートデバイスから、システム固有の情報をSNMPエージェントに照会できます。エージェントは、要求されたデータについて管理情報ベース (MIB) を検索し、そのデータをSNMPマネージャーに送信します。

NetScalerエージェントに照会するためにSNMPマネージャーを追加できます。マネージャーはSNMP V2およびV3に準拠しています。1つ以上のSNMPマネージャーを指定した場合、NetScalerエージェントは、指定されたSNMPマネージャー以外のホストからのSNMPクエリを受け入れません。

## SNMP v2マネージャーを追加する

NetScalerエージェントのSNMP v2マネージャーを追加するには：

1. **Infrastructure > Agents** に移動し、NetScalerエージェントを選択して、**Select Action > Manage SNMP** をクリックします。
2. **SNMP > SNMP Manager** タブで、**Add** をクリックします。
3. **Create SNMP Manager** ページで、次の詳細を指定します。

   - **SNMP Manager**。SNMPマネージャーの名前またはIPアドレスを入力します。
   - **Version**。v2を選択します。
   - **Community**。コミュニティ名を入力します。SNMPコミュニティ設定は、SNMPマネージャーからのSNMPクエリを認証します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enable Management Network**: このチェックボックスをオンにして、SNMPマネージャーネットワークのネットマスクを指定します。
- **Netmask**: IPアドレスに関連付けられたサブネットマスクを入力します。

4. **Create** をクリックします。

## SNMP v3マネージャーを追加する

NetScalerエージェントにSNMP v3マネージャーを追加するには：

1. **Infrastructure > Agents** に移動し、NetScalerエージェントを選択して、**Select Action > Manage SNMP** をクリックします。
2. **SNMP > SNMP Manager** タブで、**Add** をクリックします。
3. **Create SNMP Manager** ページで、次の詳細を指定します。
   - **SNMP Manager**。SNMPマネージャーの名前またはIPアドレスを入力します。
   - **Version**。v3を選択します。
   - **Enable Management Network**：このチェックボックスをオンにして、SNMPマネージャーネットワークのネットマスクを指定します。
   - **Netmask**：IPアドレスに関連付けられたサブネットマスクを入力します。
4. **Create** をクリックします。

SNMP v3マネージャーの作成(/en-us/netscaler-application-delivery-management-software/media/snmp-manager-v3.png)

SNMPマネージャーが作成されたことを確認し、SNMPユーザーを構成するように促すダイアログボックスが表示されます。

構成メッセージ(/en-us/netscaler-application-delivery-management-software/media/snmp-manager-v3-message.png)

**注**

SNMP v3マネージャーにはSNMPユーザーを構成する必要があります。SNMPユーザーを構成するには、**SNMP > SNMP User** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## SNMPユーザーを追加する

SNMPマネージャーからのSNMP v3クエリに応答するためにSNMPユーザーを追加します。

NetScalerエージェントのSNMPユーザーを追加するには：

1. **Infrastructure > Agents** に移動し、NetScalerエージェントを選択して、**Select Action > Manage SNMP** をクリックします。
2. **SNMP > SNMP User** タブで、**Add** をクリックします。
3. **Create SNMP User** ページで、次の詳細を追加します。

   - **名前**。ユーザー名を入力します。
   - **セキュリティレベル**。NetScalerエージェントとSNMPマネージャー間の通信に必要なセキュリティレベル。

     次のいずれかのセキュリティレベルを選択します。
   - **noAuthNoPriv**。認証も暗号化も不要です。

   - **authNoPriv**。認証は必要ですが、暗号化は不要です。

   - **authPriv**。認証と暗号化が必要です。

   ユーザーに割り当てたセキュリティレベルに基づいて、認証プロトコル、プライバシーパスワードなどの追加の認証プロトコルを提供し、SNMPビューを割り当てます。

## SNMPビューの管理

SNMPビューは、SNMPユーザーのアクセス制御を実装するために使用されます。SNMPビューは、ユーザーがMIBの特定のセクションにアクセスすることを制限します。

NetScalerエージェントのSNMP OIDを許可または制限するには：

1. **Infrastructure > Agents > Manage SNMP** に移動し、**SNMP View** タブで **Add** をクリックします。
2. **Create SNMP View** で、次の詳細を入力します。

   - **ビュー名**: SNMPビューの名前。インスタンスは、サブツリーパラメータ設定によって区別される、同じ名前の複数のSNMPビューを持つことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **サブツリー**: このSNMPビューに関連付けたいMIBツリーの特定のブランチ（サブツリー）。サブツリーはSNMP OIDとして指定する必要があります。
- **タイプ**: このフィールドでは、ビューからサブツリーを含めるか除外するかを設定できます。

3. **Create** をクリックします。

# エージェント設定の構成

NetScaler Consoleエージェントのキープアライブ間隔とパスワード変更要件を変更できます。

## エージェントのキープアライブ間隔を設定する

NetScaler Consoleサーバーとエージェントは、指定されたキープアライブ間隔の間、同じTCP接続を維持します。エージェントはこの接続を使用して、管理対象インスタンスのデータをNetScaler Consoleサーバーに送信します。

1. **>** の順に移動します。
2. **システム設定**で、**システム, タイムゾーン, 許可されたURL, およびエージェント設定**を選択します。
3. **>** で、キープアライブ間隔を30～120秒の間に指定します。
4. をクリックします。

## 現在のパスワードなしでエージェントのパスワードを変更する

エージェントのパスワードを現在のパスワードなしで変更できるようにすることができます。

1. **>** の順に移動します。
2. **システム設定**で、**システム, タイムゾーン, 許可されたURL, およびエージェント設定**を選択します。
3. **> >** チェックボックスで、次の操作を実行できます。
   - チェックボックスをオンにすると、 ページから フィールドが削除されます。
   - チェックボックスをオフにすると、 ページに フィールドが保持されます。
4. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

「**エージェントパスワードの変更**」ページを表示するには、**インフラストラクチャ > インスタンス > エージェント**に移動し、エージェントを選択して、**アクションの選択 > パスワードの変更**をクリックします。

# データストレージ管理ダッシュボードを使用する

NetScaler Console でどの機能が使用されているか、およびそれらの機能ごとのデータ使用量を把握することは重要です。**データストレージ管理**ダッシュボードは、この目的のために機能し、視覚化ツールとして、さまざまな機能にわたってNetScaler Consoleデータベースに保存されている合計データ量を理解するのに役立ちます。このダッシュボードは、消費されたストレージが指定された制限内にあるか、または許可されたストレージを超えているかどうかも示します。

管理者として、**データストレージ管理**ダッシュボードで次のタスクを実行できます。

- 過去30日間のデータストレージ消費量を表示する - データストレージの傾向は、過去30日間、NetScaler Console データベースに保存されます。これらの傾向は、グラフ形式または表形式で利用できます。これらの傾向は、NetScaler Console でのスケジュールされたプルーニングサイクル後に、どれだけのデータが取り込まれ、どれだけのデータが保存されているかを示します。
- データ取り込みステータスを表示する - データ取り込みアクティビティは、消費されたストレージが許可されたストレージの制限内にある限り発生します。消費されたストレージが許可されたストレージを超えると、データアクティビティは一時停止されます。
- 通知を送信する - 消費されたストレージが許可されたストレージの75%または100%に達したときに通知が送信されるように設定でき、ユーザーがストレージを管理できるようになります。
- データストレージスペースを管理する柔軟性 - 削除または削減に適していると判断したデータをプルーニングすることで、保存されているデータ内にさらにスペースを作成できます。

データストレージダッシュボードを表示するには、**設定 > データストレージ**に移動します。

以下のセクションでは、効果的なデータストレージ管理のために**データストレージ管理**ダッシュボードを使用する方法について概説します。

- データストレージを理解する - このセクションでは、ダッシュボードを使用してデータストレージに関する情報を表示する方法を理解するのに役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- データストレージを管理する - このセクションでは、データストレージを管理するためにダッシュボードで実行できるアクションに関する情報を提供します。

## データストレージを理解する

NetScaler Consoleの**データストレージ管理**ダッシュボードを使用して、データストレージの使用状況を追跡するのに役立つデータとグラフを表示できます。

データストレージの使用状況を監視するには、**設定 > データストレージ**に移動します。

データストレージダッシュボード(/en-us/netscaler-application-delivery-management-software/media/data-storage-management-dashboard.png)

データストレージ管理ダッシュボードには、次の情報が表示されます。

- データ取り込みアクティビティのステータス
- 総ストレージ消費量
- ストレージ消費の傾向
- 機能別のストレージ消費量

### データ取り込みアクティビティのステータス

データ取り込みとは、管理対象のすべてのNetScalerインスタンスから、イベント、Syslog、ネットワークレポートなどのさまざまな機能にわたる大量の多様なデータをNetScaler Consoleストレージにインポートするプロセスを指します。

データ取り込みステータスは、NetScaler ConsoleがNetScalerインスタンスから統計を収集しているかどうかを示します。データ取り込みアクティビティは、消費されたストレージが割り当てられたストレージ内にある限り継続されます。消費量が割り当てられたストレージを超えると、データ取り込みは一時停止されます。

**データ取り込み**タイルを表示して、データ取り込みの現在の状態を把握します。このタイルには、次の2つの状態のいずれかが表示されます。

- **アクティブ** - データ取り込みアクティビティが進行中です。

データストレージダッシュボード(/en-us/netscaler-application-delivery-management-software/media/data-storage-ingestion-activity.png)

- **一時停止** - 消費ストレージが割り当てストレージを超過したため、データ取り込みアクティビティは一時停止されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 一時停止されたデータ取り込みを再開する方法

データ取り込みアクティビティを再開するには、データプルーニングを実行できます。詳細については、データプルーニングの実行を参照してください。

## 総ストレージ消費量

データストレージの概要を素早く確認するには、「**ストレージ消費量**」タイルを表示します。



「**ストレージ消費量**」タイルには、展開内のすべての機能で使用されている総ストレージが表示されます。

ドーナツグラフにマウスを重ねると、以下が表示されます。

### 割り当てストレージ

割り当てストレージは、ライセンスに従って利用できる総ストレージです。Expressライセンスをお持ちの場合、500 MBの割り当てストレージが付与されます。Advancedライセンスをお持ちの場合、購入したVIPごとの500 MBのストレージの合計と、VIPを購入せずに直接購入した追加ストレージの合計が付与されます。

次のシナリオを考慮してください。

- 20個のVIPを購入しました。各VIPにつき500 MBの無料ストレージが付与されます。割り当てストレージは20*500 = 10 GBです。
- 20個のVIPと5 GBのアドオンストレージを購入しました。各VIPにつき500 MBの無料ストレージが付与されます。割り当てストレージは20*500 + 5 = 15 GBです。

### 消費ストレージ

消費ストレージとは、展開内のすべての機能で使用される合計ストレージのことです。以下の色分け基準は、機能によって使用されるストレージの量を指定します。

- **緑** - 消費ストレージが割り当てられたストレージの75%未満です。
- **琥珀色** - 消費ストレージが割り当てられたストレージの75%から99%の間です。
- **赤** - 消費ストレージの制限が現在の割り当てられたストレージに達しているか、それを超えています。

## ストレージ消費の傾向

過去30日間のデータ消費状況を知るには、「**ストレージ消費傾向**」セクションを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「**ストレージ消費傾向**」は、ある期間にどの機能が最も多くのストレージを使用しているか、または最も少ないストレージを使用しているかについての洞察を提供し、データストレージの消費を効果的に管理するのに役立ちます。

ストレージデータの傾向は、以下のいずれかの形式で表示できます。

- **グラフィカルビュー** – 異なるNetScaler Console機能間でデータストレージがどのように分散されているかを表示します。タイムラインにマウスを合わせると、その月の任意の日付のデータストレージ情報を表示できます。

  グラフィカルビュー(/en-us/netscaler-application-delivery-management-software/media/storage-consumption-trend-graph.png)

  **注:**

  **グラフィカルビュー**がデフォルトのビューです。

- **表形式ビュー** – 「**表形式ビュー**」をクリックすると、データストレージ情報が表形式で表示されます。

  表形式ビュー(/en-us/netscaler-application-delivery-management-software/media/storage-consumption-trend-table.png)

  **注:**

  表形式ビューでは、検索フィールドを使用してデータをフィルタリングできます。

次の表は、**ストレージ消費傾向**セクションに表示されるフィールドについて説明しています。

| 機能 | 説明 |
| --- | --- |
| **構成** | インスタンス、構成ジョブ、構成監査などに関する情報を含む、すべての構成可能なデータが含まれます。 |
| **HDX インサイト** | NetScaler を通過する ICA トラフィックのエンドツーエンドの可視性を提供します。 |
| **ネットワークレポート** | すべての NetScaler インスタンスのネットワークパフォーマンスを表示します。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 機能 | 説明 |
| --- | --- |
| **Web インサイト** | エンタープライズWebアプリケーションの可視性を提供し、アプリケーションの統合されたリアルタイム監視を可能にします。 |
| **Security インサイト** | アプリケーションのセキュリティ状態を評価し、アプリケーションを保護するための是正措置を講じるのに役立ちます。 |
| **Gateway インサイト** | NetScaler Gatewayへのログオン時に、アクセスモードに関わらず、すべてのユーザーが遭遇した障害を可視化します。 |
| **イベント** | NetScalerインスタンス上のイベントまたはエラーの発生を監視および管理します。 |
| **アプリダッシュボード** | アプリケーションの表示と管理を可能にします。 |
| **ボットインサイト** | ボット違反とそれらに対して取られたアクションを可視化します。 |
| **システムログ** | デバイスがすべてのsyslogメッセージをNetScaler Consoleにリダイレクトするように構成されている場合、NetScalerインスタンスで生成されたsyslogイベントを監視します。 |
| **ビデオインサイト** | NetScalerインスタンスで使用されるビデオ最適化技術のメトリックを監視します。 |
| **詳細トランザクション** | Webトランザクションを可視化し、クライアント、NetScaler、サーバーにわたる応答時間メトリックを視覚的に表示します。 |

## 機能別のストレージ消費量

To know more about how the data storage is distributed across the different features, view the **Storage Consumption by features as on *dd mmm*** section.

**Storage Consumption by features as on *dd mmm*** helps you understand:

- NetScaler Consoleにおけるすべての異なる機能によって使用されるストレージ容量

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 特定の日に機能が消費する容量の割合

機能と説明(/en-us/netscaler-application-delivery-management-software/media/data-storage-distribution.png)

テーブルのエントリをソートしたい場合は、テーブルのヘッダーを使用します。NetScaler Consoleは、選択した列のデータに基づいて、テーブルを上から下へ英数字順にソートします。テーブルを逆順にソートするには、列見出しをもう一度クリックします。

データのプルーニング、プルーン履歴、およびストレージイベントログに関する情報については、「データのストレージを管理する」を参照してください。

## ストレージ容量を管理する

**データストレージ管理**ダッシュボードを使用して、データストレージの使用状況を監視し、データストレージがライセンス制限を超過した場合に、スペースをクリアしたりストレージを増やしたりするために必要なアクションを実行できます。

アクション(/en-us/netscaler-application-delivery-management-software/media/data-storage-actions.png)

**アクション**タイルには、ストレージ容量を管理するために実行できる推奨手順のリストが表示されます。

- データ保持ポリシーを確認する
- データプルーニングを実行する
- ストレージ制限超過時に通知する

### データプルーニングを実行する

ストレージリソースを最適化し、より多くのストレージスペースを確保するためにデータをプルーニングします。スペースを解放するだけでなく、データプルーニングはデータ品質を向上させ、処理時間を短縮します。不要なデータを定期的に確認し、パージすることをお勧めします。このプロセスにより、リソースが適切に使用され、NetScaler Consoleが俊敏で応答性が高くなります。

データをプルーニングするには：

1. **データストレージ管理**ページで、***Storage Consumption by features as on yyyy-mm-dd***セクションまでスクロールダウンします。
2. 1つ以上の機能を選択し、**プルーニング**をクリックします。**Config**はすべてのシステム構成を含むため、選択できません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

選択した機能のすべてのデータを削除するかどうかを確認するポップアップウィンドウが表示されます。**はい、プルーニング**をクリックします。

機能と説明(/en-us/netscaler-application-delivery-management-software/media/prune-data-message.png)

### プルーニング履歴を表示する

NetScaler Console で実行したすべての剪定アクティビティの詳細を確認するには、「**View Prune History**」をクリックします。

「**Prune Logs: Task Logs**」ページには、すべての剪定タスクのリストと、それぞれのステータス、開始時刻、終了時刻が表示されます。

各剪定操作でどの機能が削除されたかを理解するには、タスクを選択し、「**Feature Log**」をクリックします。

### ストレージイベントログの表示

データがライセンス制限の75%を超過または到達したすべての時点に関する洞察を得るには、「**Storage Event Logs**」をクリックします。

## データ保持ポリシーの確認

データ保持ポリシーとは、NetScaler Console が履歴データを時間の経過とともにどのように管理および維持するかを決定する一連のルールと構成を指します。このポリシーは、データが自動的に削除されるまでにデータがどのくらいの期間保存されるかを概説します。

すべての異なる機能で使用されるストレージスペースを削減したい場合は、NetScaler Console でデータが保持される期間を変更できます。

「**Data Retention policy**」ページを使用して、以下のデータストレージ設定を編集します。

- イベントメッセージ
- Syslog メッセージ
- ネットワークレポートデータ

データストレージ設定の詳細については、データ保持ポリシーを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ストレージ制限超過時の通知

NetScaler Consoleで、データストレージ容量が指定された制限を超過した場合にアラートを送信する通知を設定できます。

システム通知を表示および設定するには：

1. **Actions**タイルで、**Notify on exceeding storage limit**をクリックします。
2. **Configure System Notifications**ページで、**System Event Category**の下にある**DataStorageExceeded**カテゴリが選択されていることを確認して、通知を受信します。

通知があなたまたは他のユーザーに送信される方法とタイミングに関連するさまざまなパラメータを指定できます。優先する通信方法（例：メール、Slack、PagerDuty、ServiceNow通知）を選択し、通知の受信者を定義します。

プロファイルの設定方法と通知の送信方法の詳細については、通知の設定を参照してください。

## データ保持ポリシー

NetScaler Consoleサーバーのデータベースに保存されるレポートデータの量を制限するには、NetScaler Consoleがネットワークレポートデータ、イベント、監査ログ、タスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと（00:00時）に削除されます。

### システムの削除設定を構成する

システムの削除設定を構成するには：

1. **設定 > データストレージ > データ保持ポリシー**に移動します。
2. **データ削除**ページで、**システム**をクリックします。
3. **システム**ページで、次の詳細を入力します。

    - **保持するデータ（日数）** - データを保持する日数を入力します。1から30までの値を指定する必要があります。
    - **データ削除しきい値（%）** - データ削除またはデータクリーンアッププロセスの条件として設定するしきい値（パーセンテージ）を入力します。データベース内のデータがストレージ容量のこの指定されたパーセンテージに達すると、データを削除してスペースを解放するためにデータ削除手順がトリガーされます。
    - **自動削除の詳細** - 以下のいずれかの条件が満たされたときにデータ削除を開始する場合は、**自動データ削除を有効にする**を選択します。

        ◦ **データ削除しきい値（%）**で指定されたデータしきい値に達した。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **保持するデータ（日数）**で指定された日数に達した。

- **データ取り込み設定** - データ取り込みの条件として設定するしきい値（パーセンテージ）を入力します。データベース内のデータがこの指定されたパーセンテージに達すると、データ取り込みアクティビティは一時停止されます。50%から80%の範囲で制限を指定する必要があります。

4. **保存**をクリックして設定を保存します。

### インスタンスイベントの削除設定を構成する

NetScaler Consoleサーバーのデータベースに保存されるイベントメッセージデータの量を制限するには、NetScaler Consoleがネットワークレポートデータ、イベント、監査ログ、タスクログを保持する期間を指定できます。デフォルトでは、このデータは24時間ごと（00:00時）に削除されます。

インスタンスイベントの削除設定を構成するには：

1. **設定 > データストレージ > データ保持ポリシー** に移動します。
2. **Data Pruning** ページで、**Instance Events** をクリックします。
3. **Data to keep (days)** フィールドに、NetScaler Consoleサーバーでデータを保持する期間を日数で入力し、**Save** をクリックします。

### インスタンスsyslogの削除設定を構成する

データベースに保存されるsyslogデータの量を制限するには、syslogデータをパージする間隔を指定できます。NetScaler Consoleから汎用syslogデータが削除されるまでの日数を指定できます。

インスタンスsyslogのパージ設定を構成するには：

1. **設定 > データストレージ > データ保持ポリシー** に移動します。
2. **Data Pruning** ページで、**Instance Events** をクリックします。
3. **Retain Syslog Generic Data** フィールドに、1から180までの日数を指定します。
4. **Save** をクリックします。

### ネットワークレポートの削除設定を構成する

NetScaler Consoleに保存されるネットワークレポートデータを制限するには、ネットワークレポートの履歴データを保持する期間を指定できます。

インスタンスイベントの削除設定を構成するには：

1. **設定 > データストレージ > データ保持ポリシー** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 「**データプルーニング**」ページで、「**ネットワークレポート**」をクリックします。
3. 「**保持するデータ (日数)**」フィールドで、1から30までの日数を指定します。
4. 「**保存**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# API プロキシサーバーとしての NetScaler Console

NetScaler Application Delivery Management (NetScaler Console) は、独自の管理および分析機能のために NITRO REST API リクエストを受信できることに加えて、管理対象インスタンスの REST API プロキシサーバーとして機能できます。API リクエストを管理対象インスタンスに直接送信する代わりに、REST API クライアントは NetScaler Console に API リクエストを送信できます。NetScaler Console は、自身が応答する必要がある API リクエストと、管理対象インスタンスにそのまま転送する必要がある API リクエストを区別できます。

API プロキシサーバーとして、NetScaler Console は以下の利点を提供します。

- **API リクエストの検証**。NetScaler Console は、構成されたセキュリティおよびロールベースのアクセス制御 (RBAC) ポリシーに対してすべての API リクエストを検証します。NetScaler Console はテナントを認識しており、API アクティビティがテナントの境界を越えないようにします。
- **一元化された監査**。NetScaler Console は、管理対象インスタンスに関連するすべての API アクティビティの監査ログを保持します。
- **セッション管理**。NetScaler Console は、API クライアントが管理対象インスタンスとのセッションを維持するタスクから解放します。

API プロキシサーバーとして、NetScaler Console は管理者パーティションをサポートします。

## NetScaler Console が API プロキシサーバーとして機能する方法

NetScaler Console に管理対象インスタンスへのリクエストを転送させたい場合、API クライアントを構成して、API リクエストに以下のいずれかの HTTP ヘッダーを含めます。

| ヘッダー値 | 説明 |
| --- | --- |
| MPS-API-PROXY-MANAGED-INSTANCE-NAME | 管理対象インスタンスの名前。 |
| MPS-API-PROXY-MANAGED-INSTANCE-IP | 管理対象インスタンスの IP アドレス。 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ヘッダー値 | 説明 |
| --- | --- |
| MPS-API-PROXY-MANAGED-INSTANCE-ID | 管理対象インスタンスのID。 |
| MPS-API-PROXY-TIMEOUT | NITRO APIリクエストのタイムアウト値。タイムアウト値を秒単位で設定します。プロキシタイムアウトを設定すると、NetScaler Consoleは、リクエストがタイムアウトするまで指定された期間待機します。 |
| MPS-API-PROXY-MANAGED-INSTANCE-USERNAME | 管理対象のNetScalerインスタンスにアクセスするためのユーザー名。 |
| MPS-API-PROXY-MANAGED-INSTANCE-PASSWORD | 管理対象のNetScalerインスタンスにアクセスするためのパスワード。 |
| MPS-API-PROXY-MANAGED-INSTANCE-SESSID | 管理対象インスタンスにアクセスするためのセッションID。 |

**注**

**Settings > Administration >** System Configurations **> Basic Settings** で、**Prompt Credentials for Instance Login** を選択した場合、管理対象インスタンスのユーザー名とパスワードを設定してください。または、インスタンスセッションIDを指定することもできます。

これらのHTTPヘッダーのいずれかが存在すると、NetScaler ConsoleはAPIリクエストを管理対象インスタンスに転送する必要があるものとして識別するのに役立ちます。ヘッダーの値は、NetScaler Consoleがリクエストを転送すべき管理対象インスタンスを識別するのに役立ちます。

このフローを次の図に示します。



上図に示すように、これらのHTTPヘッダーのいずれかがリクエストに現れると、NetScaler Consoleは次のようにリクエストを処理します。

1. リクエストを変更せずに、NetScaler Consoleはリクエストをインスタンスプロキシエンジンに転送します。
2. インスタンスAPIプロキシエンジンは、APIリクエストをバリデーターに転送し、APIリクエストの詳細を監査ログに記録します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. バリデーターは、リクエストが設定されたセキュリティポリシー、RBACポリシー、テナンシー境界などに違反していないことを確認します。また、管理対象インスタンスが利用可能であるかどうかのチェックなど、追加のチェックを実行します。

APIリクエストが有効で、管理対象インスタンスに転送できる場合、NetScaler Consoleはインスタンスセッションマネージャーによって維持されているセッションを識別し、そのリクエストを管理対象インスタンスに送信します。

**注**

**インスタンスログインの資格情報のプロンプト**オプションが無効になっていることを確認してください。これを行うには：

1. **設定 > 管理**に移動します。
2. **システム構成**で、**システム、タイムゾーン、許可されたURL、および今日のメッセージ**を選択します。

# NetScaler ConsoleをAPIプロキシサーバーとして使用する方法

次の例は、IPアドレス192.0.2.5を持つNetScaler ConsoleサーバーにAPIクライアントが送信するREST APIリクエストを示しています。NetScaler Consoleは、リクエストをIPアドレス192.0.2.10の管理対象インスタンスに、変更せずに転送する必要があります。すべての例でMPS-API-PROXY-MANAGED-INSTANCE-IPヘッダーを使用しています。

NetScaler ConsoleにAPIリクエストを送信する前に、APIクライアントは次のことを行う必要があります。

- NetScaler Consoleにログインする
- セッションIDを取得する
- 後続のAPIリクエストにセッションIDを含める。

ログオンAPIリクエストは次の形式です。

```
POST /nitro/v1/config/login

Content-Type: application/json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    {

        "login": {

            "username":"nsroot",

            "password":"nsroot"

         }

    }
```

NetScaler Consoleは、セッションIDを含む応答でログオンリクエストに応答します。次のサンプル応答本文は、セッションIDを示しています。

```
{


  "errorcode": 0,


  "message": "Done",


  "operation": "add",


  "resourceType": "login",


  "username": "***********",


  "tenant_name": "Owner",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"resourceName": "nsroot",

"login": [

  {

    "tenant_name": "Owner",

    "permission": "superuser",

    "session_timeout": "36000",

    "challenge_token": "",

    "username": "",

    "login_type": "",

    "challenge": "",

    "client_ip": "",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved. 

