NetScaler Application Delivery Management 13.1

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

Contents

リリースノート 50

オンプレミス NetScaler ADM を Citrix Cloud™ に移行する 53

ADM サービスエージェントを構成する 53

Citrix Cloudからクライアントとシークレットの CSVファイルを取得する 54

ADMサービスライセンスを検証する 54

スクリプトを使用した移行 55

オンプレミスADMへのロールバック 58

前提条件 59

ロールバックスクリプトを使用する 59

よくある質問 60

ADMサービス 60

ADMサービスエージェントは、オンプレミスNetScalerエージェントと同様にオプションですか? 60

ADMサービスを使用する理由? 61

オンプレミスNetScaler ADMがHAペアの場合、移行後に何が起こりますか? 61

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? 61

インスタンスのバックアップも移行されますか? 61

履歴データも移行されますか? 61

オンプレミスライセンスも移行されますか? 61

オンプレミスNetScaler ADMから移行されないものは何ですか? 61

オンプレミスNetScaler ADMはCitrix Directorと統合されています。この統合はどうなりますか? 62

移行後、インスタンスのライセンス供与や分析の有効化が再度必要になりますか? 62

移行ツール 62

移行スクリプトの実行後、エラーメッセージが表示されます。何が問題でしょうか? 62

ADC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オプション「Y」を選択するとどうなりますか? 62

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

ADCインスタンスに関する構成が移行スクリプトで失敗した場合、どうなりますか? 63

一部のADCインスタンスがADMサービスへの移行に失敗した場合、どうなりますか。移行スクリプトを再実行すると解決しますか? 63

移行ステータスを確認するためのログファイルはありますか? 63

移行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? 63

ADMサービスがオンプレミスNetScaler ADM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? 63

オンプレミスNetScaler ADMがADMサービスExpressアカウントに移行された場合、どうなりますか? 63

Citrix Cloudに招待されたユーザー（Citrix Cloudアカウントを作成した管理者ユーザー以外）がオンプレミスADMセットアップの移行を試みた場合、どうなりますか? 64

ロールバックスクリプト 64

オンプレミスADM HAペアでロールバックスクリプトを使用した場合、どうなりますか? 64

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? 64

トラブルシューティング 64

ADMサービスに追加された手動プロファイル 65

ADMサービスに追加されたNetScalerデバイス 65

StyleBookカスタムテンプレートのADMサービスへのインポート 65

ADMサービスに追加された構成ジョブ 65

ADMサービスに追加されたIPブロック 65

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 66

すべてのハウツー記事 67

インスタンス管理 67

構成管理 68

証明書管理 69

StyleBooks 70

分析 71

イベント管理 71

認証 72

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

NetScaler ADMシステム 72
ネットワーク機能 73
概要 75
機能とソリューション 75
アプリケーション分析と管理 75
ネットワーク 76
分析 77
オーケストレーション 78
アーキテクチャ 78
NetScaler® ADM がインスタンスを検出する方法 79
ポーリングの概要 81
NetScaler® ADM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 81
インスタンスをポーリングするさまざまな方法 86
インスタンスのグローバルポーリング 86
インスタンスの手動ポーリング 86
エンティティの手動ポーリング 87
NetScaler® テレメトリプログラム 89
データガバナンス 95
ライセンス 98
高可用性 102
ADM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? 102
オーケストレーション 103
仮想サーバーライセンスのアップグレード 103
検証 104
仮想サーバーの管理 104
仮想サーバーの自動ライセンス供与を無効にする 105
ライセンス供与するサードパーティ仮想サーバーを選択する 105
仮想サーバーライセンスを手動で適用する 105

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

ポリシーベースの仮想サーバーライセンスを構成する 106
ライセンスされた仮想サーバーを表示する 106
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 107
仮想サーバーライセンスの有効期限チェック 107
システム要件 109
NetScaler ADM の要件 109
NetScaler ADMオンプレミスエージェントの要件 110
NetScaler ADM機能に必要なNetScalerの最小バージョン 110
NetScaler ADMアナリティクスの要件 111
NetScaler ADM機能に必要なCitrix Virtual Apps and Desktopsの最小バージョン 111
HDX™ Insightでサポートされているシンクライアント 112
HDX Insightに必要なNetScalerインスタンスライセンス 112
サポートされているハイパーバイザー 113
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 113
サポートされているブラウザ 113
サポートされているポート 114
ADMサーバーのポート 114
ADMエージェントのポート 117
ADCインスタンスのポート 118
ADC組み込みエージェント用のポート 119
外部サーバー用のポート 119
制限事項 120
はじめに 122
ステップ1 - システム要件の確認 122
ステップ2 - NetScaler ADMの展開 123
ステップ3 - NetScaler ADMにインスタンスを追加する 123
ステップ4 - 仮想サーバーで分析を有効にする 124
ステップ5 - NetScaler ADMでNTPサーバーを構成する 124

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

ステップ6 - NetScaler ADM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 124
次のステップ 125
展開 127
NetScaler® ADMインストールの前提条件 128
NetScaler ADMの一般的な要件 128
シトリックス ハイパーバイザー™ 上の NetScaler ADM 129
前提条件 129
XenCenterのシステム要件 130
NetScaler Application Delivery Management のインストール 130
検証 131
Microsoft Hyper-V 環境での NetScaler® ADM 131
前提条件 131
Microsoft Hyper-V のシステム要件 132
NetScaler Application Delivery Managementのインストール 132
検証 134
VMware ESXi 上の NetScaler® ADM 134
前提条件 134
NetScaler ADM をインストールするには 135
検証 137
VMware ESXi上でのNetScalerエージェント展開の自動化 137
NetScalerエージェントを構成する 138
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 138
前提条件 139
NetScaler エージェントを構成および登録する方法 139
.OVF ファイルをダウンロードして編集する 139
VMware ESXiにNetScaler ADM仮想アプライアンスをインストールする 143
確認 144
Kubernetesクラスター上のNetScaler® ADM 145

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

前提条件 145
Kubernetesクラスター 145
NFS共有 145
NetScalerアプライアンス 146
KubernetesクラスターにADMをインストールする 146
Linux KVMサーバー上のNetScaler® ADM 148
前提条件 148
ハードウェア要件 148
ソフトウェア要件 149
NetScaler ADMセットアップファイルのダウンロード 149
Linux-KVMにNetScaler Application Delivery Managementをインストールする 150
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 152
高可用性展開を構成する 154
展開シナリオ 154
高可用性アーキテクチャのコンポーネント 156
監視ツール 156
プライマリノード 156
セカンダリノード 156
物理ストリーミングレプリケーション 157
ハートビートメッセージ 157
フローティングIPアドレス 157
注意すべき重要な点 157
前提条件 159
高可用性モードでNetScaler ADMをセットアップするには 160
最初のサーバー（プライマリノード）を登録して展開する 160
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 161
プライマリノードとセカンダリノードを高可用性ペアとして展開する 163
高可用性を無効にする 164

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

高可用性を再展開する 164
高可用性フェールオーバーシナリオ 165
データベース同期ログメッセージの表示 165
スプリットブレインシナリオ 165
高可用性のためのディザスタリカバリを構成する 166
災害復旧ワークフロー 167
災害前の初期設定 167
前提条件 167
初回ディザスターリカバリーのセットアップ 169
NetScaler ADMを高可用性モードで展開する 169
DRコンソールを使用してNetScaler ADM災害復旧ノードを展開および登録する 169
NetScaler ADM GUIを使用して災害復旧ノードを展開する 171
災害後のワークフロー 172
ディザスタリカバリ後 173
設定を元のプライマリサイトに戻す 173
マルチサイト展開用のオンプレミスエージェントを構成する 174
アーキテクチャ 176
はじめに 176
データセンターにエージェントをインストールする 176
ポート 177
エージェントの登録 179
エージェントをサイトにアタッチする 180
エージェントのアクション 180
NetScalerインスタンスを追加する 180
既存のインスタンスをエージェントにアタッチする 181
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 181
NetScalerエージェントのフェールオーバー 182
エージェント到達不能しきい値と通知を構成する 183