```
      "client_port": "-1",


      "cert_verified": "false",


      "sessionid":
"##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",


      "token": "b2f3f935e93db6a"
    }


  ]


}
```

## 例1：負荷分散仮想サーバーの統計情報を取得する

クライアントは、NetScaler Consoleに次の形式のAPIリクエストを送信する必要があります。

```
GET /nitro/v1/stat/lbvserver

Content-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

ここで、Cookieヘッダーの値はログインAPI呼び出しから返されたセッションIDです。MPS-API-PROXY-MANAGED-INSTANCE-IPの値はNetScalerのIPアドレスです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 例2：負荷分散仮想サーバーを作成する

クライアントは、NetScaler Consoleに次の形式のAPIリクエストを送信する必要があります。

```
POST /nitro/v1/config/lbvserver/sample_lbvserver

Content-type: application/json

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D


{

     "lbvserver":{

         "name":"sample_lbvserver",

         "servicetype":"HTTP",

         "ipv46":"10.102.1.11",

         "port":"80"

     }

}
```

## 例3：負荷分散仮想サーバーを変更する

クライアントは、NetScaler Consoleに次の形式のAPIリクエストを送信する必要があります。

```
PUT /nitro/v1/config/lbvserver

Content-type: application/json

Accept-type: application/json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

   "lbvserver":{

        "name":"sample_lbvserver",

        "appflowlog":"DISABLED"

   }

}
```

## 例4：負荷分散仮想サーバーを削除する

クライアントは、NetScaler Consoleに次の形式のAPIリクエストを送信する必要があります。

```
DELETE /nitro/v1/config/lbvserver/sample_lbvserver

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

## 例5：NetScalerでCLI実行中の構成をダウンロードする

クライアントは、NetScaler Consoleに次の形式のAPIリクエストを送信する必要があります。

```
GET /nitro/v1/config/nsrunningconfig

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# よくある質問

このセクションでは、以下のNetScaler Application Delivery Management (NetScaler Console) 機能に関するFAQを提供します。その機能のFAQリストを表示するには、以下の表の機能名をクリックしてください。

| アナリティクス | 認証 | 構成管理 |
| --- | --- | --- |
| 証明書管理 | 展開 | 展開 (ディザスタリカバリ) |
| イベント管理 | インスタンス管理 | StyleBooks |
| システム管理 | | |

## アナリティクス

### シングルホップモードで展開されたNetScaler Gatewayインスタンスで EUEM仮想チャネルを有効にする必要がありますか?

EUEM仮想チャネルデータは、NetScaler ConsoleがGatewayインスタンスから受信するHDX Insightデータの一部です。EUEM仮想チャネルは、ICA RTTに関するデータを提供します。EUEM仮想チャネルが有効になっていない場合でも、残りのHDX InsightデータはNetScaler Consoleに表示されます。

EUEM仮想チャネルは、Citrix Virtual Desktopアプリケーション (VDA) で実行されているデフォルトのサービスです。実行されていない場合は、VDAサービスで「Citrix End User Experience Monitoring」プロセスを開始してください。

### NetScaler ConsoleでWebアプリケーションおよび仮想デスクトップのトラフィックを監視するにはどうすればよいですか?

1. **インフラストラクチャ** \> **インスタンス** \> **NetScaler** の順に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. **アクションの選択** リストから、**分析の構成** を選択します。
3. **分析の構成** ページで、分析を有効にするすべての仮想サーバーを選択し、**AppFlowを有効にする** をクリックします。詳細については、「インスタンスで分析を有効にする方法」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注：**

リリース11.0、ビルド65.30以降のNetScalerインスタンスでは、NetScaler ConsoleでSecurity Insightを明示的に有効にするオプションはありません。NetScalerインスタンスでAppFlowパラメーターを構成して、NetScaler ConsoleがWeb Insightトラフィックとともに Security Insightトラフィックの受信を開始するようにしてください。NetScalerインスタンスでAppFlowパラメーターを設定する方法の詳細については、「構成ユーティリティを使用してAppFlowパラメーターを設定するには」を参照してください。

## NetScalerインスタンスを追加した後、NetScaler Consoleは自動的に分析情報の収集を開始します?

いいえ。NetScaler Consoleによって管理されているNetScalerインスタンスでホストされている仮想サーバーで分析を有効にします。詳細については、「インスタンスで分析を有効にする方法」を参照してください。

## 分析を有効にするために、個々のNetScalerアプライアンスにアクセスする必要があります?

いいえ。すべての構成はNetScaler Consoleユーザーインターフェイスから行われ、特定のNetScalerインスタンスでホストされている仮想サーバーが一覧表示されます。詳細については、「インスタンスで分析を有効にする方法」を参照してください。

## 分析を有効にするためにNetScalerインスタンスに一覧表示できる仮想サーバーの種類?

現在、NetScaler Consoleユーザーインターフェイスには、分析を有効にするための次の仮想サーバーが一覧表示されます。

- 負荷分散仮想サーバー
- コンテンツスイッチング仮想サーバー
- VPN仮想サーバー
- キャッシュリダイレクション仮想サーバー

## NetScaler Consoleにディスクを追加するにはどうすればよいですか?

NetScaler Consoleにディスクを追加するには：

1. NetScaler Console仮想マシンをシャットダウンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ハイパーバイザーで、必要なディスクサイズの追加ディスクをNetScaler Console仮想マシンに接続します。

   例えば、120 GBのNetScaler Console仮想マシンでディスク容量を200 GBに増やしたいとします。このシナリオでは、80 GBではなく200 GBのディスク容量を接続する必要があります。新しく接続された200 GBのディスク容量は、データベースデータ、NetScaler Consoleログファイルの保存に使用されます。既存の120 GBのディスク容量は、コアファイル、オペレーティングシステムログファイルなどの保存に使用されます。

3. NetScaler Console仮想マシンを起動します。

### NetScalerインスタンスでコレクターが構成されていないとはどういう意味ですか?

コレクターは、NetScalerアプライアンスによって生成されたAppFlowレコードを受信します。

AppFlow機能が有効になっている場合、NetScaler ConsoleはNetScalerインスタンスからSecurity InsightおよびWeb Insightトラフィックを受信します。NetScalerインスタンスでAppFlow機能を有効にする場合、AppFlowレコードの送信先となるコレクターを少なくとも1つ指定する必要があります。NetScalerインスタンスでコレクターが構成されていない場合、NetScaler Consoleはインスタンスからのトラフィックを受信しません。

例えば、5つのNetScalerインスタンスがNetScaler Consoleに追加されているとします。2つのインスタンスでコレクターが指定されていない場合、NetScaler Consoleにトラフィックは流れません。セルフサービス診断がこの問題を検出し、「コレクターが2つのインスタンスで構成されていません」と表示します。

AppFlow機能の構成方法の詳細については、「AppFlow機能の構成」を参照してください。

### クライアント側測定を有効にするとどうなりますか?

クライアント側測定を有効にすると、NetScaler ConsoleはHTMLインジェクションを通じて、HTMLページのロード時間とレンダリング時間のメトリックをキャプチャします。これらのメトリックを使用することで、管理者はL7レイテンシーの問題を特定できます。

## 認証

### 認証要求の負荷分散とは何ですか?

認証サーバーの負荷分散機能により、NetScaler Console は外部認証サーバーに向けられた認証要求を負荷分散できます。認証サーバーを負荷分散することで、認証負荷が複数の認証サーバーに分散され、認証サーバーの過負荷を防ぐことができます。LDAP、RADIUS、TACACS などの認証プ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ロトコルを使用して、既存の外部認証サーバーに接続し、ユーザー情報を取得するための認証サービスを作成できます。

## 外部認証サーバーをカスケード接続する必要があるのはなぜですか?

カスケード接続された外部認証サーバーは、認証処理を中断することなく提供し、認証サーバーが故障した場合でも正当なユーザーがアクセスできるようにします。カスケード接続できる認証サーバーの種類に制限はありません。すべての RADIUS サーバー、すべての LDAP サーバー、または RADIUS と LDAP サーバーの組み合わせを使用できます。

## いくつの外部認証サーバーをカスケード接続できますか?

NetScaler Console では、最大 32 台の外部認証サーバーをカスケード接続できます。

## 外部認証が失敗した場合の代替手段はありますか?

複数のサーバーをカスケード接続している場合でも、外部認証が完全に失敗する状況が発生する可能性があります。たとえば、外部サーバーに到達できなくなったり、新しいユーザーの資格情報がどの外部認証サーバーにも入力されていなかったりする場合があります。このような状況でユーザーがロックアウトされるのを防ぐために、フォールバックローカル認証を有効にできます。詳細については、「フォールバックローカル認証」を参照してください。

## フォールバックローカル認証とは何ですか?

フォールバックローカル認証は、外部認証が失敗した場合にユーザーをローカルで認証するオプションです。外部認証が失敗すると、NetScaler Console はローカルユーザーデータベースにアクセスしてユーザーを認証します。

NetScaler Console で、**設定 > 認証 > 認証設定** に移動します。このページで、複数の外部認証サーバーをカスケード接続で追加し、**フォールバックローカル認証を有効にする** オプションを選択できます。

## 外部ユーザーグループの抽出とは何ですか?

ユーザー認証のために外部サーバーを追加している場合、既存のユーザーグループを NetScaler Console にインポート（抽出）できます。個々のユーザーをインポートして個別の権限を付与するのではなく、ユーザーグループを一度インポートして、ユーザーグループにグループ権限を付与する必要があります。NetScaler Console でユーザーを再作成する必要はありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### グループ権限を割り当てる必要があるのはなぜですか?

NetScalerの負荷分散機能を使用している場合、NetScaler Consoleを外部認証サーバーと統合し、認証サーバーからユーザーグループ情報をインポートできます。NetScaler Consoleにログインし、NetScaler Consoleで同じグループ情報を手動で作成し、それらのグループに権限を割り当てます。ユーザーおよびユーザーグループの権限は、外部サーバーではなくNetScaler Consoleで管理されます。ユーザーは外部サーバー上で異なるロールベースのアクセス権限を持っています。NetScaler Consoleでもユーザーに同じ権限を設定します。各ユーザーに個別に権限を設定する代わりに、グループレベルの権限を設定して、ユーザーグループのメンバーが負荷分散された仮想サーバー上の特定のサービスにアクセスできるようにすることができます。割り当てることができる一般的な権限は、NetScalerインスタンス、NetScaler SDXインスタンス、仮想サーバーなどを管理する権限であり、そのグループのユーザーがそれらのインスタンスまたは仮想サーバーのみを管理できるようにします。後で、グループレベルでユーザーに与えられた権限を編集できます。1つ以上のユーザーグループを削除することもできます。他のグループユーザーはNetScaler Consoleで引き続き機能します。

## 構成管理

### NetScaler Consoleを使用して、複数のNetScalerインスタンス間で同時に構成を実行できますか?

はい、構成ジョブを使用して、複数のNetScalerインスタンス間で構成を実行できます。

### NetScaler Consoleの構成ジョブとは何ですか?

ジョブとは、1つ以上の管理対象インスタンスで作成および実行できる一連の構成コマンドです。ジョブを作成して、インスタンス間で構成変更を行ったり、ネットワーク上の複数のインスタンスで構成を複製したり、NetScaler Console GUIを使用して構成タスクを記録および再生したりできます。記録されたタスクをCLIコマンドに変換することもできます。

NetScaler Consoleの構成ジョブ機能を使用して、構成ジョブを作成し、電子メール通知を送信し、作成されたジョブの実行ログを確認できます。

### NetScaler Consoleの組み込みテンプレートを使用してジョブをスケジュールできますか?

はい！組み込みテンプレートオプションを使用してジョブをスケジュールできます。ジョブとは、1つ以上の管理対象インスタンスで実行できる一連の構成コマンドです。たとえば、組み込みテンプレートオプションを使用して、syslogサーバーを構成するジョブをスケジュールできます。ジョブをすぐに実行するか、後で実行するようにスケジュールするかを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以前に作成したジョブの構成を保存し、コマンド、パラメーター、構成ソース、およびターゲットインスタンスを変更した後で、そのジョブを再度実行できます。これは、同じ一連のコマンドを別のインスタンスで実行する必要がある場合や、ジョブがエラーに遭遇してそれ以上の実行を停止する場合に役立ちます。

# 証明書管理

## NetScaler ConsoleからSSL証明書を削除すると、NetScalerインスタンスからも証明書が削除されますか?

いいえ

# 展開

## デフォルトのユーザー名とパスワードは何ですか?

- 初期ネットワーク設定が完了したら、ハイパーバイザーまたはSSHコンソールから、デフォルトのユーザー名とパスワード（nsrecover/nsroot）を使用してNetScaler Consoleにログオンできます。
- GUIからログオンするためのデフォルトのユーザー名とパスワードは *nsroot/nsroot* です。

## デフォルトのパスワードを変更する方法?

**注：**

リリース14.1-8x以降、NetScaler Console GUIまたはAPIにデフォルトの資格情報で初めてログオンすると、デフォルトのパスワードを変更するよう求められます。

パスワードを変更するには：

1. NetScaler Consoleで、**Settings > User Administration > Users** に移動します。

   **Users** ページが表示されます。
2. ユーザー名 **nsroot** を選択し、**Edit** をクリックします。

   パスワードの編集(/en-us/netscaler-application-delivery-management-software/media/faq1.jpg)

   **Configure System User** ページが表示されます。
3. **Change Password** を選択し、任意のパスワードを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パスワードの変更(/en-us/netscaler-application-delivery-management-software/media/faq2.png)

4. **OK** をクリックします。

   これで、新しいパスワードを使用して、GUI、ハイパーバイザー、またはSSHコンソールからログオンできます。

   **注記:**

   ユーザー名を変更することはできません。

## パスワードをリセットする方法?

パスワードをリセットするには、このドキュメントを参照してください。

## HAペアで、プライマリノードのパスワードが変更され、その後「HAペアを解除」オプションが選択された場合、どのような動作になりますか?

新しいパスワードを使用して、両方のスタンドアロンノードにログオンできます。

## 2つのスタンドアロンサーバーが異なるパスワードを持っている場合、これら2つのサーバーをHAペアに展開する際の影響?

2つのスタンドアロンサーバーをHAペアに展開する際は、両方のサーバーでデフォルトのパスワードを使用することをお勧めします。

## HA構成は完了しましたが、プライマリノードのGUIにアクセスできません。原因は何か?

構成が有効になるまで数分かかります。数分後にもう一度アクセスしてみてください。

## HA構成は完了しましたが、フローティングIPアドレスのGUIにアクセスできません。考えられる原因?

HA構成後、まずプライマリノードのGUIにアクセスして展開を完了する必要があります。詳細については、高可用性ペアとしてプライマリノードとセカンダリノードを展開するを参照してください。展開が完了すると、サーバーは再起動し、高可用性展開の準備が整います。その後、フローティングIPアドレスのGUIにアクセスできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler ConsoleスタンドアロンとNetScaler Console HAでサポートされているDB?

NetScaler ConsoleスタンドアロンとNetScaler Console HAの両方がPostgreSQLをサポートしています。

## セカンダリノードへの潜在的なデータ損失?

セカンダリノードは、プライマリノードがNetScaler Consoleデータベースを介して送信するハートビートメッセージをリッスンします。セカンダリノードが180秒以上ハートビートを受信しない場合、セカンダリノードはプライマリノードに対してSSHベースのチェックを実行します。ハートビートとSSHベースのチェックが失敗した場合、プライマリノードはダウンしていると見なされます。

このシナリオでは、セカンダリノードがプライマリノードとして引き継ぎ、180秒という時間枠は、セカンダリノードへのデータ損失の可能性として考慮できます。

## プライマリノードがダウンした場合?

セカンダリノードが引き継ぎ、プライマリノードになります。

## 障害が発生したノードを再インストールする方法?

新しいVMビルドをインストールすることをお勧めします。再インストールするには：

1. HAペアを解除します。**Settings > Deployment** に移動します。

   展開ページが表示されます。**Break HA** をクリックします。
2. ハイパーバイザーから障害が発生したノードを削除します。
3. .XVAイメージファイルをハイパーバイザーにインポートします。
4. コンソールタブから、初期ネットワーク構成でNetScaler Consoleを設定します。詳細については、最初のサーバー（プライマリノード）を登録して展開する および 2番目のサーバー（セカンダリノード）を登録して展開する を参照してください。
5. HAペアを再展開する。

## NetScaler ConsoleはSANストレージをサポートしていますか?

NetScaler Console VHDはローカルストレージにホストすることをお勧めします。SAN内のストレージデバイスにホストされている場合、NetScaler Consoleは期待どおりに動作しない可能性があります。そのため、SANへのNetScaler Consoleの展開はサポートされていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler Consoleは追加ディスクをサポートしていますか?

はい。NetScaler Console HAペアの新規インストールでは、デフォルトで120 GBのストレージが割り当てられます。120 GBを超えるストレージの場合、最大3 TBのストレージ用に1つの追加ディスクを追加できます。複数の追加ディスクの追加はサポートされていません。

## HAペアを無効にした後、設定されているフローティングIPアドレスはどうなりますか?

フローティングIPアドレスはアクセスできなくなり、高可用性ペアを再展開する必要があります。

## 再展開時に別のフローティングIPアドレスを指定できますか?

はい。新しいフローティングIPアドレスを設定できます。

## セカンダリノードのGUIにアクセスできないのはなぜですか?

セカンダリノードは読み取り専用レプリカサーバーであり、何らかの理由でプライマリノードがダウンした場合にのみプライマリノードとして機能します。プライマリノードのGUIまたはフローティングIPアドレスのGUIにアクセスすることをお勧めします。

## プライマリノードが長期間ダウンした場合でも、フローティングIPアドレスのGUIを使用して構成を行うことはできますか?

はい。引き続き構成を行うことができ、構成はセカンダリノードに保存されます。プライマリノードが復旧すると、すべての構成が同期されます。

## 将来、プライマリノードのIPアドレス、セカンダリノードのIPアドレス、またはフローティングIPアドレスを変更する必要がある場合（たとえば、IPv6に変更する場合）、推奨される解決策は何ですか?

HAペアを解除せずにHAペアのIPアドレスを変更することはサポートされていません。

プライマリノードまたはセカンダリノードのIPアドレスを更新するには：

1. HAペアを解除します。**Settings > Deployment** に移動します。

   Deploymentページが表示されます。**Break HA** をクリックします。

   a. SSHクライアントまたはハイパーバイザーからプライマリノードにログオンします。

   b. `nsrecover` をユーザー名として使用し、設定したパスワードを入力します。

   c. **networkconfig**と入力します。最初のサーバー（プライマリノード）を登録して展開するで利用可能な**ステップ3**から手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

初期ネットワーク設定中に、別のIPアドレスを指定できます。

d. セカンダリノードに対しても同じ手順を実行し、2番目のサーバー（セカンダリノード）を登録して展開するで利用可能な**ステップ3**から手順を続行します。

フローティングIPアドレスを更新するには:

1. **Settings > Deployment**に移動します。

   Deploymentページが表示されます。

   a. **HA Settings**をクリックします。

   b. **高可用性モードのフローティングIPアドレスを設定**をクリックします。

   c. フローティングIPアドレスを入力し、**OK**をクリックします。

### NetScaler ConsoleはAMDプロセッサをサポートしていますか?

AMDプロセッサは以下でサポートされています:

- **NetScaler Console 13.1 ビルド 4.43 以降**。
- **NetScaler agent 13.1 build 17.42以降**。

## 展開（災害復旧）

### プライマリサイトとディザスタリカバリサイト間のレプリケーションはどのくらいの頻度で発生しますか?

プライマリサイトとディザスタリカバリサイト間のレプリケーションはリアルタイムで行われます。

### DRサイトでバックアップスクリプトを開始した後、プライマリサイトが復旧して完全に稼働するまで、DRサイトは一時的なプライマリサイトになりますか?

いいえ。DRサイトがプライマリサイトになります。HAペアを元のプライマリサイトに戻すには、「元のプライマリサイトに構成を戻す」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### HAペアの解除オプションが選択されている場合、両方のノードはスタンドアロンサーバーとして動作します。スタンドアロンサーバーにはDRサポートが適用されないため、HAペアの解除が選択された場合、DRサイトはどうなりますか?

HAペアの解除オプションを選択すると、プライマリサイトとDRサイト間のレプリケーションは終了します。HAペアの再展開の一部として、DRサイトを再構成する必要があります。

## イベント管理

### NetScaler Consoleを使用して、管理対象のNetScalerインスタンスで生成されたすべてのイベントを追跡するにはどうすればよいですか?

ネットワーク管理者として、NetScalerインスタンスでの構成変更、ログオン条件、ハードウェア障害、しきい値違反、エンティティの状態変更などの詳細を、特定のインスタンスでのイベントとその重大度とともに表示できます。NetScaler Consoleイベントダッシュボードを使用して、すべてのNetScalerインスタンスで生成された重大なイベントの重大度に関するレポートを表示できます。

### イベントルールとは何ですか?

NetScaler Consoleを使用して、特定のイベントを監視するためのルールを構成できます。イベントルールを使用すると、NetScaler Consoleインフラストラクチャ全体で生成される多くのイベントを簡単に監視できます。

特定の条件を持つルールを構成し、そのルールにアクションを割り当てることで、一連のイベントをフィルタリングできます。生成されたイベントがルールのフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。

フィルタを作成できる条件は、重大度、NetScalerインスタンス、カテゴリ、および障害オブジェクトです。イベントに割り当てることができるアクションは、電子メール通知の送信、管理対象NetScalerインスタンスからNetScaler ConsoleへのSNMPトラップの転送、およびSMS通知の送信です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# インスタンス管理

## NetScalerプール容量ライセンスを使用している場合、帯域幅割り当て後にNetScalerインスタンスがNetScaler Consoleに接続できないとどうなりますか?

NetScalerインスタンスとNetScaler Console間のハートビートが失敗した場合、インスタンスは30日間の猶予期間に入ります。通信が再確立されると、プールされたキャパシティライセンスが機能し始めます。猶予期間中は、NetScalerの機能に影響はありません。30日間の猶予期間が過ぎると、NetScalerインスタンスはウォームリスタートを開始し、ライセンスが解除されます。

## NetScaler Consoleにおけるデータセンターとは何ですか?

NetScaler Consoleのデータセンターとは、特定の地理的場所にあるNetScalerインスタンスの論理的なグループ化です。各サーバーは、データセンター内の複数のNetScalerインスタンスを監視および管理できます。NetScaler Consoleサーバーを使用して、管理対象インスタンスからのsyslog、アプリケーショントラフィックフロー、SNMPトラップなどのデータを管理できます。データセンターの構成の詳細については、「NetScaler Consoleでジオマップのデータセンターを構成する方法」を参照してください。

## NetScaler ConsoleでサポートされているNetScalerアプライアンスにはどのようなものがありますか?

インスタンスとは、NetScaler Consoleから検出、管理、監視したいNetScalerアプライアンスまたは仮想アプライアンスのことです。これらのインスタンスをNetScaler Consoleサーバーに追加する必要があります。NetScaler Consoleには、以下のNetScalerアプライアンスおよび仮想アプライアンスを追加できます。

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- ネットスケーラー ゲートウェイ

インスタンスは、NetScaler Consoleサーバーを初めてセットアップするとき、または後で追加できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## インスタンスプロファイルとは何ですか?

インスタンスプロファイルは、NetScaler Consoleがインスタンスにアクセスするために使用されます。

インスタンスプロファイルには、1つ以上のインスタンスにアクセスするためのユーザー名とパスワードが含まれています。各インスタンスタイプにはデフォルトプロファイルが用意されています。たとえば、ns-root-profileはNetScalerインスタンスのデフォルトプロファイルです。これには、デフォルトのNetScaler管理者資格情報が含まれています。インスタンスへのアクセスに必要な資格情報を変更する場合は、それらのインスタンス用にカスタムインスタンスプロファイルを定義できます。

## NetScaler Consoleで複数のNetScaler VPXインスタンスを再検出できますか?

はい、NetScaler Console で複数の Citrix **VPX** インスタンスを再検出して、インスタンスの最新の状態と構成を学習できます。

**Infrastructure > Instances > NetScaler > VPX** に移動し、再検出するインスタンスを選択し、**Action** リストで **Rediscover** をクリックします。詳細については、「複数のVPXインスタンスを再検出する方法」を参照してください。

## NetScaler Console は NetScaler SDX にインストールできますか?

いいえ

## パブリックIPアドレスを使用して、NetScaler Console ソフトウェアにNetScalerインスタンスを追加できますか?

はい、ネットワークアドレス変換 (NAT) を使用して追加できます。

- 単一インスタンスを追加する場合：NetScalerインスタンスのパブリックIPアドレスのNAT IPを使用します。
- NetScaler HAペアを追加する場合：HAペアのNAT IPアドレスを次の形式で追加します。

  `<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`
- NetScalerクラスターを追加する場合：クラスター内のすべてのインスタンスのNATパブリックIPアドレスをすべて追加し、それぞれをコンマで区切り、CLUSTER IPのNAT IPを括弧または丸括弧内に追加します。例：NAT1, NAT2, NAT3,(CLUSTERIPのNATIP)。

詳細については、以下のトピックを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console にインスタンスを追加する
- ネットワークアドレス変換の構成

### DRノードの資格情報が変更された場合、ディザスタリカバリノードを登録する方法?

次のコマンドを使用して、ディザスタリカバリ (DR) ノードの資格情報を `nsrecover` / `nsroot` にリセットします。

```
./mps/change_freebsd_password.sh <username> <password>
```

DRノードを登録するには、「DRコンソールを使用してNetScaler Console DRノードを展開および登録する」の手順に従います。

## StyleBook

### StyleBookを使用して、異なるバージョンのNetScalerソフトウェアで実行されている異なるNetScalerインスタンスを構成できますか?

はい、異なるバージョン間でコマンドに矛盾がない場合、StyleBookを使用して、異なるバージョンで実行されている異なるNetScalerインスタンスを構成できます。

### StyleBookを使用して複数のNetScalerインスタンスを同時に構成しているときに、1つのNetScalerインスタンスの構成が失敗した場合の動作?

NetScalerインスタンスへの構成の適用が失敗した場合、それ以上インスタンスに構成は適用されず、すでに適用された構成はロールバックされます。

### NetScalerを介して作成されたNetScalerバックアップにおけるStyleBook適用構成の有無?

はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# システム管理

## NetScaler Consoleサーバーにホスト名を割り当てることができます?

はい、NetScaler Consoleサーバーを識別するためにホスト名を割り当てることができます。ホスト名を割り当てるには、**System\> System Administration \> System Settings** に移動し、**Change Hostname** をクリックします。

ホスト名は、NetScaler Consoleのユニバーサルライセンスに表示されます。詳細については、「NetScaler Consoleサーバーにホスト名を割り当てる方法」を参照してください。

## NetScaler Consoleの構成をバックアップおよび復元できます?

はい、構成ファイル（NTPファイルとSSL証明書）、システムデータ、インフラストラクチャとアプリケーションデータ、およびすべての**SNMP**設定をバックアップできます。NetScaler Consoleが不安定になった場合でも、バックアップされたファイルを使用してNetScaler Consoleを安定した状態に復元できます。

NetScaler Consoleの構成をバックアップおよび復元するには、**「System」** > **「Advanced Settings」** > **「Backup Files」** に移動し、状況に応じて **「Back Up」** または **「Restore」** をクリックします。詳細については、「NetScaler Consoleで構成をバックアップおよび復元する方法」を参照してください。

アップグレードを実行する前、または予防措置として、この機能を使用することをお勧めします。

## NetScaler Consoleのしきい値とアラートとは何ですか?

NetScalerインスタンスの状態を監視し、管理対象インスタンス上のエンティティを監視するために、しきい値とアラートを設定できます。

カウンターの値がしきい値を超えると、NetScaler Consoleはパフォーマンス関連の問題を示すアラートを生成します。カウンター値がしきい値で指定されたクリア値に戻ると、イベントはクリアされます。

## NetScaler Consoleのテクニカルサポートファイルを生成できますか?

はい。問題のデバッグのためにテクニカルサポートに連絡する前に、NetScaler Consoleのデータと統計のアーカイブを生成することをお勧めします。アーカイブは、テクニカルサポートチームに送信できるTARファイルです。

デバッグログ、デバッグログが収集された期間、およびNetScaler Consoleデータベースからの明確で多様なログを含むテクニカルサポートファイルを生成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

テクニカルサポートファイルを設定して送信するには、**System** \> **Diagnostics** \> **Technical Support** に移動し、**Generate Technical Support File** をクリックします。詳細については、「NetScaler Consoleのテクニカルサポートファイルを生成する方法」を参照してください。

## syslogパージとは何ですか?

Syslogは、ロギングのための標準プロトコルです。Syslogは、情報を生成するシステムと情報を保存するシステムを分離することを可能にします。ロギング情報を統合し、収集されたデータから洞察を得ることができます。また、さまざまな種類のイベントをログに記録するようにsyslogを設定することもできます。

データベースに保存されるsyslogデータの量を制限するために、syslogデータをパージする間隔を指定できます。すべての汎用Syslogデータ、AppFirewallデータ、およびNetScaler GatewayデータがNetScaler Consoleから削除されるまでの日数を指定できます。

## NetScaler ConsoleでNTPサーバーを設定できますか?

NetScaler Consoleでネットワークタイムプロトコル（NTP）サーバーを設定して、NetScaler ConsoleのクロックをNTPサーバーと同期させることができます。NTPサーバーを設定することで、NetScaler Consoleのクロックがネットワーク上の他のサーバーと同じ日付と時刻設定を持つことが保証されます。

NTPサーバーを設定するには、**System** \> **NTP Servers** に移動し、**Add** をクリックします。詳細については、「NetScaler ConsoleでNTPサーバーを設定する方法」を参照してください。

## NetScaler Consoleのアクティブ/パッシブHA展開はどのバージョンからサポートされていますか?

NetScaler Consoleのアクティブ-パッシブHA展開モードは、NetScaler Consoleバージョン12.0ビルド51.24以降でサポートされています。

## NetScaler Consoleのアクティブ-アクティブHAセットアップがあり、統合GUIアクセス用にロードバランシング仮想サーバーを備えたNetScalerアプライアンスを構成していました。この構成を更新するにはどうすればよいですか?

NetScaler Console HAペアをアクティブ-パッシブモードにアップグレードした後、ロードバランシング構成を更新するために、NetScalerアプライアンスで次のコマンドを実行する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**lbモニターを追加** MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\\r\\nAccept-Encoding: identity\\r\\nUser-Agent: NetScaler-Monitor\\r\\nConnection: close\\r\\n\\r\\n\\""
-recv "{\\"statuscode\\":0, \\"is_passive\\":0}" -LRTM DISABLED**

## ポート443を使用したNetScalerインスタンス上でのNetScaler Console HAペアのロードバランシングの構成?

いいえ、ポート443を使用してNetScalerインスタンス上でNetScaler Console HAペアのロードバランシングを構成することはできません。

NetScalerで`http-ecv`と`https-ecv`モニターを構成すると、NetScaler Console HAノードが正しく監視されません。

## NetScaler Consoleサーバーのバックアップファイルを使用した別のNetScaler Consoleサーバーの構成の復元?

はい

## NetScaler ConsoleがNetScalerインスタンスをバックアップした後、そのバックアップファイルを使用して、NetScaler Consoleを介して別のNetScalerインスタンスの構成を復元できますか?

はい。NetScaler Consoleのバックアップファイルをダウンロードし、別のNetScalerインスタンスのバックアップリポジトリにアップロードして、そのインスタンスを復元します。ネットワーク情報と認証情報が競合しないことを確認してください。たとえば、IPアドレスやポートの競合、パスワードプロファイルの不一致などを確認します。また、復元されたVPXインスタンスが、バックアップされたインスタンスと同じNSIPアドレスとNetScalerライセンスを持っていることを確認してください。

高可用性ペアでインスタンスを復元する前に、バックアップファイルに保存されているIPアドレスと状態（プライマリまたはセカンダリ）が元のHA構成のものと一致していることを確認してください。また、新しいプライマリとセカンダリが同じ種類のNetScalerライセンスを持っていることも確認してください。

## NetScaler ConsoleサーバーのNSIPアドレスを使用する代わりに、SNIPアドレスを使用してNetScalerインスタンスと通信するようにNetScaler Consoleを強制できますか?

はい、NetScalerインスタンスとの通信のために、NetScaler ConsoleにSNIPアドレス（管理が有効になっているもの）を追加できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler ConsoleでNetScalerインスタンスをバックアップする場合、結果はフルバックアップですか、それともベーシックバックアップですか?

NetScaler ConsoleによるNetScalerインスタンスのバックアップは、フルバックアップです。

## NetScaler Consoleのトラブルシューティングガイドはありますか?

はい。`<https://support.citrix.com/article/CTX224502>`を参照してください。

## NetScaler Console HAフェイルオーバー発生時のNetScalerインスタンスの管理方法?

ハートビートおよびSSHベースのチェックが失敗した場合、プライマリノードはダウンしていると見なされ、セカンダリノードがプライマリノードとして引き継ぎます。すべてのNetScalerインスタンスは、デフォルトで最新のプライマリノードの詳細をSNMPトラップの宛先として更新されます。

新しいプライマリ（アクティブ）NetScaler Consoleノードは、以前アクティブだったノードがAppFlowコレクターまたはsyslogサーバーとして構成されていたかどうかを確認し、構成されていた場合は、新しいプライマリがAppFlowコレクターまたはsyslogサーバーの詳細をインスタンスに送信される情報に追加します。

syslogの場合、古いサーバーの詳細が置き換えられます。

## ダウンしたNetScaler Console HAノードが復旧した場合の動作?

サービスに復帰した後、NetScaler Consoleノードは、アクティブノードがフェイルオーバーしない限り、パッシブのままです。

## NetScalerインスタンスはNetScaler Console HAノード間でどのように分散されますか?

すべてのNetScalerインスタンスは、プライマリNetScaler Consoleノードによって管理されます。

## NetScaler Console HAフェイルオーバーが発生した場合、仮想サーバーライセンスはどのように管理されますか?

仮想サーバーライセンスが適用されているNetScaler Consoleプライマリノードがダウンした場合、新しいプライマリノードは30日間の猶予期間中、仮想サーバーライセンスを管理します。猶予期間が終了する前に、新しいプライマリにライセンスを再適用してください。代替策については、NetScalerサポートにお問い合わせください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler Console HAセットアップにはロードバランサーが必須ですか?

いいえ、必須ではありません。ただし、ロードバランサーがない場合、NetScaler Consoleノードはそれぞれの IPアドレスを介してアクセスする必要があります。パッシブノードには「Passive」というタグが付けられ、パッシブノードで構成を作成しないことをお勧めします。

パッシブノード(/en-us/netscaler-application-delivery-management-software/media/netscaler-mas-faq.png)

## NetScaler Consoleは外部データベースをサポートしていますか?

いいえ

## NetScaler Consoleによって管理されているNetScalerインスタンスを、NetScaler Console HAのロードバランサーとして使用できますか?

はい

## NetScaler Console HAノード間でどのようなデータが同期されますか?

NetScaler Consoleデータベース全体が同期され、次のフォルダーが同期されます。

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# index


- しきい値とアラートを作成する
- Logstream の概要
- ダッシュボード
- すべての違反
- アプリケーションの概要
- NetScalerインスタンスのバックアップと復元
- ネットワーク違反の詳細
- SSL インサイト
- Web Insight の問題のトラブルシューティング
- Webトランザクションの分析を表示
- デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順
- サービスメッシュトポロジを設定するための詳細な手順
- シングルティアまたは統合イングレストポロジを設定するための詳細な手順
- データガバナンス (NetScaler Console の 14.1-8.x から 14.1-21.x ビルド向け)
- データガバナンス (NetScaler ADM 14.1-4.42 またはそれ以前のビルドの場合)
- Cloud Connect 用のオプションのテレメトリデータ
- NetScaler® Telemetry プログラムのオプションのテレメトリデータ
- Cloud Connect に必要なテレメトリーデータ
- NetScaler® テレメトリプログラムに必要なテレメトリデータ
- ライセンス
- システム通知設定を構成する


## しきい値とアラートを作成する

NetScalerインスタンスの状態を監視するために、しきい値とアラートを設定できます。カウンターにしきい値を設定し、管理対象インスタンス上のインスタンスとエンティティを監視できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カウンターの値がしきい値を超えると、NetScaler Consoleはパフォーマンス関連の問題を示すイベントを生成します。カウンターの値がしきい値で指定されたクリア値と一致すると、イベントはクリアされ、その特定のしきい値が通常の状態に戻ったことを意味します。

しきい値にアクションを関連付けることもできます。アクションには、アラート、電子メール、またはSMS通知の送信が含まれます。しきい値が侵害されると、NetScaler Consoleは、アラートの有効化や電子メールまたはSMS通知の送信など、定義したアクションを自動的に実行します。

### NetScaler Consoleを使用してしきい値とアラートを作成するには

1. **System** \> **Analytics Settings** \> **Thresholds** に移動します。**Thresholds** の下で、**Add** をクリックします。
2. **Create Thresholds and Alerts** ページで、次の詳細を指定します。
   - **名前** – しきい値を設定するための名前。
   - **トラフィックタイプ** – しきい値を設定するトラフィックのタイプ。
   - **エンティティ** – しきい値を設定するカテゴリまたはリソースタイプ。
   - **参照キー** – 選択したトラフィックタイプとエンティティに基づいて自動的に生成される値。
   - **期間** - しきい値を設定する間隔。
   - **コミュニティ** – トラップリスナーに送信される各トラップのコミュニティ文字列。
3. オプションで、アラート、電子メール通知、SMS通知などのアクションを設定します。
4. **Create** をクリックします。

HDX™ Insightの場合、設定されたしきい値内のすべてのエンティティが侵害された場合にのみアラートが生成されるように、複数のしきい値を設定することもできます。

## Logstream の概要

NetScalerインスタンスはAppFlowレコードを生成し、データセンター内のすべてのアプリケーショントラフィックを制御する中心点となります。IPFIXとLogstreamは、これらのAppFlowレコードをNetScalerインスタンスからNetScaler Consoleに転送するプロトコルです。詳細については、AppFlowを参照してください。

- IPFIXは、RFC 5101で定義されているオープンなInternet Engineering Task Force (IETF) 標準です。IPFIXは、一方向のデータフローに使用される信頼性の低いトランスポートプロトコルであるUDPプロトコルを使用します。IPFIXはUDPプロトコルを使用するため、IPFIX標準に準拠すると、NetScaler Consoleでより多くのリソースを処理することになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Logstreamは、Citrixが所有するプロトコルであり、NetScalerインスタンスからNetScaler Consoleに分析ログデータを効率的に転送するためのトランスポートモードの1つとして使用されます。Logstreamは信頼性の高いTCPプロトコルを使用し、データの処理に必要なリソースが少なくて済みます。

NetScaler **11.1 Build 47.14から11.1 Build 62.8**の場合、LogstreamはWeb Insight (HTTP) を有効にするためのデフォルトのトランスポートモードであり、IPFIXは他のインサイトを有効にするための唯一のトランスポートモードです。NetScalerバージョン**12.0から最新バージョン**では、トランスポートモードとして**Logstream**または**IPFIX**のいずれかを選択できます。

## Logstreamをトランスポートモードとして有効にする

1. **インフラストラクチャ > インスタンス**に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. **アクションの選択**リストから、**分析の構成**を選択します。

   
3. 仮想サーバーを選択し、**分析を有効にする**をクリックします。

   
4. **分析を有効にする**ウィンドウで:

   a. インサイトの種類 (Web InsightまたはWAFセキュリティ違反) を選択します。

   b. トランスポートモードとして**Logstream**を選択します。

   > **注**
   >
   > NetScalerの**11.1 Build 47.14から11.1 Build 62.8**のバージョンでは、LogstreamがWeb Insight (HTTP) を有効にするためのデフォルトのトランスポートモードであり、IPFIXは他のインサイトを有効にするための唯一のトランスポートモードです。NetScalerの**12.0から最新バージョン**では、トランスポートモードとして**Logstream**または**IPFIX**のいずれかを選択できます。

   c. 式はデフォルトでtrueです

   d. **OK**をクリックします

   分析を有効にする(/en-us/netscaler-application-delivery-management-software/media/enabling-analytics1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

- ライセンスが付与されていない仮想サーバーを選択した場合、NetScaler Consoleはまずそれらの仮想サーバーにライセンスを付与し、その後分析を有効にします
- 管理パーティションでは、**Web Insight**のみがサポートされています
- キャッシュリダイレクション、認証、GSLBなどの仮想サーバーでは、分析を有効にできません。エラーメッセージが表示されます

次の表は、Logstreamをトランスポートモードとしてサポートする NetScaler Consoleの機能について説明しています。

| 機能 | IPFIX | ログストリーム |
|---|---|---|
| ウェブインサイト | • | • |
| WAFセキュリティ違反 | • | • |
| ゲートウェイインサイト | • | • |
| HDXインサイト | • | • |
| SSLインサイト | サポートされていません | • |
| CRインサイト | • | • |
| IPレピュテーション | • | • |
| AppFirewall | • | • |
| クライアント側測定 | • | • |
| Syslog/Auditlog | • | • |

# ダッシュボード

NetScaler Consoleは、**アウトバウンドトラフィックダッシュボード**と**ユーザーダッシュボード**の2つのダッシュボードを提供します。これらのダッシュボードには、企業ネットワークからアクセスされたウェブサイトやアプリケーション、およびネットワーク内のユーザーによって実行されたアクティビティを要約する複数のグラフが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# アウトバウンドトラフィックダッシュボード

**アウトバウンドトラフィックダッシュボード**は、ネットワークからアクセスされたURLまたはドメインの概要を提供します。トランザクション数またはURLやドメインによって消費されたデータ量に基づいて、すべてのURLまたはドメインの全体像を提供します。 また、次のような詳細も提供します。

1. ネットワークからアクセスされたURLまたはドメインによって消費された帯域幅の量。
2. ネットワークからURLおよびドメインにアクセスする際に発生したトランザクション数。
3. トランザクション中にNetScalerアプライアンスによって傍受されたSSL接続数。
4. トランザクション中にNetScalerアプライアンスによって傍受されなかったSSL接続数。
5. トランザクション中にNetScalerアプライアンスによってリセットされたSSL接続数。
6. トラフィックの送信に使用されたポート、ウェブトラフィックによって使用されたプロトコル、およびトラフィックの送信に使用されたクライアントオペレーティングシステムに基づいて送信されたウェブトラフィックの量。

アウトバウンドトラフィックダッシュボードにアクセスするには、**Applications \> Outbound Traffic Dashboard**に移動します。

### ネットワークからのアウトバウンドトラフィックを表示する

**アウトバウンドトラフィックダッシュボード**には、**アウトバウンドトラフィック概要**ペインが含まれています。**アウトバウンドトラフィック概要**ペインでは、NetScaler ConsoleはアクセスされたURLまたはドメインを、ショッピング、ニュース、ソーシャルネットワーキングなどのカテゴリにグループ化します。**アウトバウンドトラフィック概要**ペインには、ネットワークからアクセスされたURLまたはドメインがURLカテゴリ内のノードとして表示されます。ノードのサイズは、URLまたはドメインへのアクセスによって消費されたデータ量に応じて決定されます。ノードの色は、URLまたはドメインへのアクセス中に発生したトランザクション数を示します。

カテゴリをクリックすると、指定した期間のカテゴリに関連する詳細を表示するようにグラフをフィルタリングできます。

# ユーザーダッシュボード

**ユーザーダッシュボード**には、企業内のユーザーが実行したアクティビティの概要が表示されます。以下のことを判断するために使用できる主要なメトリックが提供されます。

1. 企業内のユーザーの閲覧行動。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 企業内のユーザーがアクセスしたURLカテゴリ。
3. リスクスコアと消費帯域幅に基づいた上位5人のユーザー。リスクスコアの詳細については、「リスクスコア」を参照してください。
4. URLまたはドメインへのアクセスに使用されたブラウザ。
5. トラフィックレピュテーションスコアに基づいた、ユーザーによって生成されたウェブトラフィック量。

**ユーザーダッシュボード**にアクセスするには、**ユーザー \> ダッシュボード**に移動します。



**トップユーザー**ペインでユーザーをクリックすると、指定した期間にそのユーザーが実行したウェブアクティビティの詳細を表示するようにグラフをフィルタリングできます。

### ユーザーアクティビティインベスティゲーター

**ユーザーダッシュボード**には、ユーザーが実行したさまざまなウェブアクティビティを表示する**ユーザーアクティビティインベスティゲーター**ペインが含まれています。選択した期間中にユーザーがアクセスしたURLカテゴリと、URLカテゴリごとにトリガーされたさまざまなイベントが表示されます。イベントをクリックすると、トランザクションレベルの詳細を取得できます。

**ユーザーアクティビティインベスティゲーター**は、ユーザーの閲覧行動、ユーザーによる高リスクアクティビティ、トリガーされたイベントなど、URLカテゴリごとの主要な情報を表示します。イベントはグラフ上に長方形の凡例として表示されます。選択した期間が1時間の場合、各凡例は1分間隔で集計され、選択した期間が1日の場合、1時間間隔で集計されます。



これらの凡例は集計され、発生したイベントの数に応じて色分けされています。凡例にマウスポインターを合わせると、時間や選択した凡例に集計されたイベントの数などの詳細が表示されます。時間期間リストから時間を選択することで、グラフの時間期間をカスタマイズできます。

イベントをクリックすると、トランザクションの詳細をさらにドリルダウンできます。

### ユーザー トランザクション

ページには、ネットワーク内のユーザー トランザクションの詳細が表示されます。トランザクションレベルの詳細は次のとおりです。

1. トランザクションが発生した時刻
2. トランザクションに使用されたプロトコル
3. ユーザー名
4. ユーザーがアクセスしたドメイン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. URL カテゴリ
6. トランザクションを傍受するために使用されたプロキシサーバー
7. クライアントポートの詳細
8. 受信バイト数
9. 送信バイト数



**概要パネル**

**サマリーパネル**には、**トランザクションの詳細**ペインに表示されるトランザクションのすべてのメトリックが表示されます。このパネルでは、メトリックを選択または選択解除することで、**トランザクションの詳細**ペインのトランザクションをソートして表示できます。**サマリーパネル**には、次のメトリックが表示されます。

| メトリック | 説明 |
|---|---|
| プロトコル | トランザクションで使用されるプロトコル |
| ポート | トランザクションに使用されるポート |
| URLレピュテーション | URLレピュテーションスコア |
| ブラウザ | トランザクションに使用されるブラウザ |
| オペレーティングシステム | トランザクションに使用されるオペレーティングシステム |
| 受信バイト数 | NetScaler Appliance を介して受信されたデータ量。 |
| 送信バイト数 | NetScaler Appliance を介して送信されたデータ量。 |

## リスクスコア

リスクスコアは、NetScaler Console で使用されるスコアリングシステムで、企業内のユーザーに関連するリスクを判断します。NetScaler Console は、ネットワーク内のユーザーがアクセスした URL に対して NetScaler アプライアンスによって割り当てられた URL レピュテーションスコアに基づいてリスクスコアを割り当てます。URL レピュテーションスコアの詳細については、「URL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レピュテーションスコア」を参照してください。次の表に、NetScaler Console によって割り当てられるリスクスコアについて説明します。

| リスクスコア | 説明 |
| --- | --- |
| 1 | ユーザーのWebアクティビティには、認識された脅威がなく、異常ではありません。 |
| 2 | ユーザーのWebアクティビティには、認識された脅威がなく、異常ではありませんが、ユーザーはURLレピュテーションスコアを持たない「不明なサイト」にアクセスしています。 |
| 3 | ユーザーのWebアクティビティで脅威は検出されませんが、ユーザーは潜在的に脆弱なサイト、または潜在的に脆弱なサイトに関連するサイトへのアクセスを試みました。 |
| 4 | 侵害される可能性のあるユーザー。 |
| 5 | ユーザーのWebアクティビティは異常であり、既知の悪意のあるサイトにアクセスしています。 |

# すべての違反

「**すべての違反**」ページには、**ネットワーク**、**WAF**、**ボット**のカテゴリに基づいて、アプリケーションセキュリティ違反の詳細が表示されます。

## 違反カテゴリ

NetScaler Consoleでは、以下の違反を表示できます。「**違反の詳細**」で、各違反タブをクリックすると、違反の詳細を表示できます。

| ネットワーク | WAF | ボット |
| --- | --- | --- |
| **HTTP スローロリス** | CSRFフォームタグ付け | マーケティング |
| **DNS スローロリス** | URL拒否 | スクレイパー |
| **HTTP スローポスト** | フォームフィールドの一貫性 | スクリーンショット作成者 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ネットワーク | WAF | ボット |
|---|---|---|
| **NXDomain フラッド攻撃** | フィールド形式 | 検索エンジン |
| **HTTP デシンク攻撃** | クッキーハイジャック | フィードフェッチャー |
| **Bleichenbacher アタック** | コンテンツタイプXMLの推測 | リンクチェッカー |
| **セグメントスマック攻撃** | バッファオーバーフロー | サービスエージェント |
| **SYN フラッド攻撃** | コンテンツタイプ | サイトモニター |
| **スモールウィンドウ攻撃** | Cookieの一貫性 | スピードテスター |
| | セーフオブジェクト | ツール |
| | HTML SQLインジェクション | 未分類 |
| | 開始URL | ウイルススキャナー |
| | クロスサイトスクリプティング | 脆弱性スキャナー |
| | XML DoS | DeviceFP待機時間超過 |
| | XML形式 | 不正なDeviceFP |
| | XML WSI | 無効なCAPTCHA応答 |
| | XML SSL | CAPTCHA試行回数超過 |
| | XML添付ファイル | 有効なCAPTCHA応答 |
| | XML SOAP障害 | CAPTCHAクライアントミュート |
| | XML検証 | CAPTCHA待機時間超過 |
| | その他 | リクエストサイズ制限超過 |
| | IPレピュテーション | レート制限超過 |
| | HTTP DOS | ブロックリスト (IP、サブネット、ポリシー式) |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| ネットワーク | WAF | ボット |
| --- | --- | --- |
| | TCPスモールウィンドウ | 許可リスト (IP、サブネット、ポリシー式) |
| | シグネチャ違反 | ゼロピクセルリクエスト |
| | ファイルアップロードタイプ | 送信元IP |
| | JSONクロスサイトスクリプティング | ホスト |
| | JSON SQL | ジオロケーション |
| | JSON DOS | URL |
| | コマンドインジェクション | クローラー |
| | 最大アップロード数 | |
| | リファラーヘッダー | |
| | セーフコマース | |

## セキュリティ違反ダッシュボード

セキュリティ違反ダッシュボードでは、以下を表示できます。

- すべてのNetScalerインスタンスとアプリケーションで発生した合計違反数。合計違反数は、選択した期間に基づいて表示されます。
- 合計違反数。
- 影響を受けたNetScalerインスタンスの合計数、影響を受けたアプリケーションの合計数、および合計発生数と影響を受けたアプリケーションに基づく上位の違反。

## 違反の詳細

各違反について、NetScaler Consoleは特定の期間の動作を監視し、異常な動作の違反を検出します。各タブをクリックして、違反の詳細を表示します。次のような詳細を表示できます。

- 合計発生数、最終発生日時、および影響を受けたアプリケーションの合計数。
- イベントの詳細では、以下を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 影響を受けたアプリケーション。2つ以上のアプリケーションが違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- 違反を示すグラフ。

  違反を一覧表示するグラフ上でドラッグして選択し、違反検索を絞り込みます。

| グラフ上でドラッグして選択 | 検索結果 |
| --- | --- |
|  |  |

  ズーム結果をリセットするには、**ズームのリセット**をクリックします。
- 問題のトラブルシューティングを提案する**推奨されるアクション**。
- 違反発生時刻や検出メッセージなど、その他の違反の詳細。