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

Kubernetesクラスターにマイクロサービスとして ADMエージェントをインストールする 183
はじめに 183
KubernetesクラスターにNetScalerエージェントをインストールする 184
NetScaler® ADMシングルサーバー展開を高可用性展開に移行する 184
既存のNetScaler ADMサーバーノードを変更する 185
2番目のサーバーノードをプロビジョニングする 185
2台のサーバーを高可用性モードで展開する 186
NetScaler® Insight Center から NetScaler ADM への移行 187
前提条件 187
ハードウェア要件 188
インストール手順 188
NetScaler® ADMとCitrix Directorを統合する 189
前提条件 190
HDX InsightからNetScaler ADMへの移行に関するハードウェア要件 190
最小要件 190
ソフトウェア要件 190
制限事項 191
NetScaler® ADM に補助ディスクを接続する 191
スタンドアロンのNetScaler ADMにディスクを追加する 192
NetScaler ADMディスクパーティションツール 193
ディスクパーティションツールを起動する 193
新しい追加ディスクにパーティションを作成する 194
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 195
追加ディスクのパーティションを削除する 196
仮想マシンを再起動する 197
ディスクデータのバックアップファイルを作成する 197
その他のコマンド 199
高可用性で展開されたNetScaler ADMに追加ディスクを接続する 200

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

設定 203
NetScaler® ADMにインスタンスを追加する 204
NetScalerプロファイルを作成する方法 204
NetScaler ADMにADCインスタンスを追加する 206
NetScaler ADMにNetScaler CPXインスタンスを追加する 208
NetScaler ADMでスタンドアロンのNetScaler BLXインスタンスを追加する 209
NetScaler ADMで高可用性NetScaler BLXインスタンスを追加する 210
NetScaler ADMからインスタンスGUIにアクセスする 211
クラウドに展開されたNetScaler VPXインスタンスをNetScaler ADMに追加する 211
仮想サーバーでのライセンス管理とアナリティクスの有効化 213
仮想サーバーのライセンスを管理する 214
アナリティクスを有効にする 214
分析を編集 216
分析を無効にする 217
仮想サーバーでアナリティクスを有効にするための統合プロセス 218
前提条件 218
アナリティクスを有効にする 219
NTPサーバーを構成する 219
システム設定を構成する 220
システムアラームを構成する 220
システム通知を構成する 221
システムプルーニング設定の構成 221
インスタンスsyslogプルーニング設定の構成 221
インスタンスイベントプルーニング設定の構成 222
システムバックアップ設定を構成する 222
インスタンスバックアップ設定を構成する 223
ADM機能の有効化または無効化 223
NetScaler® ADMとServiceNowインスタンスの統合 224

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

前提条件 224
ADMをServiceNowと統合する方法? 225
ステップ 1 - Citrix CloudでITSM Adapterサービスをサブスクライブする 225
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 225
ステップ 3 - ServiceNowインスタンスを追加する 226
ステップ4 - ADMでのServiceNowチケットの自動生成をテストする 226
ADMでServiceNow通知を設定する 226
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 227
レポートのエクスポート 227
エクスポートレポートのスケジュール設定 228
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 229
アップグレード 230
アップグレードする前に 230
13.1-xx.xx以降へのアップグレード前に注意すべき重要な点 231
単一のNetScaler ADMサーバーを13.1-12.xにアップグレードする 232
単一のNetScaler ADMサーバーを13.1-4.xまたは13.1-9.xにアップグレードする 233
データベース移行の問題のトラブルシューティング 234
12.1リリースから13.1リリースへの高可用性ペアのアップグレード 235
NetScaler ADMディザスタリカバリ展開のアップグレード 235
NetScaler ADMディザスタリカバリノードをアップグレードする 235
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 235
オンプレミスエージェントのアップグレード 236
NetScaler ADM サーバーにディスクを追加する 236
StyleBookを使用してOpenStackでNetScalerインスタンスをプロビジョニングする 237
認証 238
外部認証サーバー 238
NetScaler ADMでユーザーを認証する 239
NetScaler® ADM で外部認証サーバーを構成する 239

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

LDAP認証サーバーを追加する 239
RADIUS認証サーバーを追加 241
TACACS認証サーバーの追加 243
NetScaler® ADMのユーザー 243
NetScaler ADMのユーザーグループ 244
認証サーバーグループを抽出する 245
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 245
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 246
アクセス制御 248
ロールベースのアクセス制御 248
制限事項 249
アクセス ポリシーを構成する 250
ユーザーにStyleBook権限を付与する 253
グループを構成する 253
ユーザーグループを作成する 254
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 261
NetScaler ADMを12.0からそれ以降のリリースにアップグレードする場合のRBACのマッピング 261
役割を構成する 262
ユーザーを構成する 263
推奨事項を表示し、ADCとアプリケーションを効率的に管理する 264
ガイドミーワークフローを使用してタスクを完了する方法? 267
よくある質問 267
アプリケーション 269
前提条件 269
アプリケーションの概要 269
個別アプリケーション 269
カスタムアプリケーション 270

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

注意事項 270
マイクロサービスアプリケーション 270
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 270
アプリケーションの管理 270
アプリケーションダッシュボード 271
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 271
アプリケーションの管理 272
アプリケーションの詳細を表示 272
アプリケーションを追加 273
StyleBookを使用してアプリケーションを作成する 275
アプリケーションの編集または削除 276
アプリケーション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 276
アプリケーションの表示 276
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 278
アプリケーションダッシュボードの概要 279
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 281
アプリケーションの詳細 282
App Score コンポーネントを選択し、しきい値を設定する 284
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 286
インテリジェントアプリ分析 289
インテリジェントアプリ分析を構成する 290
アプリケーション分析のパフォーマンス指標 290
レスポンスタイム 291
アクティブサービス 291
平均CPU使用率 292
メモリ使用量 292
サービスフラップ 293

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

不安定なサーバー 293

セッションの蓄積 294

セッション再利用率の低下 295

サージキューの蓄積 296

異常に大きいHTTPパケット 296

不適切な永続性タイプ 297

TCP再構成キュー制限ヒット 298

SSLリアルタイムトラフィック 298

アプリダッシュボードのトラブルシューティング 299

トラブルシューティングのシナリオ 299

アプリケーションがライセンスされている 300

メトリックコレクターが有効になっている 300

NetScalerインスタンスの以前のビルド 300

NetScaler インスタンスの後のビルド 301

アプリケーションの使用状況と異常 304

アプリケーション使用状況分析 305

メトリックの詳細をグラフィカル形式で表示 309

Web Insight の問題のトラブルシューティング 312

Web Insight ダッシュボード 313

統合キャッシュリクエスト 314

Web Insightの問題のトラブルシューティング 315

サービスグラフ 316

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 316

Kubernetesアプリケーションのサービスグラフ 317

3層Webアプリケーションのサービスグラフ 317

Kubernetesアプリ用サービスグラフ 319

サービスグラフの設定 320

ソフトウェア要件 320

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

始める前に 321
シングルティアまたは統合イングレストポロジ 321
デュアルティアまたはService Mesh Liteトポロジ 321
サービスメッシュトポロジ 322
サービスグラフで詳細を表示 324
サービスグラフダッシュボード 324
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 326
クライアントメトリックを表示する 326
TCPおよびSSLメトリックの表示 328
サービスの詳細を表示 329
フィルターを適用 329
設定オプションの使用 330
エラーを分析する 330
HTTPトランザクションの詳細を表示 331
サービスグラフでしきい値を設定する 332
単一しきい値 333
二重しきい値 333
サービスの詳細を表示 333
メトリクスの詳細 334
バックエンドPodの詳細を表示 335
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 335
分散トレース 339
前提条件 339
サービス追跡の詳細を表示する 343
トランザクションの詳細を表示 343
サービスグラフの部分的なデータまたはデータなしの場合の診断の詳細を表示 345
データなしの診断 346
部分的なデータの診断 346