# アプリケーションの概要

**アプリケーションの概要**ページには、WAFセキュリティ違反とボットセキュリティ違反の両方に関連する脅威の詳細が完全に可視化されたアプリケーションが表示されます。また、合計違反数、WAFおよびボットの合計違反数、国別の違反などの情報も表示できます。

アプリケーションの概要(/en-us/netscaler-application-delivery-management-software/media/app-overview1.png)

**1** – 選択した期間における、影響を受けたアプリケーションの合計数、合計違反数、WAF違反の合計数、およびボット違反の合計数を表示します。

**2** – WAFおよびボットの違反の詳細を表示します。**WAF**タブと**Bot**タブをクリックすると、発生した合計違反数に基づいた上位5つのアプリケーションが表示されます。**すべて表示**をクリックすると、すべてのアプリケーションの詳細が表示されます。

**3** – 発生回数と適用されたアクションに基づいた上位の違反を表示します。

**4** – 違反が発生した場所を可視化する地理マップビューを表示します。

**5** – 違反に基づいた情報を提供します。

## 違反カテゴリ

| WAF | ボット |
| --- | --- |
| クッキーハイジャック | フィードフェッチャー |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| WAF | ボット |
| --- | --- |
| コンテンツタイプXMLの推測 | リンクチェッカー |
| CSRFフォームタグ付け | マーケティング |
| URL拒否 | スクレイパー |
| フォームフィールドの一貫性 | スクリーンショット作成者 |
| フィールド形式 | 検索エンジン |
| 最大アップロード数 | サービスエージェント |
| リファラーヘッダー | サイトモニター |
| セーフコマース | スピードテスター |
| セーフオブジェクト | ツール |
| HTML SQLインジェクション | 未分類 |
| 開始URL | ウイルススキャナー |
| クロスサイトスクリプティング | 脆弱性スキャナー |
| XML DoS | DeviceFP待機時間超過 |
| XML形式 | 無効なDeviceFP |
| XML WSI | 無効なCAPTCHA応答 |
| XML SSL | CAPTCHA試行回数超過 |
| XML添付ファイル | 有効なCAPTCHA応答 |
| XML SOAP障害 | CAPTCHAクライアントミュート |
| XML検証 | CAPTCHA待機時間超過 |
| その他 | リクエストサイズ制限超過 |
| IPレピュテーション | レート制限超過 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| WAF | ボット |
| --- | --- |
| HTTP DOS | ブロックリスト（IP、サブネット、ポリシー式） |
| TCPスモールウィンドウ | 許可リスト（IP、サブネット、ポリシー式） |
| シグネチャ違反 | ゼロピクセルリクエスト |
| ファイルアップロードタイプ | 送信元IP |
| JSONクロスサイトスクリプティング | ホスト |
| JSON SQL | 地理的位置 |
| JSON DOS | URL |
| コマンドインジェクション | クローラー |
| バッファオーバーフロー | |
| コンテンツタイプ | |
| クッキーの一貫性 | |

## WAF違反の詳細を表示

WAFの詳細を表示するには、「**Top Applications**」または「**View All**」オプションからアプリケーションをクリックします。

選択したアプリケーションの「**Security Overview**」ページが表示されます。「**WAF**」の下に、以下が表示されます。

- アプリケーションの合計違反数、脅威インデックススコア、安全インデックススコアを示すグラフビュー。

  「**View Details**」をクリックして、Application FirewallとNetScaler System Securityの設定詳細を表示します。

- タイプ、重大度、および適用されたアクションに基づく違反。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「**Logs**」をクリックして、重大度または実行されたアクションに基づいて詳細を表示します。

- アプリケーションに影響を与えた違反。「**Violation Details**」の下に、影響を受けた違反の詳細が表示されます。各違反をクリックすると、次のような詳細が表示されます。
  - 「**What Happened**」 – 合計発生回数と最終発生日時を示します。
  - 「**Event Details**」 – クライアントIPと、違反タイプ、クライアントIP、場所などのその他の違反詳細を示すジオマップが表示されます。

## ボット違反の詳細を表示

**Bot**タブから、または****オプションからアプリケーションをクリックして、ボットの詳細を表示します。

ボットの詳細(/en-us/netscaler-application-delivery-management-software/media/bot-details.png)

選択したアプリケーションの**セキュリティ概要**ページが表示されます。**ボット**の下に、以下が表示されます。

- 合計ボット数、合計不良ボット数、合計優良ボット数、およびアプリケーションにアクセスしている人間ユーザーとボットの合計比率を示すグラフ。

  ボットグラフ(/en-us/netscaler-application-delivery-management-software/media/bot-graph-details.png)
- ボットの種類、重大度、および適用されたアクションに基づく違反。

  ボット違反の種類(/en-us/netscaler-application-delivery-management-software/media/bot-violations-types.png)

  **ログ**をクリックすると、重大度または実行されたアクションに基づいて詳細が表示されます。検出されたボットがシグネチャタイプのボットである場合、ボット開発者やシグネチャIDなどの詳細を表示できます。シグネチャIDを使用すると、検出されたボットが優良ボットか不良ボットかを識別できます。

  ボットログ(/en-us/netscaler-application-delivery-management-software/media/bot-logs.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

検出されたボットがシグネチャボット以外のボットタイプである場合、シグネチャIDとボット開発者はN/Aと表示されます。

N/Aタイプ(/en-us/netscaler-application-delivery-management-software/media/na-log-bot.png)

- アプリケーションに影響を与えた違反。違反の詳細の下に、影響を受けた違反の詳細が表示されます。各違反をクリックすると、次のような詳細が表示されます。
  - **何が起こったか** – 合計発生回数と最終発生日時を示します。
  - **イベントの詳細** – クライアントIP、違反タイプ、クライアントIP、場所などの違反の詳細を示す地理マップを表示します。

**注**

**WAF**および**Bot**の下で、ロードバランシング仮想サーバーにバインドされているコンテンツスイッチング仮想サーバーの分析を表示できます。コンテンツスイッチング仮想サーバーをクリックし、**バインドされたロードバランシングサーバー**の下で、コンテンツスイッチング仮想サーバーにバインドされているロードバランシングサーバーのリストを表示できます。

### イベント履歴の表示

**イベント**タブをクリックして、ボットおよびWAFイベントを表示します。

## NetScalerインスタンスのバックアップと復元

NetScalerインスタンスの現在の状態をバックアップし、後でバックアップファイルを使用して同じ状態に復元できます。インスタンスをアップグレードする前、または予防措置として、常にバックアップしてください。安定したシステムのバックアップがあれば、不安定になった場合に安定した時点に復元できます。

NetScalerインスタンスでバックアップと復元を実行する方法は複数あります。GUIとCLIを使用して、NetScaler構成を手動でバックアップおよび復元できます。NetScaler Consoleを使用して、自動バックアップと手動復元を実行することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleは、NITROコール、Secure Shell (SSH)、およびSecure Copy (SCP) プロトコルを使用して、管理対象のNetScalerインスタンスの現在の状態をバックアップします。

NetScaler Consoleは、以下のNetScalerインスタンスタイプの完全なバックアップを作成し、復元します。

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

**注記:**

- NetScaler Consoleプロファイルに、NetScalerインスタンスをバックアップおよび復元するための管理者アクセス権があることを確認してください。
- NetScaler Consoleから、NetScalerクラスターに対してバックアップおよび復元操作を実行することはできません。
- あるインスタンスから取得したバックアップファイルを使用して、別のインスタンスを復元することはできません。

バックアップファイルは、次のディレクトリに圧縮されたTARファイルとして保存されます:

```
/var/mps/tenants/root/device_backup/
```

ディスク容量不足による問題を回避するため、このディレクトリには、NetScalerインスタンスごとに最大50個のバックアップファイルを保存できます。

NetScalerインスタンスをバックアップおよび復元するには、まずNetScaler Consoleでバックアップ設定を構成する必要があります。設定を構成した後、単一のNetScalerインスタンスまたは複数のインスタンスを選択し、これらのインスタンス内の構成ファイルのバックアップを作成できます。必要に応じて、これらのバックアップされたファイルを使用してNetScalerインスタンスを復元することもできます。

## インスタンスのバックアップ設定を構成する

**インスタンスバックアップ設定**ページでは、選択したNetScalerインスタンスまたは複数のインスタンスをバックアップするための設定をNetScaler Consoleで構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**設定** \> **管理**に移動します。
2. **バックアップ**で、**システムとインスタンスのバックアップを構成**を選択します。
3. **インスタンス**を選択し、以下を指定します。

- **インスタンスバックアップを有効にする**: デフォルトでは、NetScaler ConsoleはNetScalerインスタンスのバックアップを取得するように有効になっています。インスタンスのバックアップファイルを作成しない場合は、このオプションをオフにします。
- **ファイルをパスワードで保護**: (オプション) バックアップファイルを暗号化するには、パスワード保護オプションを選択します。バックアップファイルを暗号化することで、バックアップファイル内のすべての機密情報が安全に保たれます。

  **注:**

  暗号化されたバックアップファイルはローカルマシンにダウンロードできますが、NetScaler Console GUIまたは任意のテキストエディタでファイルを開くことはできません。暗号化されたバックアップファイルを復元する際には、パスワードの入力を求められます。ただし、暗号化されていないバックアップファイルはシステムで開くことができます。

- **保持するバックアップファイルの数**: NetScaler Consoleで保持するバックアップファイルの数を指定します。NetScalerインスタンスごとに最大50個のバックアップファイルを保持できます。デフォルトは3個のバックアップファイルです。

  **注:**

  各バックアップファイルは、ある程度のストレージ要件を占めます。お客様の要件に応じて、最適な数のNetScalerバックアップファイルをNetScaler Consoleに保存することをお勧めします。

  インスタンスバックアップを指定する(/en-us/netscaler-application-delivery-management-software/media/configure-instance-backup-settings.png)

- **バックアップスケジュール設定**: (オプション) バックアップファイルを作成するためのオプションは2つありますが、一度に1つのオプションしか使用できません。

  a. デフォルトのバックアップスケジュールオプションは「間隔ベース」です。指定された間隔が経過すると、NetScaler Consoleにバックアップファイルが作成されます。デフォルトのバックアップ間隔は12時間です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. スケジュールされたバックアップの種類を「時間ベース」に変更することもできます。このオプションでは、`hours:minutes`形式で時間を指定して、指定された時間にインスタンスをバックアップします。NetScaler Consoleでは、インスタンスに対して1日あたり最大4回のバックアップが可能です。

- **NetScaler設定**: (オプション) デフォルトでは、NetScaler Consoleは「NetScalerConfigSave」トラップを受信してもバックアップファイルを作成しません。しかし、NetScalerインスタンスが「NetScalerConfigSave」トラップをNetScaler Consoleに送信するたびにバックアップファイルを作成するオプションを有効にできます。NetScalerインスタンスは、インスタンスの構成が保存されるたびに「NetScalerConfigSave」を送信します。
- **Geoデータベースファイル**: (オプション) デフォルトでは、NetScaler ConsoleはGeoデータベースファイルをバックアップしません。これらのファイルのバックアップを作成するオプションも有効にできます。
- **外部転送:**(オプション) NetScaler Consoleでは、NetScalerインスタンスのバックアップファイルを外部の場所に転送できます。

a. 場所のIPアドレスを指定します。
b. バックアップファイルを転送する外部サーバーのユーザー名とパスワードを指定します。
c. 転送プロトコルとポート番号を指定します。
d. ファイルを保存するディレクトリパスを指定できます。
e. オプションで、外部サーバーに転送した後、NetScaler Consoleからバックアップファイルを削除することもできます。

**注:**

選択したNetScalerインスタンスのいずれかでバックアップに失敗した場合、NetScaler ConsoleはSNMPトラップまたはSyslog通知を自身に送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Console を使用して、選択した NetScaler インスタンスのバックアップを作成する

選択した NetScaler インスタンスまたは複数のインスタンスをバックアップする場合は、このタスクを実行します。

1. NetScaler Console で、**Infrastructure > Instances** に移動します。**Instances** の下で、画面に表示するインスタンスのタイプ (例: NetScaler VPX) を選択します。
2. バックアップするインスタンスを選択します。
   - MPX、VPX、および BLX インスタンスの場合は、**Select Action** リストから **Backup/Restore** を選択します。
   - SDX インスタンスの場合は、**Backup/Restore** をクリックします。
3. **Backup Files** ページで、**Back Up** をクリックします。
4. セキュリティを強化するために、バックアップファイルを暗号化するかどうかを指定できます。パスワードを入力するか、Instance Backup Settings ページで以前に指定したグローバルパスワードを使用できます。
5. **Continue** をクリックします。

## NetScaler Console を使用して NetScaler インスタンスを復元する

**注:**

HA ペアに NetScaler インスタンスがある場合は、次の点に注意する必要があります。

- バックアップファイルが作成されたのと同じインスタンスを復元します。たとえば、HA ペアのプライマリインスタンスからバックアップが取得されたシナリオを考えてみましょう。復元プロセス中に、たとえそれがプライマリインスタンスでなくなったとしても、同じインスタンスを復元していることを確認してください。
- プライマリ NetScaler インスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできなくなり、セカンダリインスタンスは **STAYSECONDARY** に変更されます。プライマリインスタンスでの復元プロセスが完了すると、セカンダリ NetScaler インスタンスは **STAYSECONDARY** から **ENABLED** モードに変わり、再び HA ペアの一部になります。復元プロセスが完了するまで、プライマリインスタンスでダウンタイムが発生する可能性があります。

以前に作成したバックアップファイルを使用して NetScaler インスタンスを復元するには、このタスクを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**Infrastructure > Instances**」に移動し、復元するインスタンスを選択して、「**Select Action > Backup/Restore**」をクリックします。

   バックアップファイルを表示(/en-us/netscaler-application-delivery-management-software/media/configure-instance-backup-restore.jpg)

2. 「**Backup Files**」ページで、復元する設定を含むバックアップファイルを選択し、「**Restore**」をクリックします。

   バックアップファイルを復元(/en-us/netscaler-application-delivery-management-software/media/restore-backup-instance.jpg)

**注：**

外部から転送されたバックアップファイルをアップロードするには、「**Upload**」ボタンを使用します。

### NetScaler Console を使用して NetScaler SDX アプライアンスを復元する

NetScaler Console では、NetScaler SDX アプライアンスのバックアップには次のものが含まれます。

- アプライアンスでホストされているNetScalerインスタンス
- SVM SSL証明書とキー
- インスタンスのプルーニング設定（XML形式）
- インスタンスのバックアップ設定（XML形式）
- SSL証明書ポーリング設定（XML形式）
- SVM dbファイル
- SDX上に存在するデバイスのNetScaler構成ファイル
- NetScalerビルドイメージ
- NetScaler XVAイメージ。これらのイメージは次の場所に保存されます。 `/var/mps/sdx_images/`
- SDXシングルバンドルイメージ (SVM+XS)
- サードパーティインスタンスイメージ (プロビジョニングされている場合)

NetScaler SDXアプライアンスを、バックアップファイルで利用可能な構成に復元します。アプライアンスの復元中に、現在の構成全体が削除されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

別のNetScaler SDXアプライアンスのバックアップを使用してNetScaler SDXアプライアンスを復元する場合は、復元プロセスを開始する前に、ライセンスを追加し、新しいアプライアンスの管理サービスネットワーク設定をバックアップファイルの設定と一致するように構成してください。つまり、新しいアプライアンスはライセンスが付与されており、バックアップファイルの最小ライセンス要件を満たしている必要があります。たとえば、バックアップに合計5 GBの5つのVPXインスタンスがあった場合、新しいアプライアンスもこれらの要件をサポートできる必要があります。または、バックアップアプライアンスがプラチナライセンスを持っていた場合、新しいアプライアンスは同じかそれ以上のライセンスを持っている必要があります。IPアドレス、ネットマスク、ゲートウェイ、XenServer IPアドレス、DNSサーバーなどのネットワーク設定は、新しいアプライアンスで適切に構成されている必要があります。

SDXアプライアンスを復元する前に、バックアップされたSDXアプライアンスのプラットフォームバリアントが現在のアプライアンスと同じであることを確認してください。異なるプラットフォームバリアントから復元することはできません。

**注:**

SDX RMAアプライアンスを復元する前に、バックアップされたバージョンがRMAバージョンと同じかそれ以降であることを確認してください。

バックアップファイルからSDXアプライアンスを復元するには:

1. NetScaler Console GUIで、**Infrastructure > Instances > NetScaler > SDX** の順に移動します。インスタンスを選択します。
2. **Backup/Restore** をクリックします。
3. 復元するインスタンスと同じバックアップファイルを選択します。
4. **Repackage Backup** をクリックします。

   SDXアプライアンスがバックアップされると、XVAファイルとイメージはネットワーク帯域幅とディスク領域を節約するために個別に保存されます。したがって、SDXアプライアンスを復元する前に、バックアップファイルを再パッケージ化する必要があります。

   バックアップファイルを再パッケージ化すると、SDXアプライアンスを復元するために、すべてのバックアップファイルがまとめて含まれます。再パッケージ化されたバックアップファイルは、SDXアプライアンスの復元が成功することを保証します。
5. 再パッケージ化されたバックアップファイルを選択し、「**Restore**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# ネットワーク違反の詳細

## HTTP スローロリス

**Slow Loris**は、HTTPヘッダーを可能な限り遅くターゲットアプリケーションに送信するサービス拒否攻撃です。ターゲットアプリケーションはヘッダーの到着を待つことを余儀なくされ、複数の同様の接続が開かれると、リクエストを処理できなくなる可能性があります。NetScalerインスタンスが大量のHTTPリクエストを受信すると、HTTPヘッダーが増加し、リクエストの完了に時間がかかります。このプロセスは、アプリケーションサーバーのリソースを使い果たし、HTTP **Slow Loris**攻撃につながる可能性があります。

**HTTP Slow Loris**インジケーターを使用すると、**Slow Loris**攻撃につながったリクエストを分析できます。

攻撃(/en-us/netscaler-application-delivery-management-software/media/slow-loris.png)

問題をトラブルシューティングするための**推奨されるアクション**：

- 不完全ヘッダー遅延 (incompHdrDelay) の設定をより小さい値に調整することを検討してください。
- デフォルトでは、NetScalerインスタンスはこれらの不完全なリクエストを破棄します。

**イベントの詳細**では、以下を表示できます。

- 影響を受けるアプリケーション。2つ以上のアプリケーションが違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- すべての違反を示すグラフ
- 違反発生時刻
- 合計不完全リクエストを**Slow Loris**攻撃として示す検出メッセージ

## DNS スローロリス

**DNS Slow Loris**インジケーターは、NetScalerが複数のパケットにまたがる多数のDNSリクエストを受信したときに検出します。このプロセスはDNSサーバーのリソースを使い果たし、**DNS Slow Loris**攻撃につながる可能性があります。デフォルトでは、NetScalerインスタンスはこれらの**DNS Slow Loris**リクエストを破棄するため、この問題のトラブルシューティングに追加のアクションは必要ありません。

DNS攻撃(/en-us/netscaler-application-delivery-management-software/media/dns-slow-loris.png)

**イベントの詳細**で、以下を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 影響を受けるアプリケーション。2つ以上のアプリケーションが違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- すべての違反を示すグラフ
- 違反発生時刻
- 合計DNSリクエストを**Slow Loris**攻撃として示す検出メッセージ

## HTTPスローポスト

スローポストは、ターゲットアプリケーションにHTTP POSTヘッダーを送信できるサービス拒否攻撃です。ヘッダーでは、本文メッセージサイズは正しく指定されていますが、メッセージ本文は低速で送信されます。複数の同様の接続が開かれると、ターゲットアプリケーションは待機を余儀なくされ、リクエストを処理できなくなる可能性もあります。

このプロセスは、アプリケーションサーバーのリソースを使い果たし、HTTPスローポスト攻撃につながる可能性があります。

**HTTPスローポスト**インジケーターを使用して、スローポスト攻撃につながったリクエストを分析できます。

HTTPスローポスト(/en-us/netscaler-application-delivery-management-software/media/http-slow-post.png)

この問題をトラブルシューティングするための**推奨されるアクション**は、NetScaler HTTPプロファイルでリクエストタイムアウトを有効にして構成することです。詳細については、「HTTP構成」を参照してください。

**イベントの詳細**で、以下を表示できます。

- 影響を受けるアプリケーション。2つ以上のアプリケーションが違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- すべての違反を示すグラフ
- 違反発生時刻
- 合計POSTリクエストが**Slow Loris**攻撃であることを示す検出メッセージ

## NXDOMAINフラッド攻撃

NXDOMAINフラッド攻撃は、DNSサーバーまたはNetScalerインスタンス（DNSプロキシサーバーとして構成されている場合）を標的とし、大量の存在しないリクエストまたは無効なリクエストを送信する分散型サービス拒否（DDoS）攻撃です。この攻撃は、DNSサーバーまたは

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスに影響を与え、速度低下やリクエストへの応答が得られない結果となる可能性があります。

**NXDOMAINフラッド攻撃**インジケーターを使用して、NXDOMAIN攻撃につながったリクエストを分析できます。

問題をトラブルシューティングするための**推奨されるアクション**：

- DNSサーバーとDNSプロキシサーバーの両方で、異常に高いリソース消費がないか確認します。
- NetScalerインスタンスでリクエストレートの制限を適用します。
- 不審なクライアントIPアドレスを特定し、ブロックします。
- ほとんどの名前がNXDOMAINになる場合、識別可能なパターンに従い、そのようなリクエストを破棄するようにDNSポリシーを構成します。
- 正当なDNSレコードのメモリを節約するために、NetScalerインスタンスでネガティブレコードの制限を構成します。詳細については、DNS DDoS攻撃の軽減を参照してください。

**イベントの詳細**で、以下を表示できます。

- 影響を受けるアプリケーション。2つ以上のアプリケーションが違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- すべての違反を示すグラフ

## HTTP Desync攻撃

HTTP Desync攻撃では、単一のHTTPリクエストが次のように解釈されます。

- フロントエンドサーバー（仮想サーバー）への単一のリクエスト
- バックエンドサーバーへの2つのリクエスト

このシナリオでは、バックエンドサーバーは2番目のリクエストが別のクライアントからのものと解釈します。仮想サーバーとバックエンドサーバー間の接続は、異なるリクエストに対して再利用されます。最初のクライアントリクエストが悪意のあるクライアントから悪意のあるデータとともに処理された場合、次のクライアントリクエストはカスタマイズされたリクエストになる可能性があります。この活動は、コンテンツ長と転送エンコーディングという2つのヘッダーの組み合わせを悪用することで攻撃を引き起こす可能性があります。

**HTTP Desync攻撃**インジケーターを使用すると、NetScalerインスタンスが以下の存在によって発生したHTTP Desync攻撃を受けている可能性があるかどうかを分析できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 単一のHTTPトランザクションにおけるコンテンツ長と転送エンコーディングヘッダー
- 単一のHTTPトランザクションにおける異なる値を持つ複数のコンテンツ長ヘッダー



**推奨されるアクション**では、無効なHTTPトランザクションを破棄することを検討するよう提案しています。

**イベントの詳細**では、以下を表示できます。

- 影響を受けるアプリケーション。この違反によって2つ以上のアプリケーションが影響を受けている場合は、リストからアプリケーションを選択することもできます。
- 違反の詳細を示すグラフ。棒グラフにマウスポインターを合わせると、無効なリクエスト/レスポンスの合計数を表示できます。
- 違反の検出メッセージ。合計リクエスト/レスポンスを示します。
  - 異なる値を持つ複数のコンテンツ長ヘッダーを含む
  - コンテンツ長と転送エンコーディングの両方のヘッダーを含む

## ブライヒェンバッハー攻撃

NetScalerインスタンスは、暗号化されたメッセージの特定のバイトシーケンスが復号化時に正しいパディング形式を持っているかどうかを検出します。

**Bleichenbacher攻撃**インジケーターを使用して、NetScalerインスタンスが誤った暗号化データを含むSSL/TLSハンドシェイク接続を受信しているかどうかを分析できます。



**推奨されるアクション**は、NetScalerインスタンスがハンドシェイク接続を終了し、この攻撃を軽減するため、それ以上の操作は不要であることを示しています。

**イベントの詳細**で、以下を表示できます。

- 影響を受けるアプリケーション。この違反によって2つ以上のアプリケーションが影響を受けている場合は、リストからアプリケーションを選択することもできます。
- 違反の詳細を示すグラフ。棒グラフにマウスポインタを合わせると、検出された誤ったハンドシェイク接続の合計数を表示できます。
- 違反の検出メッセージ。誤った暗号化データを持つ仮想サーバー上のハンドシェイク接続の合計数を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## セグメントスマック攻撃

**セグメントスマック攻撃**は、攻撃者がTCPセッション中に順序付けされていない小型パケットを送信できるサービス拒否（DoS）攻撃です。これらのカスタマイズされたTCPパケットは、CPUとメモリに影響を与え、NetScalerインスタンスでサービス拒否を引き起こす可能性があります。

**セグメントスマック攻撃**インジケーターを使用して、NetScalerインスタンスが設定されたキュー制限よりも多数のTCPパケットを受信したかどうかを分析できます。詳細については、TCP構成を参照してください。

NetScalerインスタンスは、過剰なTCPパケットをすべて破棄することでこの攻撃を軽減するため、管理者としてそれ以上の操作は不要です。

**イベントの詳細**で、以下を表示できます:

- 影響を受けるNetScalerインスタンス
- 違反の詳細を示すグラフ。棒グラフにマウスポインタを合わせると、検出された不正なクライアント接続の総数を表示できます。
- 違反の検出メッセージ。切断されたクライアント接続の総数を示します。

## SYNフラッド攻撃

SYNフラッド攻撃は、偽装されたIPアドレスを使用して数千の接続要求を送信することで、ターゲットマシンに影響を与える可能性のあるサービス拒否（DoS）攻撃です。NetScalerインスタンスがSYNフラッド攻撃を受けている場合、インスタンスは悪意のある各要求に対して接続を開こうとし、その後、決して届かない確認応答パケットを待ちます。

TCPプロファイルの**SYNCOOKIE**は、NetScalerアプライアンスへのSYN攻撃を防ぎます。デフォルトでは、NetScalerインスタンスの**SYNCOOKIE**は有効になっています。NetScalerインスタンスがSYNフラッド攻撃を受ける可能性は、SYNCOOKIEが無効になっている場合にのみ高くなります。