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

トラブルシューティング 346
アプリケーションのサービスグラフ 347
アプリケーションビュー 347
ネットワーク機能ビュー 347
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 348
メトリックを分析する 348
クライアントメトリック 348
ネットワーク機能メトリック 348
サービスメトリック 349
NetScalerメトリック（GSLBアプリケーションのみ） 349
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 350
クライアントメトリクスの表示 350
NetScalerの詳細を表示 350
個別のアプリケーションを表示する 351
マイクロサービスアプリケーションの表示 353
結果をフィルタリングするための検索バー 354
StyleBook 355
StyleBookのカテゴリ 357
デフォルトおよびカスタムStyleBook 357
パブリックおよびプライベートStyleBook 357
プライベートとしてマークされたStyleBookの例 358
StyleBookの表示 358
カスタムStyleBookをダウンロード 359
カスタムStyleBookを削除 359
StyleBookの依存関係を表示 360
StyleBookの依存関係を表示するには 360
順方向の依存関係 360
逆方向の依存関係 361

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

構成パックに対するADC構成の監査 361
StyleBookのタグを作成する 361
CLIコマンドを使用してStyleBookを構成するには 362
GitHubリポジトリからStyleBookをインポートして同期する 363
リポジトリを追加し、GitHubリポジトリからStyleBookをインポートする 364
デフォルトのStyleBookを使用する 365
デフォルトのStyleBookから構成を作成するには 365
WebアプリケーションファイアウォールStyleBook 366
アプリケーションファイアウォール構成の展開 367
StyleBookを使用してWAFおよびBOTプロファイルを作成する 370
StyleBookを使用してWAFプロファイルを作成する 370
StyleBookを使用してBOTプロファイルを作成する 370
すべてのデフォルトStyleBookを非表示にする 371
StyleBooks Configuration Builder を使用した NetScaler アプリケーション構成の移行 372
サポートされているNetScaler機能 374
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 374
制限事項 375
ビジネスアプリケーション StyleBook 376
SSO Google Apps スタイルブック 376
SSO GoogleアプリStyleBookを展開するには 377
SSO Office 365 スタイルブック 381
SSO Microsoft Office 365 StyleBookを展開するには 382
Microsoft Skype for Business スタイルブック 386
主要コンポーネント 386
エンタープライズ環境でのNetScalerインスタンスの構成 387
Microsoft Exchange スタイルブック 393
Microsoft Exchange StyleBookを使用して構成されるNetScaler機能 394
前提条件 394

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

Microsoft Exchange スタイルブックの構成 394
Microsoft SharePoint スタイルブック 396
前提条件 396
Microsoft SharePoint 2016 StyleBook によって構成される NetScaler の機能 397
SharePoint StyleBook構成の展開 399
NetScaler インスタンスで定義されたオブジェクトの表示 401
Microsoft ADFSプロキシStyleBook 401
NetScalerをADFSプロキシとして使用する利点 402
Oracle eビジネス StyleBook 406
Oracle E-Business Suite 12.2の構成を作成するには 407
Citrix StoreFront™ スタイルブック 407
Citrix StoreFrontアプリケーションの構成を作成する 408
カスタムStyleBookの作成と使用 409
はじめる前に 409
StyleBookの構造 410
ロードバランシング仮想サーバーを作成するためのStyleBook 411
ヘッダー 411
コンポーネント 416
StyleBookを構築する 418
基本的なロードバランシング構成を作成するためのStyleBook 421
ヘッダー 421
コンポーネント 424
出力 429
StyleBookを構築する 430
複合StyleBookを作成する 434
StyleBookを作成する 434
カスタムStyleBookでGUI属性を使用する 438
カスタムStyleBookをインポートする 440

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

StyleBookをインポートするには 440
カスタムStyleBookの検索 444
構成パックを作成および編集する 444
構成パックを作成する 444
構成パックのStyleBookを変更する 445
構成パックのエクスポートまたはインポート 447
構成パックからターゲットインスタンスをデタッチする 449
StyleBook を構築する 450
NetScaler® ADMにファイルをアップロードするためのStyleBookを作成する 454
StyleBook構成 454
StyleBookを作成する - 1 454
StyleBookを作成する - 2 456
ファイルをアップロードするための構成の作成 457
NetScaler ADM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 459
StyleBook構成 459
SSLファイルをアップロードするための構成の作成 462
StyleBookを構築する 463
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 467
インスタンスの役割 469
ターゲットロールセクション 470
ロール「default」 471
ロールを持つコンポーネント 471
StyleBookを構築する 474
APIの使用 477
非CRUD操作を実行するStyleBookを作成する 479
非CRUD操作のサポート 480
StyleBookの構成パックを別のStyleBookに移行する 481

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

構成パックの移行 482
StyleBookを構築する 483
API を使用して StyleBook から構成を作成する 487
例 1 487
例 2 490
例 3 492
例 4 494
構成の更新 496
構成の削除 497
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 498
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 501
APIを使用してカスタムStyleBookをインポートする 502
APIを使用してカスタムStyleBookをダウンロードする 504
APIを使用してカスタムStyleBookを削除する 505
StyleBooksの文法 506
ヘッダー 508
StyleBookのインポート 510
パラメータ 512
「名前」 512
「ラベル」 512
「説明」 512
'型' 512
'ネットワーク' 515
「動的割り当て」 516
「キー」 516
「必須」 517
'許可される値' 517
'デフォルト' 518

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

'パターン' 520
'最小値' 520
'最大値' 521
'最小長' 521
'最大長' 522
'最小項目数' 522
'最大項目数' 522
'グラフィカルユーザーインターフェース' 523
'列' 523
'更新可能' 523
'collapse_pane' 523
'レイアウト' 529
'依存パラメータ' 530
パラメータデフォルトソース構成要素 532
置換 537
置換マップ 544
置換リストを反復処理する 545
コンポーネント 548
ヘルパーコンポーネント 551
オプションのプロパティ 553
プロパティ-デフォルト-ソース構成要素 555
コンポーネントのプロパティの計算 557
ネストされたコンポーネント 558
条件構成要素 560
Repeat構文 562
繰り返し条件構成要素 565
ネストされた繰り返し 566
出力 569

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

パラメータ参照 570
親参照 572
コンポーネントリファレンス 574
置換リファレンス 575
変数参照 576
オペレーション 577
アナリティクス 581
アラーム 585
式 589
算術式 589
文字列式 589
リスト式 589
関係式 590
論理式 - ブール 590
逐語的な文字列式 591
ターゲット式 592
式の型検証 592
インプレース補間 595
補間内で許可される型 596
単純な補間 597
自動型変換 597
シーケンシャル補間 597
ネストされた補間 598
quotewrap を使用した補間 598
組み込み関数 598
str() 関数 599
int() 関数 599
bool() 関数 600

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

len() 関数 600
min() 関数 600
max() 関数 601
bin() 関数 601
oct() 関数 601
hex() 関数 602
小文字() 602
大文字() 602
合計() 602
べき乗() 603
ip() 603
base64.encode() 603
base64.decode() 604
exists() 関数 604
フィルター() 604
イフ-ゼン-エルス() 605
join() 関数 605
split() 関数 606
マップ() 606
quotewrap() 関数 607
replace() 関数 607
トリム() 608
トランケート() 608
ディスティンクト() 609
url.encode() 609
url.decode() 609
is-ipv4() 関数 609
is-ipv6() 関数 609

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

スターツウィズ() 610
エンズウィズ() 610
contains() 関数 610
substring() 関数 611
依存関係の検出 612
循環依存関係 613
セキュリティ 616
アプリケーションセキュリティダッシュボード 616
脅威インデックスの詳細 617
安全指数詳細 618
アプリケーションセキュリティ違反の詳細を表示 618
前提条件 619
Splunkとの統合 619
NetScaler ADMからデータを受信するようにSplunkを構成する 620
Splunk HTTPイベントコレクターエンドポイントを設定し、トークンを生成する 620
Splunk Common Information Modelをインストールする 621
Splunkでサンプルダッシュボードを準備する 621
NetScaler ADMを構成してSplunkにデータをエクスポートする 622
Splunkでダッシュボードを表示する 624
New Relicとの統合 625
前提条件 625
NetScaler ADMにキーの詳細を追加します 625
New Relic ダッシュボード 627
ゲートウェイ 629
ゲートウェイインサイト 629
留意事項 630
制限事項 630
Gateway Insightを有効にする 631

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

NetScaler ADM バージョン **13.0 Build 41.x 以降**の場合 632

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記録を有効にする 632

Gateway Insightレポートの表示 632

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 633

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 633

ユーザーのGateway Insightレポートを表示する 633

ユーザーの詳細を表示するには 633

アプリケーションのGateway Insightレポートを表示する 635

アプリケーションの詳細を表示するには 635

ゲートウェイのGateway Insightレポートの表示 635

ゲートウェイの詳細を表示するには 636

レポートのエクスポート 636

レポートをエクスポートするには 636

Gateway Insight のユースケース 637

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 637

認証の失敗 638

EPAの失敗 638

SSO障害 639

NetScaler Gatewayへのログオンに成功した後、ユーザーが仮想アプリケーションを起動できない 640

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 641

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 641

異なるユーザーが異なるNetScaler Gateway展開を使用しているか、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 642

© 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 642
Gateway Insight 構成チェックリスト 642
NetScaler と NetScaler ADM 間の接続チェックリスト 643
NetScaler チェックリストでのレコード生成 643
NetScaler ADM でのレコードの検証 644
NetScaler ADM での Logstream ログの検証 644
Gateway Insightカウンター 644
NetScalerログのAppFlowレコード 645
Citrixテクニカルサポートへのお問い合わせ 646
既知の問題 647
HDX™ インサイト 647
パフォーマンス低下の根本原因の特定 648
シナリオ 1 648
シナリオ2 649
HDX Insightのジオマップ 650
ユースケース 650
制限事項 651
HDX™ Insight データ収集の有効化 651
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 651
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 655
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 657
Optimal Gatewayに使用される仮想サーバーでHDX Insightを構成する 658
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 664
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 667
透過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 668

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

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 670
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676
HDX™ Insight のしきい値を作成し、アラートを設定する 679
使用例 680
HDX™ Insightレポートとメトリックの表示 682
ユーザービューのレポートとメトリック 682
アプリケーションビューのレポートとメトリック 694
デスクトップビューのレポートとメトリック 701
インスタンスビューのレポートとメトリック 714
ライセンスビューのレポートとメトリック 718
アプリケーションビューのレポートとメトリクス 718
デスクトップビューのレポートとメトリクス 725
ユーザービューのレポートとメトリクス 737
インスタンスビューのレポートとメトリック 749
ライセンスビューのレポートとメトリクス 753
HDX™ Insight の問題のトラブルシューティング 754
HDX Insight 構成チェックリスト 754
NetScalerとNetScaler ADM間の接続チェックリスト 755
NetScalerでのHDX/ICAトラフィックのレコード生成チェックリスト 755
エラーカウンター 763
nstraceの検証 768
NetScaler ADMチェックリスト内のレコードの入力 768
Citrixテクニカルサポートに問い合わせる前に 768
既知の問題 769
インフラストラクチャ 770
インフラストラクチャ分析 770
インフラストラクチャ分析 771

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

インスタンススコア 771
健全性インジケータ 771
ADC容量の問題を表示する 773
健全性インジケーターの値 774
インフラストラクチャ分析ダッシュボード 775
サークルパックビュー 775
インスタンスの円 776
グループ化されたインスタンスの円 776
クラスター化されたインスタンスの円 777
Circle Pack の使用方法 777
表形式ビュー 778
サマリーパネルの使用方法 779
インスタンス情報 781
トラフィックプロファイル 781
設定パネルの使用方法 781
表示 781
スコアしきい値 782
ダッシュボードでデータを視覚化する方法 782
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 783
ADCインスタンスのキャパシティ問題を表示する 787
容量の問題を解決するための推奨アクションを表示する 788
新しいインジケーターによるインフラストラクチャ分析の強化 789
表形式ビュー 791
異常の詳細を表示 791
インスタンス管理 791
インスタンスの追加 792
インスタンスダッシュボードの使用方法 792
グローバルに分散されたサイトを監視する 793

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

ユースケース 794
ジオマップの構成 795
タグを作成してインスタンスに割り当てる方法 797
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 799
NetScaler VPX インスタンスを検索するには 799
NetScalerインスタンスの管理パーティションを管理する 800
NetScaler高可用性ペアを作成する 803
NetScalerインスタンスのバックアップと復元 804
インスタンスのバックアップ設定を構成する 806
NetScaler ADM を使用して NetScaler インスタンスを復元する 808
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 810
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 811
インスタンスグループの作成 812
NetScaler® ADMを使用してインスタンスグループを作成するには 812
ADM を使用して SDX 上に NetScaler VPX インスタンスをプロビジョニングする 813
ステップ1 - VPXインスタンスを追加する 813
ステップ2 - ライセンスの割り当て 814
ステップ3 - リソースの割り当て 815
ステップ4 - インスタンス管理の追加 818
ステップ5 - ネットワーク設定の指定 818
手順6 - 管理VLAN設定を指定する 820
プロビジョニングされたVPXインスタンスを表示する 820
VMware ESX で NetScaler VPX インスタンスをプロビジョニングする 821
前提条件 821
NetScaler VPX ファイルをテンプレートに変換する 821
ADMでサイトを作成 821
VMware ESXでインスタンスをプロビジョニングする 823
複数のNetScaler VPXインスタンスを再検出する 824