**SYNフラッド攻撃**インジケーターを使用すると、NetScalerインスタンスがSYN攻撃を受けているかどうかを分析できます。

管理者として、**推奨されるアクション**では、TCPプロファイルでSYN COOKIEを有効にすることをお勧めします。

**イベントの詳細**で、以下を表示できます:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 影響を受けるアプリケーション。2つ以上のアプリケーションがこの違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- SYN攻撃の詳細を示すグラフ
- 検出メッセージ。アプリケーションがSYN攻撃を検出された合計回数を示します。

### スモールウィンドウ攻撃

スモールウィンドウ攻撃は、より小さいサイズのウィンドウまたはウィンドウサイズ0のTCPパケットを数千個送信することで、ターゲットマシンに影響を与えるサービス拒否 (DoS) 攻撃です。ウィンドウサイズ0は、ターゲットマシンがそれ以上の通知があるまでデータの送信を停止しなければならないことを示します。ターゲットマシンに同様の接続をできるだけ多く送信することで、ターゲットマシンのメモリが最大限に利用され、応答しなくなります。

**スモールウィンドウ攻撃**インジケータを使用して、NetScalerインスタンスがソックスストレス攻撃を受けているかどうかを分析できます。

デフォルトでは、NetScalerインスタンスは、そのようなTCPスモールウィンドウパケットをすべて破棄することで、この攻撃を軽減します。したがって、管理者として、それ以上の操作は必要ありません。

**イベントの詳細**で、以下を表示できます。

- 影響を受けるアプリケーション。2つ以上のアプリケーションがこの違反の影響を受けている場合は、リストからアプリケーションを選択することもできます。
- 攻撃の詳細を示すグラフ。棒グラフにマウスポインタを合わせると、検出されたTCPスモールウィンドウパケットの総数を表示できます。
- 破棄されたTCPスモールウィンドウパケットの総数を示す検出メッセージ。

## SSL インサイト

SSL Insight は、セキュアな Web トランザクション (HTTPS) の可視性を提供し、統合されたリアルタイムおよび履歴監視を提供することで、IT 管理者が NetScaler によって提供されるすべてのセキュアな Web アプリケーションを監視できるようにします。この可視性により、管理者は以下を評価できます。

- **顧客の使用状況に対する構成変更の影響を判断する**: 管理者は、SSLv3 をオフにしたり、RC4-MD5 のような暗号を削除したりするなどの構成変更がクライアントに与える影響を理解できます。これは、このプロトコルと暗号に関する履歴トランザクションデータを評価することで可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **クライアントのパフォーマンスを定量化する**: 管理者は、使用されている SSL 暗号/プロトコルまたはネゴシエートされた証明書に基づいて、アプリケーション応答時間への影響を理解できます。
- **アプリケーションのセキュリティ**: いずれかのアプリケーションが、セキュリティの低いプロトコル、暗号、または弱い鍵強度でトランザクションを実行しているかどうかを評価します。

NetScalerインスタンスでSSL Analyticsが有効になっている場合、すべてのSSLトランザクションについてSSL統計が記録され、ログに記録されます。統計には、SSLフローの詳細が表示されます。また、すべての成功した接続はNetScaler Console Analyticsによってログに記録され、表示されます。

SSL Insight は、NetScaler Console Analytics によって表示される以下の重要な情報を提供します。

- ネゴシエートされた SSL プロトコルバージョン
- ネゴシエートされた暗号と暗号強度
- 使用された証明書の署名ハッシュアルゴリズム
- 証明書の種類とサイズ
- SSL フロントエンドおよびバックエンドエラー

**注**

SSL 接続が成功した場合、SSL AppFlow® ロギングはすべてのトランザクションの最後に発生します。

## 前提条件

- SSL Insightを設定するNetScalerインスタンスは、NetScalerソフトウェアリリース11.1 51.21以降を実行している必要があります。11.1 51.21を実行しているADCインスタンスで次のコマンドを実行して、SSL Insightのトランスポートタイプとしてlogstreamを有効にします。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the Console>`

   バージョン12.0以降を実行しているADCインスタンスの場合は、NetScaler ConsoleからAppFlowを有効にする際に、トランスポートタイプとしてLogstreamを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Consoleのバージョンとビルドは、NetScalerのバージョンとビルド以上である必要があります。たとえば、NetScaler Console 11.1ビルド61.7をインストールしている場合は、NetScaler 11.1ビルド60.14以前がインストールされていることを確認してください。

## SSL Insightの設定

次の要素を有効にすると、SSL InsightメトリクスがWeb Insightレポートに含まれます。

- 各NetScalerインスタンスでWeb InsightのAppFlowを有効にします。
- 各NetScalerインスタンスでULFDモードを有効にします。
- 各NetScalerインスタンスで必要なAppFlowパラメータを有効にします。

## AppFlow機能の有効化

**注**

AppFlow機能は、NetScaler Consoleから、または各NetScalerインスタンスから有効にできます。

**NetScaler ConsoleからAppFlow機能を有効にするには：**

NetScaler Consoleが**13.0 Build 41.x以降**の場合：

1. 「**Infrastructure > Instances > NetScaler**」に移動し、インスタンスタイプを選択します。例: VPX。
2. インスタンスを選択し、「**Select Action**」リストから「**Configure Analytics**」をクリックします。
3. 「**Configure Analytics on Virtual Server(s)**」ページで、仮想サーバーを選択し、「**Enable Analytics**」をクリックします。
4. 「**Enable Analytics**」ウィンドウで:
   a. 「**Web Insight**」を選択します
   b. トランスポートモードとして「**Logstream**」を選択します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

NetScaler 12.0以前の場合、トランスポートモードのデフォルトオプションは「**IPFIX**」です。NetScaler 12.0以降の場合、トランスポートモードとして「**Logstream**」または「**IPFIX**」のいずれかを選択できます。

IPFIXとLogstreamの詳細については、「Logstreamの概要」を参照してください。

c. 式はデフォルトでtrueです

d. 「**OK**」をクリックします

**注**

- ライセンスが付与されていない仮想サーバーを選択した場合、NetScaler Consoleはまずそれらの仮想サーバーにライセンスを付与し、その後アナリティクスを有効にします。
- 管理パーティションの場合、「**Web Insight**」のみがサポートされます
- キャッシュリダイレクション、認証、GSLBなどの仮想サーバーでは、アナリティクスを有効にできません。エラーメッセージが表示されます。

**OK**をクリックすると、NetScaler Consoleは選択した仮想サーバーでアナリティクスを有効にする処理を行います。

NetScaler Consoleが**13.0 Build 36.27以前**の場合：

1. **Infrastructure > Instances > NetScaler**に移動し、アナリティクスを有効にするNetScalerインスタンスを選択します。
2. **Select Action**リストから、**Configure Analytics**を選択します。

   アナリティクスを構成(/en-us/netscaler-application-delivery-management-software/media/configure-analytics.png)
3. **Configure Insight**ページで：

   a. ロードバランシングまたはコンテンツスイッチングのいずれかの**Application List**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリケーションリスト(/en-us/netscaler-application-delivery-management-software/media/lb-cs.png)

b. 仮想サーバーを選択し、**Enable AppFlow**をクリックします。

仮想サーバー(/en-us/netscaler-application-delivery-management-software/media/appflow.png)

4. Enable AppFlowダイアログボックスで：

- テキストボックスに**true**と入力します
- 転送モードとして**Logstream**を選択します

**注：**

転送モードとしてLogstreamを選択することをお勧めします

- **Web Insight** を選択し、**OK** をクリックします。

**NetScaler GUI を使用して AppFlow 機能を有効にするには:**

NetScaler インスタンスの GUI で、**Configuration** \> **System** \> **Settings** に移動し、**Configure Advanced Features** をクリックし、**AppFlow** を選択します。

## SSL Insight パラメータを有効にする

各 NetScaler インスタンスで、NetScaler Console に SSL Insight レコードを表示するには、いくつかの HTTP パラメータを有効にする必要があります。

**NetScaler 構成ユーティリティから SSL Insight パラメータを有効にするには:**

1. **Configuration** \> **System** \> **AppFlow** に移動し、**Change AppFlowSettings** をクリックします。
2. 次のチェックボックスを選択します: **HTTP Domain**、**HTTP Host**、**HTTP Method**、**HTTP URL**、**HTTP User-Agent**、**HTTP Content-Type**。
3. **OK** をクリックします。

## SSL Insight メトリックを表示する

NetScaler Console の SSL Insight メトリックは、NetScaler インスタンスによって処理される SSL トランザクションのパフォーマンスの詳細なビューを提供します。クライアント、サー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バー、またはアプリケーションレベルでの SSL Insight メトリック、および SSL の成功と失敗のトランザクションのメトリックを表示できます。これらのメトリックを利用して、**NetScaler HTTPS** 設定と SSL 証明書設定を分析および最適化し、パフォーマンスの問題を追跡できます。

**注**

グループを作成すると、そのグループにロールを割り当てたり、アプリケーションレベルのアクセス権を付与したり、ユーザーを割り当てたりできます。NetScaler Console の分析機能は、仮想 IP アドレスベースの承認をサポートするようになりました。ユーザーは、承認されているアプリケーション (仮想サーバー) のすべての Insight のレポートのみを表示できるようになりました。グループとグループへのユーザーの割り当ての詳細については、「グループの構成」を参照してください。

**NetScaler Console で SSL Insight メトリックを監視するには:**

以下のSSLメトリックを表示できます。

- アプリケーション。**Applications > Dashboard** に移動し、アプリケーションをクリックして、**Web Insight** タブを選択すると、詳細なメトリックが表示されます。詳細については、「アプリケーション使用状況分析」を参照してください。
- すべてのアプリケーション。**Applications > Web Insight** に移動し、**Applications** タブと **Clients** タブをクリックすると、SSL メトリックが表示されます。

## ユースケース: SSLトランザクションの概要を取得する

次のユースケースでは、SSL Insight を使用してさまざまな SSL パラメータの使用状況を評価し、セキュリティ対策を改善する方法について説明します。

通信に SSL トランザクション (HTTPS) を使用する一連のアプリケーションがあり、NetScaler Console を構成して SSL コンポーネントを監視しているとします。最も注意が必要なアプリケーションに最初に焦点を当てられるように、アプリケーションを頻繁に確認する必要がある場合があります。アプリケーションまたはすべてのアプリケーションの **Web Insight** ダッシュボードには、**SSL Errors** および **SSL Usage** の下に、次の SSL パラメータの概要が表示されます。

- SSL証明書
- SSLプロトコル
- SSL暗号
- SSLキー強度
- SSL障害 – フロントエンド

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSL障害 – バックエンド



各タブをクリックすると、詳細が表示されます。

### ユースケース：クライアントのSSLメトリクス

クライアントのリスト（IPアドレスで識別）と、クライアントごとの合計発生回数を確認できます。**Applications > Web Insight** に移動し、**Clients** タブを選択して、**SSL Usage** の詳細を表示します。

メトリクスをクリックして詳細を表示し、**Clients** の下で任意のクライアントIPアドレスをクリックすると、選択したクライアントのSSLメトリクスが表示されます。

SSLクライアントメトリクス(/en-us/netscaler-application-delivery-management-software/media/ssl-client.png)

## Web Insight の問題のトラブルシューティング

Web Insight ダッシュボードでは、アプリケーションの使用状況を視覚化し、NetScaler が提供するすべてのアプリケーションを監視できます。Web Insight を使用すると、NetScaler は HTTP および SSL トランザクションデータを AppFlow コレクターとして構成された NetScaler Console に送信します。AppFlow は、ネットワークインフラストラクチャ内のアプリケーションおよびトランザクションデータを識別および収集するために使用されるフローエクスポート標準です。

このドキュメントは、一般的な Web Insight 展開の問題をトラブルシューティングするのに役立ちます。

### データなしの診断

Web Insight にデータが表示されない場合は、仮想サーバーで **Web Insight** が有効になっていることを確認してください。詳細については、「ライセンスの管理と仮想サーバーでの分析の有効化」を参照してください。

Web Insight にデータがない場合、**データなしの診断**という通知も表示されます。クリックしてトラブルシューティングの詳細を表示できます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

# Web Insight ダッシュボードレポートに関連する問題

NetScaler Console Web Insight ダッシュボード (**アプリケーション > Web Insight**) がレポートを表示しない場合、問題は次のいずれかである可能性があります。

- Web Insight の構成に関する問題
- NetScaler と NetScaler Console 間の接続の問題
- NetScaler から AppFlow データが受信されない
- ライセンスの問題
- 観測ポイント ID の問題
- AppFlow® パラメーターの欠落に関する問題

## 設定の問題

この問題のトラブルシューティングを行うには、次の手順を実行します。

1. NetScalerインスタンスでAppFlow機能が有効になっていることを確認します。詳細については、「AppFlowの有効化」を参照してください。
2. NetScalerのWeb Insight設定を確認します。
   a. `show running | grep -i <appflow_policy>`コマンドを実行して、ポリシーのWeb Insight設定を確認します。バインドタイプが`REQUEST`であることを確認します。例: `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`
   b. `show appflow action`コマンドを実行して、アクションのWeb Insight設定を確認します。`-webinsight`オプションが有効になっていることを確認します。
   c. LB/CS/CR仮想サーバーの`appflowlog`パラメーターと、バインドされたサービスおよびサービスグループを確認します。このパラメーターが仮想サーバー、バインドされたサービス、およびサービスグループの両方で有効になっていることを確認します。

## NetScalerとNetScaler Console間の接続の問題

この問題のトラブルシューティングを行うには、次の手順を実行します。

1. NetScalerでAppFlowコレクターのステータスを確認します。詳細については、「NetScalerとAppFlowコレクター間の接続ステータスを確認する方法」を参照してください。
2. NetScaler GUIで、AppFlowポリシーがヒットしているかどうかを確認します。`show appflow policy <policy_name>`コマンドを実行してAppFlowポリシーのヒットを確認します。GUIで**Settings > AppFlow > Policies**に移動して、AppFlowポリシーのヒットを確認することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ファイアウォールがNetScalerからNetScaler ConsoleへのAppFlowデータをブロックしていないことを確認します。

### NetScaler®からAppFlowデータが受信されない

この問題のトラブルシューティングを行うには、次の手順を実行します。

1. AppFlowの設定および接続に問題がないことを確認します。詳細については、このトピックの設定の問題とNetScalerとNetScaler Console間の接続の問題の解決策のセクションを参照してください。
2. NetScalerで、シェルプロンプトで、`nsconmsg -g appflow_tmpl -d current`コマンドを実行し、次のカウンタを確認します。

   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   いずれかのカウンタが欠落している場合は、NetScalerでトレースを取得します。次に、トランザクションが完了し、応答がオリジンサーバーから提供されていることを確認します。トランザクションが完了していて一部のカウンタが欠落している場合は、サポートチームにお問い合わせください。

### ライセンスの問題

この問題では、Web Insightレポートを表示したい特定の仮想サーバーのライセンスが、**Settings > Licensing & Analytics Configuration > Configure License**の下に「No」と表示されます。

この問題をトラブルシューティングするには、次の手順を完了します。

1. NetScalerで、AppFlowポリシーのヒット数が増加していること、およびインスタンスがNetScaler ConsoleにAppFlowレコードを送信していることを確認します。
2. 対応する仮想サーバーがライセンスされているか確認します。仮想サーバーがライセンスされていない場合、NetScaler ConsoleはAppFlowレコードを破棄します。その結果、Web Insightレポートは表示されません。

### 観測ポイントIDの問題

この問題は、観測ポイントIDが一意ではないために発生します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注**

観測ポイントIDは、AppFlowレコードがエクスポートされているNetScalerの識別子です。デフォルトでは、NetScaler IPが観測ポイントIDです。

この問題をトラブルシューティングするには、次の手順を実行します。

1. NetScalerで、AppFlowポリシーのヒット数が増加しており、インスタンスがAppFlowレコードをNetScaler Consoleに送信していることを確認します。
2. 対応する仮想サーバーがライセンスされているか確認します。
3. 設定が1つのNetScalerから別のNetScalerにコピーされていないことを確認します。コピーされた場合、設定によってエクスポーターIDの問題が発生し、NetScaler ConsoleがAppFlowレコードを処理しなくなる可能性があります。
4. NetScalerにログインし、`unset appflow param -observationpointId`コマンドを実行します。

### 不足しているAppFlowパラメーターの問題

この問題は、データが不足しているためにNetScaler ConsoleがAppFlowレコードを破棄するため発生します。

この問題をトラブルシューティングするには、次の手順を実行します。

1. NetScalerで、AppFlowポリシーのヒット数が増加しており、インスタンスがAppFlowレコードをNetScaler Consoleに送信していることを確認します。
2. 対応する仮想サーバーがライセンスされているか確認します。
3. 設定が1つのNetScalerから別のNetScalerにコピーされていないことを確認します。コピーされた場合、設定によってエクスポーターIDの問題が発生し、NetScaler ConsoleがAppFlowレコードを処理しなくなる可能性があります。
4. NetScalerで次のAppFlowパラメーターが有効になっていることを確認します。
   - `HTTP method logging`
   - `HTTP domain name logging`
   - `HTTP URL logging`
   - `HTTP host logging`
   - `HTTP Content-Type header logging`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### カウンターを使用したトラブルシューティング

AppFlowまたはWeb Insight関連の問題については、以下のAppFlowカウンターを確認してください。

| カウンター | 説明 |
| --- | --- |
| `appflow_tot_record_drop` | 無効なコレクターが原因でAppFlowレコードがドロップされました。通常、コレクター構成が変更され、既存の接続が古いコレクター構成を使用している場合に発生します。 |
| `lstream_tot_trans_written` | このカウンターは、ログに記録されるすべてのトランザクションに対してインクリメントされる必要があります。 |
| `lstream_sent` | このカウンターは、送信されるすべてのトランザクションログに対してインクリメントされます。 |

## Webトランザクションの分析を表示

Webトランザクション分析を使用すると、以下の詳細なトランザクションを表示できます。

- 応答時間 > 500ミリ秒
- 5xxエラー

注:

> 選択したアプリケーションの2xxトランザクションのサンプルをいくつかのみ表示できます。

**前提条件**:

Webトランザクション分析を表示するには、次の操作を行う必要があります。

- 分析を有効にします。
- 2xxを表示するには、**Webトランザクション設定**を変更します。**設定** > **分析設定**に移動し、**分析の機能を有効にする**を選択して、**すべて**を選択します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 詳細なWebトランザクション

この機能により、詳細なトランザクションを調査できるだけでなく、クライアント、NetScaler、およびサーバー間で分割された応答時間メトリックを視覚的に理解することもできます。

注

シナリオによっては、NetScalerが一部のトランザクションのRTT値を計算できない場合があります。このようなトランザクションの場合、NetScaler ConsoleはRTT値を次のように表示します。

- **NA** – NetScalerインスタンスがRTTを計算できない場合に表示されます。
- **< 1ms** – NetScalerインスタンスが0ミリ秒から1ミリ秒の間の小数でRTTを計算する場合に表示されます。例：0.22ミリ秒。

**トランザクションサマリー**には、以下からアクセスできます。

- **アプリケーション** - **アプリケーション** > **ダッシュボード**に移動し、アプリケーションを選択して**トランザクションログ**をクリックします。

  

- **Kubernetesアプリ** - **アプリケーション** > **サービスグラフ**に移動し、サービスをクリックして**トランザクションログ**を選択します。

  

  選択したアプリケーションの**トランザクションサマリー**ページが表示されます。

  

**アプリ応答**にマウスポインターを合わせると、NetScalerインスタンスおよびサーバーからのRTTや処理時間などの詳細を表示できます。

以下の例は、問題がサーバー側にあることを分析するのに役立ちます。サーバーの応答時間は10秒を示しています。



また、ドラッグして選択することで、特定の期間のトランザクションを表示できます。



## イベントの表示

特定のイベントに関する詳細情報を表示できます。**トランザクションサマリー**パネルで、各メトリックからオプションを選択して結果をフィルタリングできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、4xxトランザクションを表示したいとします。

**トランザクションサマリー**パネルで、**応答コード**をクリックし、**404**を選択して結果を表示します。

トランザクションをクリックすると、クライアントからサーバーへのメトリック情報が表示された詳細が表示されます。

SSLエラーが発生したトランザクションの場合、クライアントとサーバーの両方の詳細が表示されます。次のSSLメトリックが表示されます。

- SSLプロトコルバージョン
- SSLフロントエンド障害
- SSL暗号強度
- SSLキー強度
- SSL証明書タイプ

**トランザクションサマリー**パネルから**SSLフロントエンド**および**SSLバックエンドメトリック**をクリックして、結果をフィルタリングすることもできます。

結果をフィルタリングするには、**トランザクションサマリー**の下にあるオプションを選択します。

- **ブラウザ**: クライアントが使用するブラウザの種類。例: Chrome、Firefox。
- **クライアントOS**: ブラウザのユーザーエージェント情報に基づくクライアントOS。例: Windows
- **デバイス**: ブラウザのユーザーエージェント情報に基づくデバイス。例: タブレット、モバイル。
- **リクエストタイプ**: トランザクションのリクエストタイプ。例: GET。
- **応答コード**: サーバーから受信した応答コード。例: 501、404、200。
- **応答コンテンツタイプ**: トランザクションのコンテンツタイプ。クライアントのリクエストがtext/htmlの場合、サーバーからの応答もtext/htmlである必要があります。
- **フロントエンドSSLプロトコルバージョン**: クライアントが使用するSSLプロトコルバージョン。例: SSLv3。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **フロントエンドSSL暗号強度**: 高、中、低などのSSL証明書キーサイズに基づく暗号強度。
- **フロントエンドSSLキー強度**: SSL暗号強度はSSL証明書キーサイズから計算されます。キー長はSSLアルゴリズムのセキュリティを定義します。例: 2048
- **フロントエンドSSL障害**: フロントエンドSSLハンドシェイクエラーメッセージ。例: SSL CLIENTAUTH FAILURE
- **フロントエンドSSL証明書タイプ**: クライアントが使用する証明書タイプ。例: RSA、DSA、ECDSA、DH。
- **バックエンドSSLプロトコルバージョン**: サーバーが使用するSSLプロトコル。例: SSLv3
- **バックエンドSSL暗号強度**: 高、中、低などのSSL証明書キーサイズに基づく暗号強度。
- **バックエンドSSLキー強度**: SSL暗号強度はSSL証明書キーサイズから計算されます。キー長はSSLアルゴリズムのセキュリティを定義します。例: 2048
- **バックエンドSSL証明書タイプ**: サーバーで使用される証明書タイプ。例: RSA、DSA、ECDSA、DH。

## イベントリストに列を追加する

ボタンをクリックしてオプションのリストを選択し、**列の追加**をクリックすると詳細が表示されます。

## 高度な検索

トランザクションサマリーには、検索テキストボックスと期間リストもあり、要件に応じてイベントを表示できます。検索ボックスにカーソルを置くと、検索ボックスに検索候補のリストが表示されます。検索クエリで演算子を使用して、検索の焦点を絞り込むこともできます。

検索クエリで使用できる演算子は次のとおりです。

| 演算子 | 説明 | 例 | 出力 |
| --- | --- | --- | --- |
| = | 特定の値と等しい | 仮想サーバー = テスト | 名前が「test」の仮想サーバーのイベントを表示します。 |
| > | ある値より大きい | アプリ応答時間 > 500 | アプリケーション応答時間が500ミリ秒を超えるアプリケー |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 演算子 | 説明 | 例 | 出力 |
| --- | --- | --- | --- |
| | | | ションのイベントを表示します |
| < | ある値より小さい | アプリ応答時間 < 300 | アプリケーション応答時間が300ミリ秒未満のアプリケーションのイベントを表示します |
| >= | ある値以上 | 合計バイト数 >= 1024 | 1KB以上のトランザクションのイベントを表示します |
| <= | ある値以下 | 合計バイト数 <= 1024 | 1 KB以下のトランザクションのイベントを表示します。 |
| != | ある値と等しくない | レスポンスコード != 200 | 失敗したトランザクションを除く、すべてのトランザクションのイベントを表示します。 |
| ~ | ある値を含む | 仮想サーバー ~ mas | 名前がmasである仮想サーバーのイベントを表示します。 |

たとえば、合計バイト数が300バイト未満のイベントを生成したいシナリオを考えてみましょう。検索クエリは次のように指定する必要があります。

1. 検索ボックスに必要な単語を入力して、関連する候補を取得します。

   ▢

2. **Total-Bytes**を選択し、検索テキストボックスをもう一度クリックして、**<**を選択します。

   ▢

3. 値300を入力します。

   「例」(/en-us/netscaler-application-delivery-management-software/media/example3.png)

4. 期間を選択し、**Search**をクリックして、検索クエリに基づいてイベントを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

検索結果が表示されます。

「例」(/en-us/netscaler-application-delivery-management-software/media/example4.png)

### 検索を保存

提案と演算子を使用した後に、検索クエリを保存できます。その後、提案と演算子を再度使用する代わりに、リストから後でそれを使用できます。

- 検索クエリを保存するには、ブックマークアイコンをクリックし、任意の名前を指定して、**Save**をクリックします。

  「検索を保存」(/en-us/netscaler-application-delivery-management-software/media/save-searches.png)
- リストから検索クエリを使用するには、アイコンをクリックし、リストから検索クエリを選択して結果を表示します。

  「保存された検索」(/en-us/netscaler-application-delivery-management-software/media/search-list.png)
- 検索クエリを削除するには、アイコンをクリックし、保存された検索クエリにマウスポインターを合わせ、**Remove**をクリックします。

  「削除」(/en-us/netscaler-application-delivery-management-software/media/web-remove.png)

  また、ブックマークアイコンをクリックして**Remove**をクリックすることもできます。

  「削除」(/en-us/netscaler-application-delivery-management-software/media/remove-bookmark.png)

### データをエクスポート

「**エクスポート**」アイコンをクリックすると、選択した期間のWebトランザクション分析データをエクスポートできます。PDF、PNG、JPEG、CSV形式でエクスポートできます。「**エクスポート**」オプションでは、次のいずれかを実行できます。

- 「**今すぐエクスポート**」を選択して、レポートをPDF、JPEG、PNG、またはCSV形式で表示およびエクスポートします。
- 「**エクスポートのスケジュール**」タブを選択して、レポートを毎日、毎週、または毎月スケジュールし、電子メールまたはSlackメッセージでレポートを送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順