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

インスタンスの管理を解除する 824
インスタンスへの経路をトレースする 825
NetScalerインスタンス間で構成をレプリケートする 825
あるインスタンスから他のNetScalerインスタンスへ構成をレプリケートするには 825
SSL証明書管理 826
エンタープライズSSLポリシー設定 827
NetScaler ADM証明書の仕組み 827
SSL証明書管理のユースケース 828
SSL証明書のインストール 828
証明書有効期限の通知設定 828
証明書の更新 829
SSL証明書のリンクとリンク解除 830
監査ログ 830
SSLダッシュボードを使用する 830
SSL証明書を監視するには 831
SSL証明書の監査証跡を表示するには 832
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 832
SSLファイルの表示、アップロード、ダウンロード 833
SSL証明書の有効期限切れに関する通知を設定する 833
インストール済みの証明書を更新する 835
NetScalerインスタンスにSSL証明書をインストールする 835
証明書署名要求 (CSR) を作成する 837
SSL証明書のリンクとリンク解除 838
エンタープライズポリシーを構成する 839
NetScalerインスタンスからSSL証明書をポーリングする 840
イベント 841
イベントダッシュボードを使用する 841
イベントのイベント期間を設定する 842

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

イベントフィルターをスケジュールする 843
イベントの繰り返しメール通知を設定する 844
イベントを抑制する 845
イベントルールを作成する 845
ステップ1 - イベントルールを定義する 847
ステップ2 - イベントの重大度を選択します 847
ステップ3 - イベントカテゴリを指定します 848
ステップ 4 - NetScalerインスタンスを指定する 848
ステップ 5 - 障害オブジェクトを選択する 848
ステップ 6 - 高度なフィルターを指定する 849
ステップ 7 - イベントルールアクションの追加 849
NetScalerインスタンスで発生するイベントの報告される重大度を変更する 857
イベント概要の表示 857
イベントの重大度とSNMPトラップの詳細を表示する 858
NetScaler syslogメッセージの表示とエクスポート 860
ADMをsyslogサーバーとして設定する 860
syslogメッセージの表示と検索 860
syslogメッセージのエクスポートとスケジュール設定 861
syslogメッセージを抑制する 861
フィルタを作成してsyslogメッセージを抑制する 862
フィルターの無効化 863
インスタンスイベントのプルーニング設定を構成する 863
ネットワーク機能 863
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 864
結合されたロードバランシングレポートを生成する 865
個別の負荷分散エンティティレポートを生成する 866
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 867
ネットワークレポート 869

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

ネットワークレポートダッシュボード 869
ネットワークレポートのエクスポート 871
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 873
NetScaler ADM でネットワークレポートのしきい値を管理する方法 874
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 876
ネットワークレポートのプルーニング設定を構成する 876
構成ジョブ 877
構成テンプレート 877
インスタンス 878
ファイル 878
記録と再生 878
関連記事 878
構成ジョブを作成する 879
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 882
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 885
構成ジョブで変数を使用する 886
修正コマンドから構成ジョブを作成する 890
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 891
実行済み構成ジョブの再利用 892
構成ジョブでSCP (put) コマンドを使用する 893
構成テンプレートを使用する 895
マスター構成テンプレートを使用する 896
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 901
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 902
組み込みテンプレートを使用して設定されたジョブを再スケジュールする 904
構成ジョブで構成監査テンプレートを再利用する 904

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

構成テンプレートのインポートとエクスポート 907
構成監査 908
監査テンプレートを作成する 909
監査レポートを表示 911
インスタンス全体での構成変更の監査 914
ネットワーク構成に関する構成アドバイスを取得する 916
NetScalerインスタンスの構成監査をポーリングする 918
ConfigChange SNMPトラップの構成監査差分を生成する 918
アップグレードジョブ 920
NetScalerインスタンスのアップグレードをスケジュールする 921
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 924
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 925
Autoscale™ グループのアップグレードをスケジュールする 927
NetScalerインスタンスのHAペア構成をスケジュールする 928
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 929
インスタンスアドバイザリ 930
アップグレードアドバイザリ (プレビュー) 930
アップグレードアドバイザリの表示 930
セキュリティアドバイザリ (プレビュー) 931
セキュリティアドバイザリの表示 931
セキュリティアドバイザリでサポートされているCVE 932
オーケストレーション 935
ヴイエムウェア NSX マネージャー 936
Cisco ACIハイブリッドモード 937
OpenStack: NetScalerインスタンスの統合 937
OpenStack Neutron LBaaS用NetScalerドライバー 938
NetScaler ADMとOpenStackの相互登録 938
OpenStackのテナント 938

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

配置ポリシー 938
サービスパッケージ 938
LBaaS V1およびLBaaS V2でサポートされる機能 939
ユースケースシナリオ 940
NetScaler ADMとOpenStackワークフローの統合 941
OpenStack: NetScalerインスタンスの統合 941
前提条件 945
NetScaler® ADM および OpenStack での事前構成タスク 946
Horizonを使用してLBaaS V1を設定する 954
コマンドラインを使用してLBaaS V2を構成する 955
レイヤー7コンテンツスイッチングを構成する 959
OpenStackでのNetScaler VPXインスタンスの手動プロビジョニング 967
StyleBookを使用したOpenStackでのNetScaler VPXインスタンスのプロビジョニング969
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 971
管理パーティションの共有VLANサポート 972
トライアルライセンスのワークフロー 973
OpenStack Heatサービスとの統合 974
サービスパッケージの分離ポリシー 978
柔軟なポリシーベースのデバイス割り当て 980
NSX Manager: NetScalerインスタンスの手動プロビジョニング 983
前提条件 984
VMware ESXi のハードウェア要件 984
VMware NSXの構成 985
NetScaler ADMでのNetScaler VPXインスタンスの追加 986
NetScaler ADMへのVMware NSX Managerの登録 986
NetScaler ADMでのサービスパッケージの作成 987
エッジのロードバランサーサービス挿入の実行 988

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

NSX ManagerでのL2ゲートウェイの表示 990
割り当てられたNetScalerの表示 990
StyleBookを使用したNetScaler VPXインスタンスの構成 991
ロードバランサー構成の表示 991
ロードバランサーサービスの削除 992
NSX Manager: NetScalerインスタンスの自動プロビジョニング 992
概要 992
前提条件 993
NetScaler ADMおよびNetScalerインスタンスの高可用性展開 993
NetScaler® ADM HAエンドポイントの詳細設定 993
VMware NSX ManagerをNetScaler ADMに登録する 994
NetScaler ADMでのライセンスのアップロード 994
NetScaler ADM で NetScaler VPX イメージをアップロードする 995
NetScaler ADM でサービスパッケージを作成する 995
Edge向けロードバランサーサービス挿入の実行 997
VMware NSX Manager GUIでNetScaler VPXの負荷分散サービスを構成する 999
NetScaler ADM GUIでのNetScaler VPXにおけるロードバランシングサービスの設定 1000
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 1000
ロードバランシングサービスの削除 1001
NetScaler ADM を使用した Cisco ACI ハイブリッドモードでの NetScaler の自動化 1001
前提条件 1002
Cisco APICとNetScaler ADMを使用してNetScalerをハイブリッドモードで構成する 1003
APIC 障害レポート 1025
NetScaler® ADM によって生成されたログ 1025
ハイブリッドモードデバイスパッケージによって生成されたログ 1030
Cisco ACIのクラウドオーケストレーターモードにおけるNetScalerデバイスパッケージ 1034
NetScaler® ADM で Kubernetes Ingress 構成を管理する 1037
開始する前に 1038

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

シークレットトークンを使用してNetScaler ADMを構成し、Kubernetesクラスターを管理する 1039
NetScaler ADMにKubernetesクラスターを追加する 1039
ビデオインサイト 1040
Video Insight の構成 1041
サンプル 1042
NetScaler ADM で Video Insight メトリックを表示する 1042
ネットワーク効率を表示 1043
最適化されたABRビデオと最適化されていないABRビデオが使用するデータ量を比較する 1044
ネットワークからストリーミングされたビデオの種類と消費されたデータ量を表示する 1044
ABRビデオの最適化された再生時間と最適化されていない再生時間を比較する 1045
最適化されたABRビデオと最適化されていないABRビデオの帯域幅消費量を比較する 1046
ABRビデオの最適化された再生回数と最適化されていない再生回数を比較する 1047
特定の時間枠のピークデータレートを表示する 1047
IPアドレス管理 (IPAM) の構成 1049
外部IPアドレスプロバイダーの追加 1049
ネットワークを追加する 1050
割り当てられたIPアドレスを表示する 1051
インフラストラクチャの管理と監視にADM監査ログを使用する 1052
ADCインスタンス関連の監査ログ 1052
ADMサービスをsyslogサーバーとして構成する 1052
ADM関連の監査ログ 1053
アプリケーション関連の監査ログ 1053
インスタンスライセンスの管理 1054
NetScaler プール型キャパシティ 1054
NetScalerプール型キャパシティライセンスの仕組み 1055
ゼロキャパシティハードウェア 1055
プラットフォームライセンスの管理とインストール 1056

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

スタンドアロンNetScaler VPXインスタンス 1056
スタンドアロンのNetScaler CPXインスタンス 1057
スタンドアロンのNetScaler BLXインスタンス 1058
帯域幅プール 1058
インスタンスプール 1058
NetScaler ADMライセンスサーバー 1058
表1。MPXおよびSDXインスタンス用のサポートされているプール型キャパシティ 1059
表2. CPXインスタンスでサポートされるプール容量 1063
表3. ハイパーバイザーおよびクラウドサービス上のVPXインスタンスでサポートされるプール容量 1063
表4. BLXインスタンス向けにサポートされるプール容量 1064
表 5. 異なるフォームファクターのライセンス要件 1064
NetScaler プールキャパシティの構成 1065
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 1066
ADCプール容量の状態 1066
ステップ1 - ADMでライセンスを適用する 1066
ステップ2 - NetScaler ADMをライセンスサーバーとして登録する 1067
ステップ 3 - プールされたライセンスをADCインスタンスに割り当てる 1070
ADCインスタンスでプールされたキャパシティを構成する 1071
ADMサーバーをプール型ライセンスサーバーとしてのみ構成する 1073
ADMサーバーをプール型ライセンスサーバーとしてのみ構成する方法 1074
NetScaler VPX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 1076
前提条件 1077
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 1078
NetScaler MPX の永続ライセンスを NetScaler Pooled Capacity にアップグレードする 1080
NetScaler MPX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 1083

© 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 1085
クラスターモードのNetScalerインスタンスにおけるNetScaler pooled capacity 1088
ADCクラスターにADCプール容量を割り当てる 1089
CLI を使用して ADC プール容量を ADC クラスターに割り当てる 1090
ヘルスモニタリング 1091
猶予期間 1092
通知とアラーム 1092
問題発生時の予期される動作 1093
ライセンスサーバーが応答を停止する 1094
NetScalerプール容量対応インスタンスが応答を停止する 1094
ライセンスサーバーとNetScalerプール容量対応インスタンスの両方が応答を停止する 1094
NetScalerプール容量対応インスタンスが正常にシャットダウンする 1094
ネットワーク接続が失われる 1095
プール型キャパシティライセンスの有効期限チェックを設定する 1095
NetScaler VPXおよびBLXライセンスのチェックインとチェックアウト 1097
前提条件 1098
NetScaler ADMでのライセンスのインストール 1098
検証 1099
NetScaler GUIを使用して、VPXおよびBLXライセンスをADCインスタンスに割り当てる 1099
NetScaler CLI を使用して ADC インスタンスに VPX および BLX ライセンスを割り当てる 1100
APIを使用してADCインスタンスにVPXおよびBLXライセンスを割り当てる 1101
ライセンスサーバーのIPアドレスを更新する 1102
NetScaler VPXおよび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 1102
NetScaler仮想CPUライセンス 1103
NetScaler VPX の仮想 CPU ライセンス 1104
CLIを使用したNetScaler VPXライセンスでのライセンスサーバーの構成 1106
ライセンスサーバーのIPアドレスを更新する 1106

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

NetScaler ADMでの仮想CPUライセンスの管理 1107
NetScaler CPXの仮想CPUライセンス 1107
システム設定の管理 1110
ネットワーク構成 1110
システム構成 1111
システムメンテナンス 1112
データプルーニング 1112
バックアップ 1113
イベント通知 1114
SSL設定 1114
機能の構成 1115
システムバックアップ設定の構成 1115
NTPサーバーを構成する 1115
NetScaler® Application Delivery Management (ADM) のアップグレード 1117
NetScaler® ADM のパスワードをリセットする方法 1117
NetScaler® ADM にアクセスするためのセカンダリ NIC の構成 1121
前提条件 1122
NetScaler ADM で2番目の NIC を構成する 1122
ADMエージェントにアクセスするためのセカンダリNICを構成する 1123
CLIを使用してIPV4 NICネットワークアドレスを変更する 1124
Syslogパージ間隔の設定 1124
システムプルーニングとイベントプルーニングの設定 1125
NetScaler® ADM を使用してイベントの削除設定を構成する 1126
デフォルト以外のユーザーのシェルアクセスを有効にする 1127
アクセスできない NetScaler® ADM サーバーを復旧する 1127
NetScaler ADMスタンドアロン展開におけるNetScaler ADMデータベースリカバリスクリプトの使用方法 1128

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

NetScaler ADM高可用性展開でNetScaler ADMデータベースリカバリスクリプトを使用する方法 1130
NetScaler® ADMサーバーにホスト名を割り当てる 1130
NetScaler® ADMサーバーのバックアップと復元 1131
NetScaler ADM構成をバックアップする 1132
NetScaler ADMバックアップファイルを外部システムに転送する 1133
バックアップファイルからNetScaler ADM構成を復元する 1133
高可用性展開におけるNetScaler® ADMのVMスナップショット 1134
NetScaler ADMサーバーのスナップショットを取得する 1134
NetScaler ADMサーバーのスナップショットを復元する 1135
監査情報の表示 1135
SSL設定を構成する 1137
CPU、メモリ、ディスクの使用状況を監視する 1137
通知設定を構成する 1137
メール配信リストを作成する 1138
SMS配信リストを作成する 1139
Slackプロファイルの作成 1139
PagerDutyプロファイルを作成する 1140
ServiceNowプロファイルの表示 1140
テックサポートファイルを生成する 1141
暗号グループを構成する 1143
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 1143
システムアラームの設定と表示 1145
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 1146
SNMP v2マネージャーを追加する 1146
SNMP v3マネージャーを追加する 1147
SNMPユーザーを追加 1147
SNMPビューの管理 1148

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

エージェント設定の構成 1149
エージェントのキープアライブ間隔を設定する 1149
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 1149
NetScaler® ADM を API プロキシサーバーとして 1150
NetScaler ADM が API プロキシサーバーとして機能する方法 1150
NetScaler ADM を API プロキシサーバーとして使用する方法 1152
例 1: 負荷分散仮想サーバーの統計情報を取得する 1155
例 2: 負荷分散仮想サーバーを作成する 1156
例 3: 負荷分散仮想サーバーを変更する 1156
例 4: 負荷分散仮想サーバーを削除する 1157
例 5: ADC 上の CLI 実行構成をダウンロードする 1157
よくある質問 1159
アナリティクス 1159
シングルホップモードで展開されている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? 1159
NetScaler ADM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? 1159
NetScalerインスタンスを追加した後、NetScaler ADMは分析情報の収集を自動的に開始しますか? 1160
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? 1160
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? 1160
NetScaler ADMにディスクを追加する方法? 1160
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? 1161
クライアント側測定を有効にするとどうなりますか? 1161
認証 1161
認証リクエストの負荷分散とは何ですか? 1161
外部認証サーバーをカスケードする必要があるのはなぜですか? 1162
外部認証サーバーをいくつカスケードできますか? 1162