## ソフトウェア要件

| KUBERNETESディストリビューション | KUBERNETESバージョン | コンテナネットワークインターフェース(CNI) | CPXバージョン | CICバージョン | NETSCALER CONSOLEバージョン | NETSCALERエージェントバージョン |
|---|---|---|---|---|---|---|
| オープンソース | v1.16.3 | フランネル | 13.0–41.28 | 1.5.25 | 13.0–47.22 | 13.0–47.22 |

## 始める前に

以下のシナリオを使用して、サービスグラフを表示できます。

- NetScaler ConsoleとKubernetesクラスターが同じネットワーク上にある場合（例：Citrix HypervisorでホストされているNetScaler ConsoleとKubernetesクラスター）。
- NetScaler ConsoleとKubernetesクラスターが異なるネットワーク上にある場合。このシナリオでは、オンプレミスエージェントを構成し、Kubernetesクラスターがホストされているネットワークにエージェントを登録する必要があります。

NetScaler Consoleでサービスグラフを使用するには、以下を確認してください。

- NetScaler CPXをプロキシとするKubernetesクラスター。詳細については、NetScaler Ingress Controllerを参照してください。
- NetScaler ConsoleとNetScaler CPX間の通信を有効にするために、NetScaler Consoleで静的ルートを構成済みであること
- GitHubリポジトリからサンプル展開ファイルをダウンロード済みであること。
- NetScaler ConsoleへのCPXの登録を成功させるために、CPX YAMLファイルに必要なパラメーターを追加済みであること。
- NetScaler ConsoleにKubernetesクラスターを追加済みであること。
- サンプルマイクロサービスアプリケーションを展開済みであること。
- NetScaler CPXを展開し、CPXをNetScaler Consoleに登録済みであること。
- 仮想サーバーのライセンスを付与するために、**仮想サーバーの自動選択**を有効にしていること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScalerエージェントがHTTPトランザクションを取得できるように、**Webトランザクション設定**を**すべて**に変更していること。
- NetScalerエージェントがTCPメトリックを取得できるように、**Istream.conf**ファイルを更新し、TCP設定を**All**に変更しました。

## ソフトウェア要件

| KUBERNETESディストリビューション | KUBERNETESバージョン | コンテナネットワークインターフェース(CNI) | CPXバージョン | CICバージョン | NETSCALER CONSOLEバージョン | NETSCALERエージェントバージョン |
|---|---|---|---|---|---|---|
| オープンソース | v1.16.3 | フラネル | 13.0–41.28 | 1.5.25 | 13.0–47.22 | 13.0–47.22 |

## 始める前に

以下のシナリオを使用してサービスグラフを表示できます。

- NetScaler ConsoleとKubernetesクラスターが同じネットワーク上にある場合（例：NetScaler ConsoleとKubernetesクラスターがCitrix Hypervisorでホストされている場合）。
- NetScaler ConsoleとKubernetesクラスターが異なるネットワーク上にある場合。このシナリオでは、オンプレミスエージェント を構成し、Kubernetesクラスターがホストされているネットワークにエージェントを登録する必要があります。

NetScaler Consoleでサービスグラフを使用するには、以下を確認してください。

- NetScaler CPXをプロキシとして使用するKubernetesクラスター。詳細については、NetScaler Ingress Controller を参照してください。
- NetScaler ConsoleとNetScaler CPX間の通信を有効にするために、NetScaler Consoleで静的ルート を構成済みであること
- GitHubリポジトリ からサンプル展開ファイルをダウンロード済みであること。
- NetScaler ConsoleへのCPXの登録を成功させるために、CPX YAMLファイル に必要なパラメーターを追加済みであること。
- NetScaler ConsoleにKubernetesクラスター を追加済みであること。
- サンプルマイクロサービスアプリケーション を展開済みであること。
- NetScaler CPXを展開し、CPXをNetScaler Consoleに登録済みであること。
- 仮想サーバーをライセンスするために、**仮想サーバーの自動選択** を有効にしていること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScalerエージェントがHTTPトランザクションを取得できるように、**Webトランザクション設定** を **すべて** に変更していること。
- NetScaler エージェントが TCP メトリックを取得できるように、**Istream.conf** ファイルを更新し、TCP 設定を **All** に変更しました。

## NetScaler Console で静的ルートを構成する

Kubernetes クラスター内では、すべてのコンテナ化されたポッドがオーバーレイネットワークを使用します。これらのプライベート IP アドレスを使用して直接通信を確立することはできません。NetScaler Console から Kubernetes クラスターへの通信を有効にするには、NetScaler Console で静的ルーティングを構成する必要があります。

注

> オンプレミスエージェントを使用している場合は、エージェントで静的ルートを構成してください。SSH クライアントを使用して NetScaler エージェントにログオンし、静的ルートを構成します。

Kubernetes クラスター用に次の IP アドレスがあるとします。

- Kubernetes マスター – 101.xx.xx.112
- Kubernetes ワーカー 1 – 101.xx.xx.111
- Kubernetes ワーカー 2 – 101.xx.xx.110

Kubernetes マスターで、静的ルーティングを行うポッドネットワークを特定するために、次のコマンドを実行します。

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

コマンドを実行した後の出力例を次に示します。

1. SSH クライアントを使用して、NetScaler Console にログオンします
2. コマンド `route add -net <public IP address range> <Kubernetes IP address>` を使用して静的ルーティングを構成します

   例えば：

   ```
   route add -net 192.168.0.0/24 101.xx.xx.112
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
route add -net 192.168.1.0/24 101.xx.xx.111
```

```
route add -net 192.168.2.0/24 101.xx.xx.110
```

3. `netstat -rn` を使用して構成を確認します。



4. これらのルートコマンドを `/mpsconfig/svm.conf` ファイルに追加します。

   a. NetScaler Console で、次のコマンドを使用して **svm.conf** ファイルにアクセスします。

   ```
   vim /mpsconfig/svm.conf
   ```

   b. **svm.conf** ファイルに静的ルートを追加します。

   例えば、`route add -net 192.168.0.0/24 101.xx.xx.112`。

## GitHub からサンプルデプロイメントファイルをダウンロードする

1. マスターノードで git hub リポジトリをクローンするには、コマンド **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git` を使用します。
2. YAML にアクセスするには：

```
cd citrix-k8s-ingress-controller/example/servicegraph-demo/
```

## CPX YAMLファイルにパラメータを追加する

**注**

CPX 58.x以降を使用している場合、エージェントに登録する際にnsroot以外のパスワードを使用する必要があります。セキュリティを確保するため、NetScalerエージェント61.x以降のリリースではパスワードの変更が必須です。NetScalerエージェントが61.x以降のバージョンにアップグレードされている場合、**CPX 58.x以降**のビルドを使用していることを確認する必要があります。

NetScaler ConsoleへのCPX登録を確実にするために、`cpx.yaml`ファイルに以下のパラメータを含める必要があります。

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
- name: "NS_MGMT_FINGER_PRINT"

  value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

- name: "NS_HTTP_PORT"

  value: "9080"

- name: "NS_HTTPS_PORT"

  value: 9443"

- name: "NS_MGMT_USER"

  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – NetScaler ConsoleのIPアドレスを示します

  **注**

  エージェントを使用している場合、これはエージェントのIPアドレスを示します。

- **NS_MGMT_FINGER_PRINT** – NetScaler ConsoleにおけるCPXの認証を示します。フィンガープリントを取得するには：

  a. NetScaler Consoleで、**Settings > Administration**に移動します。

  b. **System Configurations**の下で、**View ADM Fingerprint**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

オンプレミスエージェントを設定している場合は、**Infrastructure > Instances > Agents**に移動し、エージェントを選択してから**View Fingerprint**をクリックします。

- **NS_HTTP_PORT** – 通信用のHTTPポートを示します
- **NS_HTTPS_PORT** – 通信用のHTTPSポートを示します
- **NS_MGMT_USER** - ユーザー名を示します
- **NS_MGMT_PASS** - パスワードを示します。任意のパスワードを指定してください
- **LOGSTREAM_COLLECTOR_IP** – NetScalerエージェントのIPアドレスを示します。CPXからNetScaler Consoleにログデータを転送するには、**Logstream**プロトコルを有効にする必要があります

## NetScaler ConsoleにVPX、SDX、MPX、またはBLXインスタンスを追加する

サービスグラフでティア1のNetScalerインスタンス分析を取得するには、NetScaler ConsoleにVPX/SDX/MPX/BLXインスタンスを追加し、**Web Insight**を有効にする必要があります。

1. **Infrastructure > Instances > NetScaler**に移動します
2. **Add**オプションをクリックしてインスタンスを追加します。詳細については、「NetScaler Consoleでのインスタンスの追加」を参照してください。
3. インスタンスを追加した後、仮想サーバーを選択し、**Web Insight**を有効にします。詳細については、「仮想サーバーでのライセンス管理と分析の有効化」を参照してください。

## NetScaler ConsoleにKubernetesクラスターを追加する

Kubernetesクラスターを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Orchestration** > **Kubernetes** > **Cluster**に移動します。 クラスターページが表示されます。
3. **Add**をクリックします。
4. **Add Cluster**ページで、次のパラメーターを指定します。
   a. **名前** - 任意の名前を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **APIサーバーURL** - KubernetesマスターノードからAPIサーバーURLの詳細を取得できます。

   i. Kubernetesマスターノードで、コマンド`kubectl cluster-info`を実行します。

   ii. **「Kubernetes master is running at.」**と表示されるURLを入力します。

c. **認証トークン** - 認証トークンを指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信のアクセスを検証するために必要です。認証トークンを生成するには、次の手順を実行します。

   Kubernetesマスターノードで、次の手順を実行します。

   i. 次のYAMLを使用してサービスアカウントを作成します。

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

   ii. `kubectl create -f <yaml file>`を実行します。

   サービスアカウントが作成されます。

   iii. クラスターロールをサービスアカウントにバインドするには、`kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>`を実行します。

   サービスアカウントは、クラスター全体のアクセス権を持つようになります。

   サービスアカウントの作成中にトークンが自動的に生成されます。

   iv. トークンを表示するには、`kubectl describe sa <name>`を実行します。

   v. シークレット文字列を取得するには、`kubectl describe secret <token-name>`を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. リストからエージェントを選択します。

注

オンプレミスエージェントを使用している場合は、CPX YAMLに追加したエージェントと同じエージェントを選択していることを確認してください。

e. **作成**をクリックします。

## サンプルマイクロサービスアプリケーションを展開する

マスターノードで：

1. 名前空間を作成するには、`kubectl create -f namespace.yaml`を実行します。
2. 次のコマンドを使用して、`hotdrink`マイクロサービス、イングレス、およびシークレットを展開します。

```
kubectl create -f team_hotdrink.yaml -n sg-demo
```

```
kubectl create -f hotdrink-secret.yaml -n sg-demo
```

## CPXを展開し、NetScaler ConsoleにCPXを登録する

1. クラスターロールとクラスターバインディングを展開するには、`kubectl create -f rbac.yaml`を実行します。
2. CPXを展開するには、`kubectl create -f cpx.yaml -n sg-demo`を実行します。

デプロイ後、CPXの登録は自動的に行われます。

## ライセンス供与のために仮想サーバーの自動選択を有効にする

注

仮想サーバーライセンスが十分にあることを確認してください。詳細については、「ライセンス」を参照してください。

NetScaler ConsoleにKubernetesクラスターを追加した後、ライセンス供与のために仮想サーバーを自動選択するようにしてください。Service Graphにデータを表示するには、仮想サーバーがライセンスされている必要があります。仮想サーバーを自動選択するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **設定 > ライセンスと分析の設定**に移動します。
2. **仮想サーバーライセンスの概要**で、**仮想サーバーの自動選択**と**アドレス指定不可能な仮想サーバーの自動選択**を有効にします。



### WebトランザクションとTCPトランザクションの設定を有効にする

Kubernetesクラスターを追加し、仮想サーバーの自動選択を有効にした後、**Webトランザクション設定**と**TCPトランザクション設定**を**すべて**に変更します。

1. **設定 > 分析設定**に移動します。

   **分析設定**ページが表示されます。
2. **分析機能の有効化**をクリックします。
3. **Webトランザクション設定**で、**すべて**を選択します。
4. **TCPトランザクション設定**で、**すべて**を選択します。



5. 「**OK**」をクリックします。

### マイクロサービスにトラフィックを送信する

次に、NetScaler Consoleでサービスグラフを表示させるために、マイクロサービスにトラフィックを送信する必要があります。

1. NodePort経由でCPXを公開するために、`kubectl get svc -n sg-demo`を実行します。



2. **etc/host**ファイルを編集し、`hotdrink.beverages.com`のドメインIPエントリを作成します。

   これで、`https://hotdrink.beverages.com`を使用してマイクロサービスにアクセスできます。

## サービスメッシュトポロジを設定するための詳細な手順

サービスメッシュトポロジを展開するための前提条件は、サービスグラフの設定で確認できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler Consoleで静的ルートを構成する

Kubernetesクラスター内では、すべてのコンテナ化されたPodがオーバーレイネットワークを使用します。これらのプライベートIPアドレスを使用して直接通信を確立することはできません。NetScaler ConsoleからKubernetesクラスターへの通信を有効にするには、NetScaler Consoleで静的ルーティングを構成する必要があります。

注

> オンプレミスエージェントを使用している場合は、エージェントで静的ルートを構成していることを確認してください。SSHクライアントを使用してNetScalerエージェントにログオンし、静的ルートを構成します。

Kubernetesクラスターに次のIPアドレスがあるとします。

- Kubernetesマスター – 101.xx.xx.112
- Kubernetesワーカー 1 – 101.xx.xx.111
- Kubernetesワーカー 2 – 101.xx.xx.110

Kubernetesマスターで、静的ルーティングを行うためのPodネットワークを識別するために、次のコマンドを実行します。

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

コマンドを実行した後の出力例を次に示します。

1. SSHクライアントを使用してNetScaler Consoleにログオンする
2. コマンド `route add -net <public IP address range> <Kubernetes IP address>` を使用して静的ルーティングを構成します

   例:

   ```
   route add -net 192.168.0.0/24 101.xx.xx.112
   ```

   ```
   route add -net 192.168.1.0/24 101.xx.xx.111
   ```

   ```
   route add -net 192.168.2.0/24 101.xx.xx.110
   ```
3. `netstat -rn` を使用して構成を確認します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. これらのルートコマンドを `/mpsconfig/svm.conf` ファイルに追加します。

   a. NetScaler Console で、次のコマンドを使用して **svm.conf** ファイルにアクセスします。

   `vim /mpsconfig/svm.conf`

   b. **svm.conf** ファイルに静的ルートを追加します。

   例: `route add -net 192.168.0.0/24 101.xx.xx.112`。

## 必要なパラメータを構成する

Kubernetes マスターで:

1. イングレスゲートウェイ/サイドカーとしてCPXが展開されているすべての名前空間で、エージェント資格情報を含むシークレットを作成します。

   `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>`

2. `helm repo add citrix https://citrix.github.io/citrix-helm-charts/`
3. NetScaler CPX をイングレスゲートウェイとして展開する

   `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   次の表に、Helm チャートで設定可能なパラメータとそのデフォルト値を示します。

| パラメータ | 説明 | デフォルト | オプションまたは必須 (HELM) |
|---|---|---|---|
| citrixCPX | NetScaler CPX | FALSE | NetScaler CPX の場合必須 |
| xDSAdaptor.image | Citrix xDS アダプターコンテナのイメージ | quay.io/citrix/citrix-istio-adaptor:1.2.1 | 必須 |
| ADMSettings.ADMIP | NetScaler Console IPアドレス | なし | NetScaler CPXには必須 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 | デフォルト | オプションまたは必須 (HELM) |
|---|---|---|---|
| ADMSettings.ADMFingerPrint | NetScaler Consoleのフィンガープリントです。**Settings > Adminstration**に移動し、**System Configurations**の下にある**View Fingerprint**をクリックします。 | なし | オプション |
| ingressGateway.EULA | エンドユーザーライセンス契約 (EULA) の利用規約。はいの場合、ユーザーはEULAの利用規約に同意します。 | いいえ | NetScaler CPXには必須 |
| ingressGateway.image | Ingress Gatewayとして実行するように指定されたNetScaler CPXのイメージ | quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30 | NetScaler CPXに必須 |

4. Citrix SideCar Injectorを展開します。

```
helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --version 1.2.1 --namespace <namespace> set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<xx.xx.xx.xx> citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30
```

次の表に、Helmチャートで設定可能なパラメータとそのデフォルト値を示します。

| パラメータ | 説明 | デフォルト値 |
|---|---|---|
| ADMSettings.ADMIP | NetScaler ConsoleのIPアドレス | NIL |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 | デフォルト値 |
| --- | --- | --- |
| cpxProxy.image | サイドカープロキシとして使用されるNetScaler CPXイメージ | quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30 |
| cpxProxy.imagePullPolicy | NetScaler のイメージプルポリシー | IfNotPresent |
| cpxProxy.EULA | エンドユーザーライセンス契約 (EULA) の利用規約。はいの場合、ユーザーは EULA の利用規約に同意します。 | NO |
| cpxProxy.cpxSidecarMode | NetScaler CPX の環境変数。NetScaler CPX がサイドカーモードで実行されているかどうかを示します。 | YES |

5. CPX サイドカーインジェクションが必要なすべての名前空間にラベルを設定します。

   `kubectl label namespace <app-namespace> cpx-injection=enabled`

   手順 3 と 5 を実行すると、NetScaler CPX が NetScaler Console に登録されていることを確認できます。

## サンプルアプリケーションの展開

以下のアプリケーションを展開するとします。

- [ ] サンプルアプリケーションをデプロイするには、次の手順を実行します。

1. `kubectl create namespace citrix-system`
2. `kubectl create namespace bookinfo`
3. `kubectl label namespace bookinfo cpx-injection=enabled`
4. `kubectl create secret generic admlogin --from-literal=username=<uername> --from-literal=password=<password> -n citrix-system`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

ユーザー名とパスワードは任意で設定できます。

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   注

   ユーザー名とパスワードは任意で設定できます。

6. `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace citrix-system --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSetting IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   注

   コンソールのフィンガープリントと、エージェントまたはコンソールのIPアドレスを入力する必要があります。

7. `helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --namespace citrix-system --set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<ADM agent IP address>,cpxProxy.image=quay.io/citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30`

   注

   ConsoleのフィンガープリントとエージェントまたはConsoleのIPアドレスを指定する必要があります

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## NetScaler ConsoleでKubernetesクラスターを追加する

Kubernetesクラスターを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Orchestration** > **Kubernetes** > **Cluster** に移動します。 クラスターページが表示されます。
3. **Add** をクリックします。
4. **Add Cluster** ページで、次のパラメーターを指定します。

   a. **名前** - 任意の名前を指定します。

   b. **APIサーバーURL** - APIサーバーURLの詳細は、Kubernetesマスターノードから取得できます。

      i. Kubernetesマスターノードで、コマンド `kubectl cluster-info` を実行します。

      ii. **「Kubernetes master is running at.」** に表示されるURLを入力します。

   c. **認証トークン** - 認証トークンを指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信アクセスを検証するために必要です。認証トークンを生成するには：

      Kubernetesマスターノードで：

      i. サービスアカウントを作成するには、以下のYAMLを使用します。

      ```
      apiVersion: v1

      kind: ServiceAccount

      metadata:

        name: <name>

        namespace: <namespace>
      ```

      ii. `kubectl create -f <yaml file>`を実行します。

      サービスアカウントが作成されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iii. クラスターロールをサービスアカウントにバインドするには、`kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>`を実行します。

サービスアカウントは、クラスター全体のアクセス権を持つようになりました。

サービスアカウントの作成中に、トークンが自動的に生成されます。

iv. トークンを表示するには、`kubectl describe sa <name>`を実行します。

v. シークレット文字列を取得するには、`kubectl describe secret <token-name>`を実行します。

d. リストからエージェントを選択します。

注

エージェントを使用している場合は、CPX YAMLに追加したエージェントと同じエージェントを選択してください。

e. **作成**をクリックします。

## ライセンス供与のために仮想サーバーの自動選択を有効にする

注

十分な仮想サーバーライセンスがあることを確認してください。詳細については、「ライセンス」を参照してください。

NetScaler Console に Kubernetes クラスターを追加したら、ライセンスのために仮想サーバーを自動選択するようにしてください。Service Graph にデータを表示するには、仮想サーバーがライセンスされている必要があります。仮想サーバーを自動選択するには、次の手順を実行します。

1. **設定 > ライセンスと分析の設定** に移動します。
2. **仮想サーバーライセンスの概要** で、**仮想サーバーの自動選択** と **アドレス指定不可能な仮想サーバーの自動選択** を有効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## Web トランザクションと TCP トランザクションの設定を有効にする

Kubernetes クラスターを追加し、仮想サーバーの自動選択を有効にしたら、**Web トランザクション設定** と **TCP トランザクション設定** を **すべて** に変更します。

1. **設定 > 分析設定** に移動します。

   **分析設定** ページが表示されます。
2. **分析の機能を有効にする** をクリックします。
3. **Web トランザクション設定** で、**すべて** を選択します。
4. **TCP トランザクション設定** で、**すべて** を選択します。

   
5. **OK** をクリックします。

## マイクロサービスにトラフィックを送信する

次に、NetScaler Consoleにサービスグラフを表示させるには、マイクロサービスにトラフィックを送信する必要があります。

1. Ingress IPとポートを特定します

   ```
   export INGRESS_HOST=$(kubectl get pods -l app=citrix-ingressgateway -n citrix-system -o 'jsonpath={.items[0].status.hostIP}')
   ```

   ```
   export INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')
   ```

   ```
   export SECURE_INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')
   ```
2. cURLを使用してBookinfoフロントエンドアプリケーションにアクセスします。
   `productpage`サービスは200 OK応答を返す必要があります。

   ```
   curl -kv https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage
   ```

   ```
   curl -v http://$INGRESS_HOST:$INGRESS_PORT/productpage
   ```
3. ブラウザから`https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage`にアクセスします。

   **Bookinfo**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. $INGRESS_HOSTと$SECURE_INGRESS_PORTがIPアドレスとポート値に置き換えられていることを確認してください。

マイクロサービスにトラフィックを送信すると、サービスグラフは約10分で表示されます。

サンプル(/en-us/netscaler-application-delivery-management-software/media/sample-service-graph.png)

サービスグラフを使用すると、メトリック、エラーなど、さまざまなサービスの詳細を分析できます。詳細については、「サービスグラフ」を参照してください。

# シングルティアまたは統合イングレストポロジを設定するための詳細な手順

シングルティアまたは統合イングレストポロジを展開するための前提条件は、サービスグラフの設定で確認できます。

## NetScaler ConsoleでVPX、SDX、MPX、またはBLXインスタンスを追加する

サービスグラフでティア1 NetScalerインスタンスの分析を取得するには、NetScaler ConsoleにVPX/SDX/MPX/BLXインスタンスを追加し、**Web Insight**を有効にする必要があります。

1. **Infrastructure > Instances > NetScaler**に移動します
2. インスタンスを追加するには、**Add**オプションをクリックします。詳細については、NetScaler Consoleでインスタンスを追加するを参照してください。
3. インスタンスを追加したら、仮想サーバーを選択し、**Web Insight**を有効にします。詳細については、ライセンスを管理し、仮想サーバーで分析を有効にするを参照してください。

## NetScaler ConsoleでKubernetesクラスターを追加する

Kubernetesクラスターを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Orchestration** > **Kubernetes** > **Cluster**に移動します。 クラスターページが表示されます。
3. **Add**をクリックします。
4. **Add Cluster**ページで、次のパラメーターを指定します。

    a. **Name** - 任意の名前を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **API Server URL** - KubernetesマスターノードからAPIサーバーURLの詳細を取得できます。

   i. Kubernetesマスターノードで、コマンド `kubectl cluster-info` を実行します。

   

   ii. **「Kubernetes master is running at.」**に表示されるURLを入力します。

c. **認証トークン** - 認証トークンを指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信アクセスを検証するために必要です。認証トークンを生成するには：

   Kubernetesマスターノードで：

   i. YAMLを使用してサービスアカウントを作成します。

   ```
   kubectl create -f adm_svc_account.yaml
   ```

   サービスアカウントが作成されます。

   ii. クラスターロールをサービスアカウントにバインドするには、`kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa` を実行します。

   サービスアカウントは、クラスター全体のアクセス権を持つようになります。

   サービスアカウントの作成中にトークンが自動的に生成されます。

   iii. トークンを表示するには、`kubectl describe sa citrixadm-sa` を実行します。

   iv. シークレット文字列を取得するには、`kubectl describe secret <token-name>` を実行します。

   

d. リストからエージェントを選択します。

   注記

   > CPX YAMLで追加したエージェントと同じエージェントを選択してください。

e. **作成**をクリックします。

   

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# データガバナンス (NetScaler Console の 14.1-8.x から 14.1-21.x ビルド向け)

Cloud Connect を使用すると、Citrix Cloud はライセンスコンプライアンスのためにライセンス、構成、使用状況データを収集し、サービスを管理、測定、改善できます。14.1-8.x 以降のリリースでは、Cloud Connect を構成して、NetScaler Console サービスと NetScaler Console オンプレミス間の接続を有効にできます。Cloud Connect を有効にすると、次のことが可能になります。

- Flexed Licensing compliance の必須ライセンスおよび使用状況データが収集されます。
- NetScaler Console オンプレミスで **セキュリティアドバイザリ** 機能を利用できます。詳細については、Cloud Connect を参照してください。

## データカテゴリ

次の表に、Cloud Connect を有効にした後に収集されるパラメータの詳細を示します。

| カテゴリ | 説明 | 用途? | 必須/オプション |
|---|---|---|---|
| ライセンステレメトリデータ | ライセンスの資格、使用状況、高レベルの NetScaler 展開データ、および NetScaler 機能の使用状況に関する情報。 | ライセンスコンプライアンス、およびサービスの管理、測定、改善のため。 | 必須 |
| 機能使用状況データ | Consoleの展開とConsole機能の使用状況に関する情報。 | サービスを管理、測定、改善するため。 | オプション |

# データガバナンス (NetScaler ADM 14.1-4.42 またはそれ以前のビルドの場合)

NetScaler ADMが14.1-4.xまたはそれ以前のバージョンの場合、Citrix CloudでカスタマーIDを作成し、ADMの健全性、ステータス、その他のメトリックに関する重要な統計をオンプレミス展開からCitrix Cloudアカウントに送信できます。Citrixは、NetScaler ADMの使用状況を把握するために統計情報を収集します。