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

外部認証が失敗した場合の代替手段はありますか? 1162

フォールバックローカル認証とは何ですか? 1162

外部ユーザーグループの抽出とは何ですか? 1162

グループ権限を割り当てる必要があるのはなぜですか? 1163

構成管理 1163

NetScaler ADM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? 1163

NetScaler ADMの構成ジョブとは何ですか? 1163

NetScaler ADM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? 1163

証明書管理 1164

NetScaler ADMからSSL証明書を削除すると、NetScalerインスタンスから証明書が削除されますか? 1164

展開 1164

デフォルトのユーザー名とパスワードは何ですか? 1164

デフォルトのパスワードを変更する方法? 1164

パスワードをリセットする方法は? 1165

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ペアの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? 1165

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、これらの2つのサーバーをHAペアに展開する際にどのような影響があります? 1165

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。原因は何ですか? 1165

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。原因は何ですか? 1165

NetScaler ADMスタンドアロンおよびNetScaler ADM HAでサポートされているDB? 1165

セカンダリノードへの潜在的なデータ損失? 1166

プライマリノードがダウンした場合、どうなりますか? 1166

障害が発生したノードを再インストールする方法? 1166

NetScaler ADMはSANストレージをサポートしていますか? 1166

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

NetScaler ADMは追加ディスクをサポートしていますか? 1166

HAペアを無効にした後、設定されたフローティングIPアドレスはどうなりますか? 1167

再デプロイ中に別のフローティングIPアドレスを指定できますか? 1167

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? 1167

プライマリノードが長期間ダウンしている場合でも、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? 1167

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? 1167

ADMはAMDプロセッサをサポートしていますか? 1168

展開（ディザスタリカバリ） 1168

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? 1168

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? 1168

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? 1168

イベント管理 1169

NetScaler ADM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? 1169

イベントルールとは何ですか? 1169

インスタンス管理 1169

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ADCインスタンスがADMに接続できない場合はどうなりますか? 1169

NetScaler ADMのデータセンターとは何ですか? 1169

NetScaler ADMでサポートされているNetScaler ADCアプライアンスにはどのようなものがありますか? 1170

インスタンスプロファイルとは? 1170

NetScaler ADMで複数のNetScaler VPXインスタンスを再検出できますか? 1170

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

NetScaler ADMをNetScaler SDXにインストールできますか? 1171

パブリックIPアドレスを使用して、ADMソフトウェアにNetScalerインスタンスを追加できますか? 1171

DRノードの資格情報が変更された場合、災害復旧ノードを登録するにはどうすればよいですか? 1171

StyleBooks 1172

StyleBooksは、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するために使用できますか? 1172

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、どうなりますか? 1172

NetScalerを介して作成されたNetScalerバックアップには、StyleBooksを介して適用された構成が含まれます? 1172

システム管理 1172

NetScaler ADMサーバーにホスト名を割り当てることはできますか? 1172

NetScaler ADMの構成をバックアップおよび復元できますか? 1172

NetScaler ADMのしきい値とアラートとは何ですか? 1173

NetScaler ADMのテクニカルサポートファイルを生成できますか? 1173

Syslogパージとは何ですか? 1173

NetScaler ADMでNTPサーバーを設定できますか? 1173

NetScaler ADM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? 1174

NetScaler ADM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アプライアンスを設定していました。この構成を更新するにはどうすればよいですか? 1174

ポート443を使用してNetScalerインスタンス上でNetScaler ADM HAペアのロードバランシングを構成できますか? 1174

NetScaler ADMサーバーのバックアップファイルを使用して、別のNetScaler ADMサーバーの構成を復元できますか? 1174

NetScaler ADM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 ADMを介して別のNetScalerインスタンスの構成を復元できますか?1175

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

NetScaler ADM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 ADMを強制できますか? 1175

NetScaler ADMでNetScalerインスタンスをバックアップする場合、結果は完全バックアップですか、それとも基本バックアップですか? 1175

NetScaler ADMのトラブルシューティングガイドはありますか? 1175

NetScaler ADM HAフェイルオーバーが発生した場合、NetScalerインスタンスはどのように管理されますか? 1175

NetScaler ADM HAノードがダウンから復旧した場合の動作? 1176

NetScaler ADM HAノード間でのNetScalerインスタンスの分散方法? 1176

NetScaler ADM 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? 1176

NetScaler ADM HAセットアップにはロードバランサーが必須ですか? 1176

NetScaler ADMは外部データベースをサポートしていますか? 1176

NetScaler ADMによって管理されているNetScalerインスタンスを、NetScaler ADM HAのロードバランサーとして使用できますか? 1176

NetScaler ADM HAノード間でどのようなデータが同期されますか? 1176

index 1178

適応型しきい値を設定する 1178

NetScaler® ADM を使用して適応型しきい値を作成するには 1179

データベース集約を構成する 1179

データベース集約を構成するには 1179

SLA管理を構成する 1180

NetScalerインスタンスのSLA違反を設定するには 1180

しきい値とアラートを作成する 1181

NetScaler ADMを使用してしきい値とアラートを作成するには 1181

URLデータ収集を無効にする 1181

NetScaler ADMからURLデータ収集を無効にするには 1182

Logstream の概要 1182

Logstreamをトランスポートモードとして有効にする 1182

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

ダッシュボード 1184
アウトバウンドトラフィックダッシュボード 1184
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 1185
ユーザーダッシュボード 1185
ユーザーアクティビティインベスティゲーター 1186
ユーザー トランザクション 1186
リスクスコア 1187
すべての違反 1188
違反カテゴリ 1188
セキュリティ違反ダッシュボード 1190
違反の詳細 1190
アプリケーションの概要 1191
違反カテゴリ 1191
WAF違反の詳細を表示 1193
ボット違反の詳細を表示 1194
イベント履歴の表示 1195
ネットワーク違反の詳細 1195
HTTP スローロリス 1195
DNS スローロリス 1196
HTTPスローポスト 1196
NXDOMAINフラッド攻撃 1197
HTTP デシンク攻撃 1198
ブライヒェンバッハー攻撃 1199
セグメントスマック攻撃 1199
SYNフラッド攻撃 1200
スモールウィンドウ攻撃 1200
SSLインサイト 1201
前提条件 1202

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

SSL Insightの構成 1202
AppFlow機能を有効にする 1202
SSL Insightパラメータを有効にする 1204
SSL Insightメトリックを表示する 1205
ユースケース: SSLトランザクションの概要を取得する 1205
ユースケース: クライアント向けSSLメトリック 1206
TCP インサイト 1206
前提条件 1207
TCP Insightの有効化 1207
NetScaler ADMでTCP Insightメトリックを表示する 1207
ユースケース 1208
TCP最適化の利点を評価する 1208
TCPパラメータを調整する 1208
トラフィック量に対するTCP最適化の影響を測定する 1209
Web Insight の問題のトラブルシューティング 1209
データなしの診断 1209
Web Insight ダッシュボードレポートに関連する問題 1210
設定の問題 1210
NetScalerとNetScaler ADM間の接続の問題 1210
NetScalerからAppFlowデータが受信されない 1211
ライセンスの問題 1211
観測ポイントIDの問題 1211
AppFlowパラメータの欠落に関する問題 1212
カウンターを使用してトラブルシューティング 1213
Webトランザクションの分析を表示 1213
詳細なWebトランザクション 1214
イベントの表示 1214
イベントリストに列を追加 1216