- **Citrix Cloud™でカスタマーIDを作成する** - ADMの健全性、ステータス、その他のメトリックに関する重要な統計をADMオンプレミス展開からCitrix Cloudアカウントに送信するため。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタマーIDを作成すると、「Cloud Connect」がCitrix Cloudアカウントを作成することで、ADMオンプレミスとNetScaler® Consoleサービス間の接続を確立します。詳細については、「カスタマーIDの構成」を参照してください。

- **メンテナンススクリプトの構成** - データベースを最適化するため。データベースの最適化により、テーブルの作成、列の変更などが行われる場合があります。同じ「Cloud Connect」機能を使用して、メンテナンススクリプトを構成します。詳細については、「メンテナンススクリプトを使用したデータベースの最適化」を参照してください。
- **カスタマーユーザーエクスペリエンス向上プログラム (CUXIP)** - このプログラムはデフォルトで有効になっています。NetScaler ADMから使用状況データを収集します。このデータにより、ガイド付きワークフロー、検索記事、製品通知、フィードバック、アンケートなどを通じてADMエクスペリエンスを最適化できます。詳細については、「カスタマーユーザーエクスペリエンス向上プログラム」を参照してください。

## カスタマーIDの構成

NetScaler Consoleでは、情報にアクセスを開始する前にADM GUIで認証を行う必要があります。ADMで認証を行う前に、Citrix Cloudサービスに登録する必要があります。ADM GUIでCitrix Cloudユーザー資格情報を入力してください。詳細については、「Citrix Cloudにサインアップ」を参照してください。

NetScaler ADMで認証を行う方法はいくつかあります。以下のセクションでは、ADMの新規ユーザーまたは既存ユーザーの場合のワークフローについて説明します。

### ワークフロー1 - 新規ユーザーの場合

1. 選択したハイパーバイザーにNetScaler ADMのインストールを完了します。
2. 必要なさまざまなIPアドレスを構成します。
3. Webブラウザで、NetScaler ADMのIPアドレスを入力します。
4. **ユーザー名**フィールドと**パスワード**フィールドに、管理者資格情報を入力します。

   **カスタマーIDの構成**ページが開き、Citrix Cloud資格情報を使用して本人確認を行う必要があります。

   Citrix Cloudでアカウントを作成していない場合は、登録するにはCitrix Cloud をクリックします。
5. **認証**をクリックし、Citrix Cloudに登録した際に使用したメールアドレスを入力します。
6. テレメトリのために**データの共有に同意します**の横にあるチェックボックスをオンにし、**送信**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### ワークフロー2 - 最新のADMバージョンにアップグレードする既存ユーザーの場合

1. NetScaler ADMを最新バージョンにアップグレードした後、WebブラウザでNetScaler ADMのIPアドレスを入力します。
2. **ユーザー名**と**パスワード**のフィールドに、管理者資格情報を入力します。
3. **顧客IDの構成**ページが開き、Citrix Cloudの資格情報を使用して本人確認を行う必要があります。

   Citrix Cloudでアカウントを作成していない場合は、登録するにはCitrix Cloud をクリックします。
4. **認証**をクリックし、Citrix Cloudに登録した際に使用したメールアドレスを入力します。
5. 「テレメトリのためにデータを共有することに同意します」の横にあるチェックボックスをオンにし、送信をクリックします。

既存ユーザーとして、後でADMでIDを構成するには、次の2つの方法のいずれかを使用できます。

- **設定 > システム管理**に移動し、**認証**をクリックします。
- ADM GUIの右上にあるクラウドシンボルをクリックします。 認証が成功すると、`X` は緑色のチェックマークに変わります。

**注**

次のドメインがホワイトリストに登録されていることを確認してください。

- `*.citrixnetworkapi.net`
- `*.blob.core.windows.net`

NetScaler ADM にデータをアップロードし、NetScaler ADM の機能を使用することにより、Citrix がお客様の NetScaler 製品およびサービスに関する技術情報、ユーザー情報、または関連情報を収集、保存、送信、維持、処理、使用することに同意するものとします。

Citrix が受領した情報は、常にCitrix.com プライバシーポリシー に従って取り扱われます。

## 診断およびデータ収集

NetScaler ADM は、顧客 ID を使用して以下のテレメトリを収集します。

- **ADM で実行されたアクション**:
  - NetScaler ADM UI/API インターフェイスを使用して実行されたアクション。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADM SDK インターフェイスを使用して実行されたアクション。
- 1 日あたりの操作数。この数には、API または UI からの非 GET リクエストが含まれます。
- ADM によって実行された NetScaler アップグレードの数。

- **NetScaler ADM ライセンス情報**: 資格のある仮想サーバーの数。
- **主要な統計**:
  - イベントルールの総数。
  - およびユーザー定義の StyleBook の総数。
  - 管理対象アプリケーションとカスタムアプリケーションの数。
  - 登録済みエージェントの数。
  - NetScaler全体の総スループット (Rx+Tx)。
  - 管理対象インスタンスの数。この数には、管理者パーティションも含まれます。
  - NetScaler ADM SaaSを使用している管理者の数。
- **NetScaler ADMの地理的位置**
- **展開情報**: この情報には、高可用性、ディザスタリカバリ、ADMエージェントなどの展開タイプが含まれます。

### データが収集される理由?

収集されたテレメトリデータは、次の目的に役立ちます。

- 適切なNetScaler ADMのサイジングと展開を推奨するため。
- ADMオンプレミス展開における問題をプロアクティブにトラブルシューティングするため。

### このデータを使用できるのは誰ですか?

収集された情報の唯一の所有者はCitrixです。Citrixは、お客様が自発的に提供する情報にアクセスし、収集します。当社はこの情報を誰にも販売または貸与しません。お客様のリクエストを満たすために必要な場合を除き、お客様の情報を当社の組織外の第三者と共有することはありません。例：注文の発送や問題のプロアクティブな解決のため。

### お客様のデータをどのくらいの期間保持しますか?

通常、当社はユーザーが当社のサービスを利用している間、個人データ/利用状況データを保存します。または、そうする別の目的がある場合も同様です。その後、データは法律で要求または許可

© 1997–2026 Citrix Systems, Inc. All rights reserved.

されている期間、または内部報告および照合の目的で必要な期間を超えて保存されることはありません。

すべてのテレメトリデータは、13か月または396日を超えない期間保存されます。

## メンテナンススクリプトを使用したデータベースの最適化

メンテナンススクリプトは、ADMオンプレミス展開におけるデータベース関連の問題を解決するために使用されます。ADMソフトウェアは、ADMサービスからデータベースメンテナンススクリプトを自動的にダウンロードし、データベース関連の問題をより迅速に解決します。以前は、これらの問題はスクリプトを手動で実行することで解決されていました。

この機能により、ADMオンプレミス展開はADMサービスからデータベースメンテナンススクリプトを定期的にダウンロードします。そのためには、顧客IDを構成することを確認してください。

メンテナンススクリプトは毎日および毎週実行されます。また、スクリプトはデータベースのパフォーマンスを向上させるために、テーブルを作成したり、列を追加または削除したりする場合があります。

## 顧客ユーザーエクスペリエンス向上プログラム

Citrix Systemsでは、ユーザーに魅力的な製品体験を提供することを目指しています。**顧客ユーザーエクスペリエンス向上プログラム (CUXIP)** は、Pendo を使用して、検索記事やアプリ内ガイドなどを提供することで、一般的でありながら詳細なタスクをユーザーが実行できるようにガイドします。また、ユーザーがすべての最新発表を常に把握できるように支援します。

### CUXIPで収集される使用状況データとは?

使用状況データは、ユーザーのアクションに関するものです。イベントレベルデータとも呼ばれ、使用状況データには、ユーザーがウェブサイトで訪問するページから特定の機能のクリック数まで、あらゆるものが含まれます。使用状況データは、ユーザーがアプリケーション内でどのように移動するかに関する貴重な情報です。このデータにより、ユーザーエクスペリエンスを最適化できます。

収集する使用状況データの一部を以下に示します。

- ページビューの詳細、各ページでの滞在時間。
- 訪問者IDは、ページ上のユニーク訪問者数を特定するのに役立つ、一意の匿名化された識別子です。
- アンケート統計 – スコア、閲覧数、提出数など。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### CUXIPはどのように役立ちますか?

ADMでのエクスペリエンスを向上させるために、使用状況データを使用しています。顧客ユーザーエクスペリエンスを向上させるためのいくつかの方法を以下に示します。

- アプリ内ガイド付きワークフローと関連記事を検索する機能。
- 製品改善のため、アプリ内からアンケートに参加する。
- 最新のお知らせやその他の通知について常に情報を得る。
- 製品チームに質問やフィードバックを投稿する。

### CUXIPの仕組み?

NetScaler ADMアプライアンスは内部ネットワークに配置できます。CUXIPのガイド付きアシスタンスの利点を得るには、ブラウザがインターネットに接続されている必要があります。

### ADMでCUXIPを無効にするにはどうすればよいですか?

CUXIPを無効にするには、ADM GUIで次の操作を行います。

1. **設定 > システム管理**に移動します。
2. **CUXIP設定**で、CUXIPを無効にします。

## プライバシーポリシーの変更

当社は、プライバシーポリシーを随時更新することがあります。変更があった場合は、このページに新しいプライバシーポリシーを掲載してお知らせします。変更が有効になる前に、電子メールおよび/または当社のサービス上の目立つ通知を通じてお知らせし、このプライバシーポリシーの冒頭にある「発効日」を更新します。

変更がないか、このプライバシーポリシーを定期的に確認することをお勧めします。このプライバシーポリシーの変更は、Citrix Privacy policyページに掲載された時点で有効になります。

### 参照

Citrixプライバシーポリシー: `<https://www.citrix.com/about/legal/privacy/>`

# Cloud Connect 用のオプションのテレメトリデータ

Cloud Connect を有効にした後に収集されるオプションのデータの一覧を次の表に示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| t_ten | NetScaler Console に接続されているテナントの総数 |
| デプロイ | NetScaler Console の展開タイプがスタンドアロンか HA ペアであるかを確認します。 |
| is_dr | ディザスタリカバリノードが構成されているかどうかを確認します。 |
| is_agt | エージェントが構成されているかどうかを確認します。 |
| is_cloud | NetScaler Console の展開が NetScaler Console サービスか NetScaler Console オンプレミスであるかを確認します。 |
| is_cntr | NetScaler ConsoleのデプロイがKubernetesクラスター内にあるかどうかを確認します |
| プラットフォーム | NetScaler Consoleがホストされているプラットフォーム。例: Citrix Hypervisor |
| security_advisory_enabled | NetScaler Consoleオンプレミスでセキュリティアドバイザリが有効になっているかどうかを確認します |
| total_users | NetScaler Consoleのローカルユーザーの総数 |
| total_gui_requests | 過去24時間以内にNetScaler Console GUIにログインしたユーザーの総数 |
| total_api_requests | 過去24時間以内にAPIを介してNetScaler Consoleへのリクエストの総数。これにはリモートプロキシユーザー（エージェントからのリクエスト）も含まれます。 |
| total_api_external_requests | エージェントからのリクエストを除外した、APIを介してNetScaler Consoleへのリクエストの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| total_success_preauth_requests | 事前認証トークンを生成するための成功したリクエストの総数 |
| total_custom_apps | NetScaler Console内の総カスタムアプリケーション |
| total_managed_apps | NetScaler Console内の総管理対象アプリケーション |
| total_apps | NetScaler Console内の総アプリケーション |
| total_custom_sites | NetScaler Consoleで設定されている総カスタムサイト |
| total_agents | 設定されている総エージェント |
| total_active_agents | UP状態のエージェントの総数 |
| total_custom_event_rules | NetScaler Consoleで作成された総カスタムイベントルール |
| total_event_rules | NetScaler Consoleで作成されたイベントルールの総数 |
| total_stylebook_config_store_count | NetScaler Consoleで作成された設定パックの総数 |
| total_user_sb_stylebook_count | NetScaler Consoleで作成されたカスタム設定パックの総数 |
| total_config_audit | NetScaler Consoleで設定された設定監査テンプレートの総数 |
| total_config_job | NetScaler Consoleで作成された設定ジョブの総数 |
| total_ssl_certs | NetScaler Consoleで作成/変更/削除されたSSL証明書の総数 |
| total_network_report | NetScaler Consoleで作成されたネットワークレポートの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| total_k8s | Kubernetesクラスターでホストされている NetScaler Console。Kubernetesクラスターの総数。 |
| total_ipam | NetScaler Consoleに追加されたIPAMプロバイダーの総数 |
| total_rbac_groups | NetScaler Consoleで構成されたRBACグループの総数 |
| total_ingress_deployed | Kubernetes内のイングレスコントローラーの総数. |
| total_ipam_configured | NetScaler Consoleに追加されたIPAMネットワークの総数 |
| total_web_transaction_analytics | Webトランザクション分析が有効になっているNetScalerインスタンスの総数 |
| total_pager_duty_profile | NetScaler Consoleに追加されたPagerDutyプロファイルの総数 |
| total_slack_profile | NetScaler Consoleに追加されたSlackプロファイルの総数 |
| total_api_discovery | APIリクエストを受信するNetScalerインスタンスの総数 |
| t_radius_svr | NetScaler Consoleで構成されているRADIUS認証サーバーの総数 |
| t_ldap_svr | NetScaler Consoleで構成されているLDAP認証サーバーの総数 |
| t_tacacs_svr | NetScaler Consoleで構成されているTACACS認証サーバーの総数 |
| t_att | Security Insightが有効になっているデバイスからのリクエストの総数 |
| カウント | HDX Insightが有効になっているデバイスからのリクエストの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| カウント | VPN経由で接続しているユーザーの総数 |
| カウント | 仮想デスクトップ経由で接続しているユーザーの総数 |
| agent_id | 展開されたエージェントの一意のID |
| プラットフォーム | エージェントがホストされているプラットフォーム。例: Citrix Hypervisor |
| バージョン | エージェントのバージョン |
| 都市 | エージェントが展開されている都市 |
| 国 | エージェントが展開されている国 |
| 地域 | エージェントが展開されている地域 |
| ルート | /var、/root、/flash、/var/mps ディレクトリにおけるNetScaler Consoleのディスク使用率の詳細 |
| 合計 | NetScaler Consoleの総ディスク容量 (単位: バイト) |
| 使用済み | NetScaler Consoleの総使用済みディスク容量 |
| 空き | NetScaler Consoleの総空きディスク容量 |
| Adm_analt_dx - 機能 | 問題が特定された分析タイプ (Bot、WAF、Web Insight、Service Graphなど) |
| Adm_analt_dx - issue_type | 特定された問題が属する問題カテゴリ。例: ライセンス、構成 |
| Adm_analt_dx - sub_issue_type | 特定された問題のサブ問題カテゴリ。サブ問題は、NO_VIPS_LICENSED、BOT_INSIGHT_IN_ACTION_DISABLED、NS_FEATURE_DISABLED、VSERVER_WITHOUT_BOT_POLICY_BINDING、NO_COLLECTORS_PRESENT、APPFLOWPARAM_DISABLED、 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| | ICA_APPFLOW_POLICY_BINDING、VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING、SECURITY_INSIGHT_IN_ACTION_DISABLED、NO_CPX_VIPS_PRESENT、COLLECTOR_UNBOUND_IN_VSERVER、VSERVER_WITHOUT_APPFLOW_POLICY_BINDING のいずれかです。 |
| 製品 | 製品名 |
| isCloud | オンプレミスかクラウドか |
| isContainer | コンテナ展開であるかどうか |
| mas_platform | NetScaler Consoleプラットフォーム |
| 機能 | 負荷分散/コンテンツスイッチング仮想サーバーで有効になっている分析機能 |
| total_lbvserver_ft_enabled | 少なくとも1つの分析機能が有効になっている負荷分散仮想サーバーの合計数 |
| total_csvserver_ft_enabled | 少なくとも1つの分析機能が有効になっているコンテンツスイッチング仮想サーバーの合計数 |
| feature_enabled_on_vpn | VPN仮想サーバーで有効になっている分析機能 |
| total_vpnvserver_ft_enabled | 少なくとも1つの分析機能が有効になっているVPN仮想サーバーの合計数 |

# NetScaler® Telemetry プログラムのオプションのテレメトリデータ

## NetScaler Console の機能使用状況

次の表は、NetScaler Telemetry プログラムの一部として収集されるオプションのデータの一覧を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| プラットフォーム | NetScaler Console がホストされているプラットフォーム。例: Citrix Hypervisor |
| デプロイ | NetScaler Console の展開タイプがスタンドアロンか HA ペアかを確認します。 |
| is_agt | エージェントが構成されているかどうかを確認します。 |
| is_cloud | NetScaler Console の展開が NetScaler Console サービスか NetScaler Console オンプレミスかを確認します。 |
| is_cntr | NetScaler Console の展開が Kubernetes クラスター内にあるかどうかを確認します。 |
| is_dr | ディザスタリカバリノードが構成されているかどうかを確認します |
| t_ten | NetScaler Consoleに接続されているテナントの総数 |
| num_of_ns_upgrade_jobs | 使用されたアップグレードジョブの総数 |
| security_advisory_enabled | NetScaler ConsoleオンプレミスでSecurity Advisoryが有効になっているかどうか |
| ウェブインサイト | Web InsightがLBまたはCS仮想サーバーで有効になっているかどうか |
| webinisight_usage | アクティブなHDXセッションがあるかどうか（はい/いいえ） |
| adm_analyt_hdx_apps | HDX Insightが有効になっているデバイスからのリクエストの総数 |
| adm_analyt_hdx_users | 仮想デスクトップ経由で接続されたユーザー数 |
| adm_analyt_sec_insight | Security Insightが有効になっているデバイスからのリクエストの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| adm_analyt_vpn_users | VPN経由で接続しているユーザーの総数 |
| adm_analyt_webinsight | Web Insightが有効になっているデバイスからのリクエストの総数 |
| アノマリーインサイト | リクエスト機能がlbまたはcs仮想サーバーで有効になっているかどうかを示します |
| カウント | アナリティクスに関連する問題の総数 |
| 機能 | 特定された問題の機能カテゴリ。機能はBOT_INSIGHT、DEVICE、GATEWAY_INSIGHT、HDX_INSIGHT、SECURITY_INSIGHT、SERVICE_GRAPH、SWG_INSIGHT、WEB_INSIGHT、WEB_SECURITY_BOT_INSIGHTのいずれかです。 |
| 機能 | ロードバランシング仮想サーバーで有効になっているアナリティクス機能 |
| 機能 | コンテンツスイッチング仮想サーバーで有効になっているアナリティクス機能 |
| 機能 | VPN仮想サーバーで有効になっているアナリティクス機能 |
| GWインサイト | VPN仮想サーバーでICA_REQUEST機能が有効になっているかどうかを示します |
| gwinsight_usage | 過去1日間にHDXユーザーがいたかどうかを示します（はい/いいえ） |
| gw_hdx_insights | HDX InsightとGateway Insightのエクスポートが有効になっています |
| HDXインサイト | VPNサーバーでICA_Request機能が有効になっているかどうかを示します |
| hdxinsight_usage | 過去1日間にHDXユーザーがいたかどうかを示します |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| issue_type | 識別された問題が属する問題カテゴリ。例：ライセンス、構成 |
| セックインサイト | セキュリティインサイトがLBまたはCS仮想サーバーで有効になっているかどうかを示します。 |
| secinsight_usage | 過去1日間にセキュリティ攻撃が検出されたかどうか（はいまたはいいえ） |
| sub_issue_type | 識別された問題のサブ問題カテゴリ。サブ問題は、NO_VIPS_LICENSED、BOT_INSIGHT_IN_ACTION_DISABLED、NS_FEATURE_DISABLED、VSERVER_WITHOUT_BOT_POLICY_BINDING、NO_COLLECTORS_PRESENT、APPFLOWPARAM_DISABLED、ICA_APPFLOW_POLICY_BINDING、VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING、SECURITY_INSIGHT_IN_ACTION_DISABLED、NO_CPX_VIPS_PRESENT、COLLECTOR_UNBOUND_IN_VSERVER、VSERVER_WITHOUT_APPFLOW_POLICY_BINDING のいずれかです。 |
| total_api_discovery | APIリクエストを受信するNetScalerインスタンスの総数 |
| total_csvserver_ft_enabled | 少なくとも1つの分析機能が有効になっているコンテンツスイッチング仮想サーバーの総数 |
| total_lbvserver_ft_enabled | 少なくとも1つの分析機能が有効になっているロードバランシング仮想サーバーの総数 |
| total_vpnserver_ft_enabled | 少なくとも1つの分析サーバーが有効になっているVPN仮想サーバーの総数 |
| total_web_transaction_analytics | Webトランザクション分析が有効になっているNetScalerインスタンスの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| t_radius_svr | NetScaler Consoleで構成されているRADIUS認証サーバーの総数 |
| t_ldap_svr | NetScaler Consoleで構成されているLDAP認証サーバーの総数 |
| t_tacacs_svr | NetScaler Consoleで構成されているTACACS認証サーバーの総数 |
| agt_pl_azure | エージェントのプラットフォームタイプ |
| agt_pl_citrix_hypervisor | エージェントのプラットフォームタイプ |
| agt_pl_docker | エージェントのプラットフォームタイプ |
| agt_pl_esx | エージェントプラットフォームの種類 |
| agt_pl_hyper_v | エージェントプラットフォームの種類 |
| agt_pl_gcp | エージェントプラットフォームの種類 |
| agt_pl_kvm | エージェントプラットフォームの種類 |
| agt_pl_kubernetes | エージェントプラットフォームの種類 |
| agt_pl_unknown | エージェントプラットフォームの種類 |
| agt_pl_aws | エージェントプラットフォームの種類 |
| agent_id | 展開されたエージェントの一意のID |
| 都市 | エージェントが展開されている都市 |
| 国 | エージェントが展開されている国 |
| プラットフォーム | NetScaler Consoleがホストされているプラットフォーム。例: Citrix Hypervisor |
| 地域 | エージェントが展開されている地域 |
| アクティブなエージェントの総数 | UP状態のエージェントの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| エージェントの総数 | 設定されているエージェントの総数 |
| バージョン | エージェントのバージョン |
| 都市 | データセンターの都市 |
| isCloud | オンプレミスかクラウドか |
| mas_platform | NetScaler Consoleプラットフォーム |
| 製品 | 製品名 |
| prodVer | Consoleのビルドバージョン |
| total_k8s | Kubernetesクラスターでホストされている NetScaler Console。Kubernetesクラスターの総数 |
| total_apps | NetScaler Console内のアプリケーション総数 |
| total_custom_sites | NetScaler Consoleで構成されているカスタムサイトの総数 |
| total_managed_apps | NetScaler Consoleにおける管理対象アプリケーションの総数 |
| total_custom_apps | NetScaler Consoleにおけるカスタムアプリケーションの総数 |
| ルート | NetScaler Consoleの/var、/root、/flash、/var/mpsディレクトリにおけるディスク使用状況の詳細 |
| 合計 | NetScaler Consoleのディスク領域の合計 (単位: バイト) |
| 使用済み | NetScaler Consoleのディスク領域の使用済み合計 |
| 空き | NetScaler Consoleのディスク領域の空き合計 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| total_api_requests | 過去24時間におけるNetScaler ConsoleへのAPI経由の総リクエスト数。これには、リモートプロキシユーザー（エージェントからのリクエスト）も含まれます。 |
| total_api_external_requests | エージェントからのリクエストを除外した、NetScaler ConsoleへのAPI経由の総リクエスト数 |
| total_gui_requests | 過去24時間においてNetScaler Console GUIにログインした総ユーザー数 |
| total_users | NetScaler Consoleのローカルユーザーの総数 |
| total_config_audit | NetScaler Consoleで構成されたConfig Auditテンプレートの総数 |
| total_config_job | NetScaler Consoleで作成されたConfigジョブの総数 |
| total_ssl_certs | NetScaler Consoleから作成/変更/削除されたSSL証明書の総数 |
| total_custom_event_rules | NetScaler Consoleで作成されたカスタムイベントルールの総数 |
| total_event_rules | NetScaler Consoleで作成されたイベントルールの総数 |
| total_ingress_deployed | Kubernetes内のIngressコントローラーの総数。 |
| total_ipam | NetScaler Consoleに追加されたIPAMプロバイダーの総数 |
| total_ipam_configured | NetScaler Consoleに追加されたIPAMネットワークの総数 |
| total_network_report | NetScaler Consoleで作成されたネットワークレポートの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメータ | 説明 |
| --- | --- |
| total_pager_duty_profile | NetScaler Consoleに追加されたPagerDutyプロファイルの総数 |
| gw_hdx_insights | HDX InsightおよびGateway Insightのエクスポートが有効になっているかどうか |
| total_rbac_groups | NetScaler Consoleで構成されたRBACグループの総数 |
| total_slack_profile | NetScaler Consoleに追加されたSlackプロファイルの総数 |
| total_ssl_certs | NetScaler Consoleで作成/変更/削除されたSSL証明書の総数 |
| total_stylebook_config_store_count | NetScaler Consoleで作成された設定パックの総数 |
| total_user_sb_stylebook_count | NetScaler Consoleで作成されたカスタム設定パックの総数 |
| コンフィグパック | StyleBooksから保存されたconfigpackの総数 |
| isContainer | NetScaler Consoleがコンテナプラットフォームに展開されているかどうか |
| パーセント | var_mps、root、flash、varに使用されているディスク領域の総量 |

## Cloud Connect に必要なテレメトリーデータ

次の表は、Cloud Connect を有効にした後に収集される必須データの一覧を示しています。

| パラメーター | 説明 |
| --- | --- |
| onprem_ip | NetScaler Console の IP アドレス |
| onprem_customer_id | シトリックス クラウド ID |
| onprem_time_stamp | データがアップロードされた日時 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメーター | 説明 |
| --- | --- |
| on_prem_version | NetScaler Console オンプレミスバージョン |
| total_blx_device | NetScaler Console オンプレミスで管理されている BLX インスタンスの合計数 |
| total_managed_devices | NetScaler Console内の管理対象NetScalerインスタンスの総数 |
| total_active_managed_devices | UP状態のNetScalerインスタンスの総数 |
| total_ns_device | NetScaler Console内の管理対象MPXインスタンスの総数 |
| total_ng_device | NetScaler Console内の管理対象Gatewayインスタンスの総数 |
| total_ngvpx_device | NetScaler Console内の管理対象Gateway VPXインスタンスの総数 |
| total_nswg_device | NetScaler Console内の管理対象Web Gatewayインスタンスの総数 |
| total_nswgvpx_device | NetScaler Console内の管理対象Web Gateway VPXインスタンスの総数 |
| total_nsvpx_device | NetScaler Console内の管理対象VPXインスタンスの総数 |
| total_cpx_device | NetScaler Consoleで管理されているCPXインスタンスの総数 |
| total_nsap_device | NetScaler Consoleの管理パーティションインスタンスの総数 |
| total_nssdx_device | NetScaler Consoleで管理されているSDXインスタンスの総数 |
| total_waf_devices | WAF違反が有効になっているNetScalerインスタンスの総数 |
| total_gw_devices | SSL VPNが有効になっているNetScalerインスタンスの総数 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメーター | 説明 |
| --- | --- |
| total_icaproxy_devices | NetScaler ConsoleでHDX Insightが有効になっているNetScalerインスタンスの総数 |
| total_bot_devices | Bot違反が有効になっているNetScalerインスタンスの総数 |
| total_pooled_devices | プールされたライセンスを持つNetScalerインスタンスの総数（管理対象および非管理対象の両方） |
| total_lb_devices | 負荷分散仮想サーバーで構成されたNetScalerインスタンスの総数 |
| total_lb_devices_http | 負荷分散HTTP仮想サーバーで構成されたNetScalerインスタンスの総数 |
| total_lb_devices_ssl | 負荷分散SSL仮想サーバーで構成されたNetScalerインスタンスの総数 |
| total_cs_devices | コンテンツスイッチング仮想サーバーで構成されたNetScalerインスタンスの総数 |
| total_gslb_devices | グローバルサーバー負荷分散仮想サーバーで構成されたNetScalerインスタンスの総数 |
| total_aaa_devices | AAA仮想サーバーで構成されたNetScalerインスタンスの総数 |
| device_id | VPXインスタンスの一意のID |
| バージョン | VPXインスタンスのビルドバージョン |
| 状態 | VPXインスタンスの現在のステータス (UPまたはDown) |
| device_platform | VPXインスタンスがホストされているプラットフォーム |
| st | データがプルされた現在の時刻 |
| pool_instances_entitled | 付与されたプールインスタンスの合計 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメーター | 説明 |
| --- | --- |
| pool_instances_used | 使用済みのプールインスタンスの合計 |
| pool_fips_instances_entitled | 付与されたプールFIPSインスタンスの合計 |
| pool_fips_instances_used | 合計使用済みプールFIPSインスタンス |
| pool_entvcpu_entitled | 合計割り当て済みプールエンタープライズvCPU |
| pool_entvcpu_used | 合計使用済みプールエンタープライズvCPU |
| pool_entbw_entitled | 合計割り当て済みプールエンタープライズ帯域幅 [MBps] |
| pool_entbw_used | 合計使用済みプールエンタープライズ帯域幅 [MBps] |
| pool_pltbw_entitled | 合計割り当て済みプールプラチナ帯域幅 [MBps] |
| pool_pltbw_used | 合計使用済みプールプラチナ帯域幅 [MBps] |
| pool_pltvcpu_entitled | 合計割り当て済みプールプラチナvCPU |
| pool_pltvcpu_used | プールPlatinum vCPUの合計使用数 |
| pool_stdbw_entitled | プールStandard帯域幅の合計割り当て量 |
| pool_stdbw_used | プールStandard帯域幅の合計使用量 |
| pool_stdvcpu_entitled | プールStandard vCPUの合計割り当て数 |
| pool_stdvcpu_used | プールStandard vCPUの合計使用数 |
| pool_cpxvcpu_entitled | プールCPX vCPUの合計割り当て数 |
| pool_cpxvcpu_used | プールCPX vCPUの合計使用数 |
| pool_perc_instances_used | 使用済みインスタンスの割合 |
| pool_perc_vcpu_used | 使用済みvCPUの割合 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメーター | 説明 |
| --- | --- |
| pool_perc_bw_used | 使用済み帯域幅の割合 |
| total_entitled_vservers | エンタイトルド仮想サーバーの合計 |
| total_used_vservers | 使用済み仮想サーバーの合計 |
| total_discovered_vservers | 検出済み仮想サーバーの合計 |
| perc_used_vservers | 使用済み/エンタイトルド仮想サーバーの割合 |
| perc_discovered_vservers | 検出済み/エンタイトルド仮想サーバーの割合 |
| is_local_license | ライセンスがNetScaler Consoleでホストされているかを確認します |
| license_edition | ライセンスの種類（Platinum/Standard/Enterprise） |
| is_pooled_license | ライセンスがプールされたライセンスであるかを確認します |
| model_id | インスタンスのモデルID |
| plt_license_allocation | プラチナライセンスの割り当て |
| ent_license_allocation | エンタープライズライセンスの割り当て |
| std_license_allocation | 標準ライセンスの割り当て |
| license_end_date | ライセンスの有効期限が切れるまでの合計日数 |
| プラットフォーム | デバイスタイプ |
| instance_id | インスタンスの一意の識別子 |
| instance_mode | インスタンスがスタンドアロンかHAペアであるかを確認します |
| instance_state | インスタンスのステータス（稼働中/停止中） |
| flex_vpx_inst_entitled | 許可されたVPXインスタンスの合計 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| パラメーター | 説明 |
| --- | --- |
| flex_vpx_inst_allocated | 割り当てられたVPXインスタンスの合計 |
| flex_sdx_inst_entitled | 許可されたSDXインスタンスの合計 |
| flex_sdx_inst_allocated | 割り当てられたSDXインスタンスの合計 |
| flex_mpx_inst_entitled | 資格のあるMPXインスタンスの合計 |
| flex_mpx_inst_allocated | 割り当てられたMPXインスタンスの合計 |
| flex_plt_bw_entitled | 資格のあるプラチナ帯域幅 |
| flex_plt_bw_allocated | 割り当てられたプラチナ帯域幅 |
| flex_ent_bw_entitled | 資格のあるエンタープライズ帯域幅 |
| flex_ent_bw_allocated | 割り当てられたエンタープライズ帯域幅 |
| flex_std_bw_entitled | 権利のある標準帯域幅 |
| flex_std_bw_allocated | 割り当てられた標準帯域幅 |
| flex_vpx_fips_inst_entitled | 権利のあるFIPSインスタンスの合計 |
| flex_vpx_fips_inst_allocated | 割り当てられたFIPSインスタンスの合計 |
| NSライセンスタイプ | ライセンスの種類 (FlexedまたはFixed) |

## NetScaler® テレメトリプログラムに必要なテレメトリデータ

NetScaler テレメトリプログラムの一環として収集されるデータは、Telemetry Data Governance ドキュメントに記載されています。

**注:**

一部のパラメータは、NetScaler Console から NetScaler インスタンスにプッシュされるスクリプトを介して収集されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

テレメトリを介して収集される情報（メールアドレス、ユーザー名、IPアドレスなど）は、一方向ハッシュアルゴリズムを使用してソースで情報をハッシュ化することにより、安全に仮名化されます。その結果、Citrix はこれらの値にアクセスしたり読み取ったりすることはできません。このテレメトリデータは、論理的な資産照合の目的でのみ使用されます。

# ライセンス

NetScaler Console は、インスタンスが `https` プロトコルを介して検出された場合、NetScaler インスタンスを管理および監視するために、検証済みの NetScaler ライセンスを必要とします。

NetScaler Console は、以下のライセンスエディションをサポートしています。NetScaler Console ライセンスの購入については、NetScaler の営業担当者またはパートナーにお問い合わせください。

**Express エディション** – Express エディションライセンスを使用すると、任意の数のインスタンスを管理および監視できます。デフォルトでは、Express エディションライセンスが適用されます。

**Advanced エディション** - 検出されたアプリケーションを管理し、購入した仮想サーバーと無料の仮想サーバーの両方について分析を表示できます。

**注意点：**

- ビルド **13.1-9.x 以前**の場合、最大 30 個の検出されたアプリケーションまたは仮想サーバーを管理し、分析を表示できます。30 個の検出されたアプリケーションまたは 30 個の仮想サーバーを超えて使用する場合は、Advanced ライセンスを購入して適用する必要があります。たとえば、100 個の仮想サーバーライセンスを購入した場合、最大 130 個の仮想サーバーライセンスを使用する権利があります。
- ビルド **13.1-12.x 以降**の場合、最大 2 個の検出されたアプリケーションまたは仮想サーバーを管理し、分析を表示できます。2 個の検出されたアプリケーションまたは 2 個の仮想サーバーを超えて使用する場合は、Advanced ライセンスを購入して適用する必要があります。たとえば、100 個の仮想サーバーライセンスを購入した場合、最大 102 個の仮想サーバーライセンスを使用する権利があります。

**13.1-12.x から 14.1-17.x までのビルドへのアップグレード後：**

- すべての Express デフォルトの無料仮想サーバーは 30 日間機能し続けます。30 日以内に 2 つの仮想サーバーを選択し、2 つのデフォルトライセンスを適用できます。アップグレード後 30 日間ユーザーアクションがない場合、NetScaler Console はランダムに 2 つの仮想サーバーに

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスを適用し、残りの仮想サーバーのライセンスを解除します。これらの仮想サーバーを有効にするには、新しい Advanced ライセンスを購入して適用する必要があります。

- アップグレード後、NetScaler Console の動作には以下の変更点があります。
  - NetScaler Console は、必要なアクションを実行するためにさらに 30 日間を提供します。
  - 30 日間以内は、30 個の Express 無料仮想サーバーに対する新しい仮想サーバーの割り当てはブロックされます。
    - たとえば、12.x にアップグレードする前の利用可能な仮想サーバーライセンスの数が 30 で、ライセンスされた仮想サーバーが 20 個しか使用されていなかった場合、30 日間は 20 個の仮想サーバーのみを使用でき、残りの 10 個の仮想サーバーをライセンスすることはできません。
  - ただし、30 日間以内であれば、管理者として Advanced NetScaler Console ライセンスを適用し、新しい仮想サーバーを割り当てることができます。

以下の表にライセンスの詳細を示します。

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| **アプリケーション** | アプリケーションダッシュボード | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の仮想サーバー2台が対象です。 | App Dashboard上のNetScaler Web App Firewall関連情報には、Premium (または) App Firewallライセンス付きAdvancedが必要です。 |
| | ウェブインサイト | 仮想サーバー2台まで。 | 購入済みのすべての仮想サーバーライセンスと、追加の仮想サーバー2台が対象です。 | 該当なし |
| | サービスグラフ | 最大2つの仮想サーバー。 | 購入済みのすべての仮想サーバーライセンス | 該当なし |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| | | | と追加の2つの仮想サーバーの権利があります。 | |
| | 構成 > StyleBooks | 無制限 | 無制限 | 該当なし |
| **セキュリティ** | セキュリティダッシュボード | 最大2つの仮想サーバー。 | 購入済みのすべての仮想サーバーライセンスと追加の2つの仮想サーバーの権利があります。 | セキュリティダッシュボード上のNetScaler Web App Firewall関連情報には、Premium (または) Advanced with App Firewallライセンスが必要です。 |
| | セキュリティ違反 | 最大2つの仮想サーバー。 | 購入済みのすべての仮想サーバーライセンスと追加の2つの仮想サーバーの資格があります。 | Premium (または) Advanced (App Firewallライセンス付き) |
| | ユーザーおよびエンドポイント | 最大2つの仮想サーバー。 | 購入済みのすべての仮想サーバーライセンスと追加の2つの仮想サーバーの資格があります。 | NA |
| **ゲートウェイ** | HDX インサイト | 最大2つの仮想サーバー。 | 購入済みのすべての仮想サーバーライセンスと追加の2つの | Advanced (レポート作成 < 1時間) Premium |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| | | | 仮想サーバーの資格があります。 | (レポート作成 = 無制限) |
| | Gateway インサイト | 最大2つの仮想サーバー。 | 購入済みのすべての仮想サーバーライセンスと追加の2つの仮想サーバーの資格があります。 | Advanced (レポート作成 < 1時間) Premium (レポート作成 = 無制限) |
| **インフラストラクチャ** | インフラストラクチャ分析 | 無制限 | 無制限 | 該当なし |
| | インスタンス | 無制限 | 無制限 | 該当なし |
| | SSLダッシュボード | 無制限 | 無制限 | 該当なし |
| | イベント | 無制限 | 無制限 | 該当なし |
| | ネットワーク機能 | 無制限 | 無制限 | 該当なし |
| | ネットワークレポート | 無制限 | 無制限 | 該当なし |
| | プールライセンス | 無制限 | 無制限 | 該当なし |
| | 構成 > 構成ジョブ、構成テンプレート、および構成アドバイス | 無制限 | 無制限 | 該当なし |
| | アップグレードジョブ | 無制限 | 無制限 | 該当なし |
| | オーケストレーション | 無制限 | 無制限 | 該当なし |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 機能 | オプション | EXPRESSエディション | ADVANCEエディション | NETSCALERライセンス |
|---|---|---|---|---|
| **設定** | RBACおよび外部認証 (インスタンスレベル) | 無制限 | 無制限 | NA |
| | RBACと外部認証 | 無制限 | 無制限 | NA |

*NetScaler ConsoleサポートとのCitrix Director統合の場合 – Citrix DirectorにはPremiumライセンスが必要です。

追加の仮想サーバー用ライセンスは、10個の仮想サーバーパックで利用可能です。有効なライセンスを取得し、NetScaler Console GUIを介してNetScaler Consoleサーバーにライセンスを追加できます。

## 高可用性

NetScaler Consoleサーバーには、VIP、CICO、およびプールされた容量ライセンスを含めることができます。ライセンスがNetScaler Consoleサーバーに発行されると、ライセンスはサーバーのホストIDにバインドされます。別のNetScaler Consoleサーバーにライセンスを割り当てることは制限されています。

NetScaler Consoleの高可用性ペアをライセンスサーバーとして構成する場合、プライマリサーバーとセカンダリサーバーは同じライセンスファイルを持っている必要があります。したがって、NetScaler Consoleの高可用性展開では、NetScaler Consoleは両方のサーバーに同じライセンスファイルを割り当てることをサポートしています。

**注**

- NetScaler Consoleリリース12.1-49.x以前をインストールしている場合、セカンダリノードでのライセンス維持に30日間が与えられます。30日後、元のライセンスを再ホストするためにCitrixに連絡する必要があります。
- リリース12.1-50.x以降では、NetScaler Consoleライセンスはセカンダリノードに自動的に同期されます。
- プールされたライセンスは、リリース12.1-50.x以降でセカンダリノードに自動的に同期されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### NetScaler Console高可用性ノード間でライセンスはどのように同期されますか?

フェイルオーバーが発生すると、セカンダリサーバーがプライマリサーバーの役割を引き継ぎます。プライマリサーバーのリアルホストIDは、新しいプライマリサーバーの仮想ホストIDとして構成されます。ライセンスファイルは、仮想ホストIDを使用して新しいプライマリサーバーを認識します。

- **リアルホストID** - このIDは、NetScaler ConsoleサーバーのMACアドレスから生成されます。各NetScaler Consoleスタンドアロン展開には、一意のホストIDがあります。
- **仮想ホストID** - このIDは、HA展開中に自動生成されます。NetScaler Consoleプライマリサーバーのリアルホストは、セカンダリサーバーの仮想ホストIDとして使用されます。このIDは、NetScaler Consoleデータベースに暗号化された形式で保存され、このIDへの変更は制限されています。仮想ホストIDはリアルホストIDよりも優先されます。

NetScaler Console高可用性ノード間で同期されたライセンス(/en-us/netscaler-application-delivery-management-software/media/license-ha-support-console.png)

Node-1がプライマリサーバーで、Node-2がセカンダリサーバーであると仮定します。Node-1の仮想ホストIDはNode-2と同期されます。

1. Node-1で利用可能なライセンスファイルはNode-2に同期されます。
2. Node-1上の新しいライセンスファイルは、定期的にNode-2に同期されます。
3. NetScaler Consoleは、ライセンス容量の倍増を避けるために、ライセンスサーバーがNode-1でのみ実行されていることを保証します。
4. NetScalerインスタンスは、フローティングIPアドレスを使用してNode-1からライセンスをチェックアウトします。

ライセンスはNetScalerインスタンスにロックされます。NetScaler Console HAからライセンスをチェックアウトするには、インスタンスは特定のNetScalerNetScaler IPアドレスを必要とします。ライセンスを担当するプライマリサーバーにライセンスを適用すると、そのインスタンスの将来のすべてのライセンスに適用されます。ライセンスをインストールしたサーバーからのみライセンスを削除できます。

## オーケストレーション

オーケストレーションモジュールはライセンスとは独立しており、常に利用可能です。

## 仮想サーバーライセンスのアップグレード

NetScaler Consoleのライセンスをアップグレードして、NetScalerでホストされているより多くの仮想サーバーを監視および管理できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**NetScalerライセンスをアップグレードするには：**

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **インフラストラクチャ > プールされたライセンス**に移動します。
3. **ライセンスファイル**に移動し、次のいずれかのオプションを選択します。
   - **ローカルコンピューターからライセンスファイルをアップロード**します。ライセンスがすでにローカルコンピューターに存在する場合は、**参照**をクリックし、ライセンスを割り当てるために使用するライセンスファイル（.lic）を選択します。**完了**をクリックします。
   - **ライセンスアクティベーションコードを使用**します。Citrixは、購入したライセンスのライセンスアクセスコードをメールで送信します。テキストボックスにライセンスアクセスコードを入力し、**ライセンスの取得**をクリックします。

   **注**

   このオプションを選択した場合、NetScaler Consoleはインターネットに接続されているか、プロキシサーバーが利用可能である必要があります。

   
4. ライセンス設定ページから、いつでもライセンスを追加できます。

   

## 検証

**設定 > ライセンスと分析の構成**に移動して、NetScaler Consoleにインストールされているライセンスを確認できます。



## 仮想サーバーの管理

NetScaler Consoleを介して管理および監視したい仮想サーバーまたはサードパーティの仮想サーバーを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注意点**

- デフォルトでは、NetScaler Console は、各仮想サーバーのポーリングサイクル後に仮想サーバーに自動的にランダムにライセンスを付与します。
- NetScaler Console で検出された仮想サーバーの総数が、インストールされている仮想サーバーライセンスの数よりも少ない場合、NetScaler Console は、デフォルトですべての仮想サーバーにライセンスを付与します。

仮想サーバーを手動で選択するには、またはライセンスを限られた仮想サーバーに制限するには、まず仮想サーバーの自動ライセンスを無効にし、その後、管理したい仮想サーバーを選択する必要があります。

### 仮想サーバーの自動ライセンスを無効にする

1. 「**設定 > ライセンスと分析の構成**」に移動します。

   ダッシュボードには、利用可能な仮想サーバーライセンス、管理されている仮想サーバーと仮想サーバーの種類、およびライセンスの有効期限情報が表示されます。
2. 「**仮想サーバーライセンス割り当て**」で、「**自動ライセンス仮想サーバー**」と「**アドレス指定不可能な仮想サーバーを自動選択**」を無効にします。



### ライセンス供与のためにサードパーティの仮想サーバーを選択する

1. 「**設定 > ライセンスと分析の設定**」に移動します。

   ダッシュボードには、利用可能な仮想サーバーライセンス、管理されている仮想サーバーと仮想サーバーの種類、およびライセンスの有効期限情報が表示されます。
2. 「**サードパーティ仮想サーバーの概要**」で、「**サードパーティ仮想サーバーの自動選択**」を無効にします。



## 仮想サーバーライセンスを手動で適用する

個々の仮想サーバーに手動でライセンスを適用できます。

1. **仮想サーバーライセンス割り当て**で、**ライセンスの構成**を選択します。

   **すべての仮想サーバー**ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. プロパティ `Licensed: No` を使用して、ライセンスのない仮想サーバーをフィルタリングします。
3. ライセンスを適用する仮想サーバーを選択します。
4. **ライセンス**をクリックします。

## ポリシーベースの仮想サーバーライセンスを構成する

仮想サーバーにライセンスを適用するポリシーを構成できます。このポリシーは、自動ライセンスを適用する仮想サーバーの数を制御します。また、選択したインスタンスの仮想サーバーにのみライセンスを適用します。

**ポリシーの編集**をクリックすると、以下を指定できます。

- ライセンスを適用するために、CPXインスタンスの仮想サーバー制限を個別に設定します。NetScaler Consoleは、指定された制限までCPXインスタンスの仮想サーバーにライセンスを適用します。

  **重要**

  この制限は、サイドカー展開タイプを除くCPXインスタンスに適用されます。

  サイドカー展開タイプのCPXインスタンスを表示するには、プロパティ `License Type: Freely Managed` を使用して仮想サーバーをフィルタリングします。
- ライセンスを適用するために、選択したNetScalerインスタンス（MPX/VPX/BLX）の仮想サーバー制限を設定します。NetScaler Consoleは、指定された制限までNetScalerインスタンスの仮想サーバーにライセンスを適用します。
- 仮想サーバーライセンスを適用する優先NetScalerインスタンスを選択します。したがって、NetScaler Consoleは、選択したインスタンスの仮想サーバーにのみライセンスを適用できます。

仮想サーバーにライセンスを適用するためのポリシーを編集する(/en-us/netscaler-application-delivery-management-software/media/configure-license-policy.png)

## ライセンスされた仮想サーバーを表示する

仮想サーバーにライセンスが適用された後、ライセンスされた仮想サーバーまたはサードパーティの仮想サーバーを表示できます。

1. **設定 > ライセンスと分析の構成**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **仮想サーバーライセンスの概要**の**合計ライセンス数**セクションで、仮想サーバーの種類をクリックします。

## アドレス指定不可能な仮想サーバーの自動ライセンスサポートを構成する

NetScaler Consoleは、デフォルトでは、アドレス指定不可能な仮想サーバーにライセンスを自動的に適用しません。アドレス指定不可能な仮想サーバーにライセンスを適用するには、自動ライセンスオプションを無効にし、アドレス指定不可能な仮想サーバーを手動で選択する必要があります。これにより、ライセンスを適用する際に、最初にアドレス指定不可能なサーバーを手動で選択する手間が増えます。また、新しいアドレス指定不可能な仮想サーバーがネットワークに追加されるたびに、それらを手動で選択する必要があります。

NetScaler Consoleは、**仮想サーバーライセンス割り当て**の下にオプションを提供します。**アドレス指定不可能な仮想サーバーを自動選択**オプションを有効にすると、ライセンスはアドレス指定不可能な仮想サーバーに自動的に適用されます。

**注**

- NetScaler Consoleは、デフォルトでは、ライセンスのためにアドレス指定不可能な仮想サーバーを自動的に選択しません。
- アプリケーション分析 (App Dashboard) は、ライセンスされたアドレス指定不可能な仮想サーバーで現在サポートされている唯一の分析です。

# システム通知設定を構成する

さまざまなシステム関連機能について、選択したユーザーグループに通知を送信できます。これらのシステム機能は、SystemReboot、StatusPoll、SystemStateなどのイベントカテゴリに分類されます。NetScaler Consoleを構成して、電子メールまたはSMSのいずれかで通知を送信できます。ユーザーに電子メールおよびテキスト通知を送信するには、電子メールサーバーまたはショートメッセージサービス（SMS）ゲートウェイサーバー、あるいはその両方を構成する必要があります。これにより、ユーザーログオンやシステム再起動などのシステムレベルのアクティビティが通知されます。

たとえば、CLIを使用してNetScaler Consoleにログオンしようとしてログオンが失敗した場合に、2人のユーザーに電子メール通知を送信したいとします。UserLoginカテゴリを選択してシステム

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通知を構成し、電子メール通知サーバーを作成するか、既存の電子メール配布リストを選択して通知を送信する必要があります。

**NetScaler Consoleでシステム通知設定を構成するには：**

1. **System** > **Notifications** に移動します。**Settings** の下にある **Change Notification Settings** をクリックします。
2. **Configure System Notification Settings** ページで、**Category** の下にある **UserLogin** などのカテゴリを選択します。

   
3. **Send Email** を選択し、ドロップダウンリストから電子メール配布を選択するか、「**+**」アイコンをクリックして、次の図に示すように新しい電子メール配布リストを作成します。テキスト通知を送信する場合は、**Send SMS (Text Message)** を選択し、「**+**」アイコンをクリックしてSMSサーバーの詳細を指定してSMS配布リストを作成します。

   

   特定のイベントカテゴリの通知が設定されると、そのカテゴリに関連するイベントが発生するたびに、電子メールまたはSMSを使用して受信者に通知が送信されます。この例では、ユーザーがCLIを使用してNetScaler Consoleにログオンできなかった場合の電子メール通知を確認できます。

   

システム通知は、次のイベントに対して送信されます。

| カテゴリ | 原因 |
| --- | --- |
| バックアップ失敗 | システムバックアップが失敗しました |
| DataStorageExceeded | データベースストレージがライセンスで指定された制限を超えました |
| DeviceBackupFailure | インスタンスのバックアップが失敗しました |
| `HAMonitoring` | システムHAフェイルオーバーが発生し、ピアノードからのハートビートがなく、データベース同期が失敗しました |
| HealthMontoring | CPU、RAM、またはディスクの使用率がしきい値を超えました |
| LicensePool | ライセンスプールがしきい値を超えました |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| カテゴリ | 原因 |
| --- | --- |
| ライセンス | ライセンスの適用に失敗しました |
| PasswordRecovery | パスワードの回復が失敗または成功しました |
| PerfCounterThresholdHigh | パフォーマンスカウンターの値が制限を超過しました |
| PerfCounterThresholdNormal | パフォーマンスカウンターの値が正常です |
| PolicyFailed | いずれかのシステムポリシーが失敗しました |
| RemoteDeviceBackupFailure | リモートインスタンスのバックアップに失敗しました |
| RemoteSystemBackupFailure | リモートシステムのバックアップに失敗しました |
| RemoteSystemBackupNormal | リモートシステムのバックアップが成功しました |
| SSLCertThreshold | 証明書のしきい値を超過しました |
| StatusPoll | インスタンスの状態の変更 |
| SubSystemState | サブシステムの状態の変更 |
| SystemReboot | システムが再起動されました |
| SystemState | システムの状態の変更 |
| TrapConfigFailure | インスタンスにSNMPトラップを追加する際に障害が発生しました |
| UserLogin | ユーザー認証に失敗しました |

© 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.