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

高度な検索 1216
検索を保存 1218
データのエクスポート 1218
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セットアップするための詳細な手順 1219
ソフトウェア要件 1219
始める前に 1219
ソフトウェア要件 1220
始める前に 1220
NetScaler ADM で静的ルートを構成する 1221
GitHub からサンプル展開ファイルをダウンロードする 1222
CPX YAMLファイルにパラメータを追加する 1222
NetScaler ADMにVPX、SDX、MPX、またはBLXインスタンスを追加する 1224
NetScaler ADMにKubernetesクラスターを追加する 1224
サンプルマイクロサービスアプリケーションの展開 1226
CPXを展開し、ADMにCPXを登録する 1226
ライセンス付与のために仮想サーバーの自動選択を有効にする 1226
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 1227
マイクロサービスにトラフィックを送信する 1227
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 1228
NetScaler® ADMで静的ルートを構成する 1228
必要なパラメータを構成します 1229
サンプルアプリケーションを展開する 1231
NetScaler ADMでKubernetesクラスターを追加する 1233
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 1234
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 1235
マイクロサービスにトラフィックを送信する 1235
NetScaler® テレメトリープログラムのオプションのテレメトリーデータ 1236
NetScaler Console の機能使用状況 1236

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

NetScaler® テレメトリープログラムに必要なテレメトリーデータ 1243
ライセンス 1243
NetScaler Gateway の機能使用状況 1247
NetScalerの展開 1247
NetScaler機能の使用状況 1249
データガバナンス 1257
顧客IDの構成 1258
ワークフロー 1 - 新規ユーザーの場合 1258
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 1258
診断とデータ収集 1259
データが収集される理由? 1260
このデータを使用できるのは誰ですか? 1260
お客様のデータをどのくらいの期間保持しますか? 1260
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 1260
顧客ユーザーエクスペリエンス改善プログラム 1261
CUXIPで収集される使用状況データとは? 1261
CUXIPはどのように役立ちますか? 1261
CUXIPの仕組み? 1262
ADMでCUXIPを無効にする方法? 1262
プライバシーポリシーの変更 1262
参照 1262
HAペアでのNetScaler® ADM構成のバックアップと復元 1262
システム通知設定を構成する 1263
ジオマップのサイトを構成する 1265
fix 1267

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

リリースノート

NetScaler Console 13.1 のリリースノートでは、新しい機能、既存機能の強化、およびビルドにおける既知の問題について説明します。13.1 リリースのリリースノートドキュメントには、次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と、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 の特定と修復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 13.1 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、次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 13.1 のリリースノート	公開日
ビルド 13.1-62.27	Mar 25, 2026
ビルド 13.1-61.28	Mar 26, 2026
ビルド 13.1-60.33	Mar 26, 2026
ビルド 13.1-59.19	Jun 25, 2025
ビルド 13.1-58.32	Jun 17, 2025
ビルド 13.1-57.26	Feb 04, 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 13.1 のリリースノート	公開日
ビルド 13.1-56.18	Nov 18, 2024
ビルド 13.1-55.29	Sep 23, 2024
ビルド 13.1-54.29	Jul 22, 2024
ビルド 13.1-53.24	Jul 09, 2024
ビルド 13.1-52.19	Mar 12, 2024
ビルド 13.1-51.14	Dec 14, 2023
ビルド 13.1-50.23	Oct 20, 2023
ビルド 13.1-49.13	Jul 18, 2023
ビルド 13.1-48.47	Jun 14, 2023
ビルド 13.1-45.61	Apr 26, 2023
ビルド 13.1-42.47	Mar 23, 2023
ビルド 13.1-37.38	Dec 01, 2022
ビルド 13.1-33.50	Oct 31, 2022
ビルド 13.1-30.52	Oct 31, 2022
ビルド 13.1-27.62	Oct 31, 2022
ビルド 13.1-24.38	Oct 31, 2022
ビルド 13.1-21.53	Oct 31, 2022
ビルド 13.1-17.42	Oct 31, 2022
ビルド 13.1-12.50	Oct 31, 2022
「ビルド 13.1-9.60」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-	Oct 31, 2022

© 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 13.1 のリリースノート	公開日
prem%2520%28ADM%29&version=13.1&build=9.60)	
「ビルド 113.1-4.43」(https://docs.netscaler.com/ja-jp/updates?product=NetScaler%2520Console%2520on-prem%2520%28ADM%29&version=13.1&build=4.43)	Sep 14, 2021

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

オンプレミス NetScaler ADM を Citrix Cloud™ に移行する

オンプレミスの **NetScaler ADM 13.0 64.35 以降のバージョン** を Citrix Cloud に移行できます。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。

Citrix Cloud を介した ADM サービスでは、次の機能を利用できます。

- 最新の機能アップデートを含む、約2週間ごとの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、および使用状況に関する機械学習ベースの分析。
- ピークおよび閑散期の分析、アプリケーションセキュリティとボット向けの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 ADM サービスでのみサポートされているその他さまざまな機能。

移行を成功させるには、次の操作を行う必要があります。

- Citrix Cloud へのアクセスを可能にするため、オンプレミス ADM でインターネット接続があることを確認する
- ADM サービスエージェントを構成する
- Citrix Cloud からクライアントとシークレットの CSV ファイルを取得する
- ADM サービス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

オンプレミス ADM から ADM サービスに移行した後、再度オンプレミス ADM 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、オンプレミス ADM へのロールバック を参照してください。

ADM サービスエージェントを構成する

NetScaler インスタンスと NetScaler ADM 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

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

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、エージェントのアップグレード設定の構成 を参照してください。

- 既存のオンプレミスADM (スタンドアロンまたはHAペア) にオンプレミスエージェントが構成されていない場合は、ADM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。
- 既存のオンプレミスADM (スタンドアロンまたはHAペア) にマルチサイト展開用にオンプレミスエージェントが構成されている場合は、ADM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からクライアントとシークレットの 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とシークレットの 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、オンプレミスADMにCSVファイルを保存します。

   たとえば、CSVファイルを/varディレクトリに保存します。

ADMサービスライセンスを検証する

ADMサービス用にライセンスを取得する必要があります。

- ADMサービスのVIPライセンスは、オンプレミス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、仮想サーバーはランダムに選択され、ADMサービスのVIPレベルの構成は失敗します。

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

- ADM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は、移行前にライセンスをADMサービスに再割り当てしてください。詳細については、プールされたライセンスサーバーとしてのみADMサーバーを構成する および ライセンスファイルを再割り当てする方法 を参照してください。
- オンプレミスADMでプールされたライセンスを使用している場合は、ADMサービス用のプールされたライセンスを取得し、ADC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、プールされたライセンスの構成 を参照してください。ADMからライセンス割り当てを変更できるサポート対象のADC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

- ADM 82.xビルドを使用すると、機能を選択して移行できます。
- ADM 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利用可能で、`cd /mps/scripts` で入手できます。
- ADM 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、オンプレミスADMにスクリプトをコピーする必要があります。

  注

  > 移行中は、オンプレミスADMにインターネット接続があ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、オンプレミスADMにログオンします。

   注

   > ADM HAペアの場合は、プライマリノードにログオンします。

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. クライアントIDとシークレット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。

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

CSVを追加(/en-us/netscaler-application-delivery-management-software/media/csv-add-adm.png)

注

> ADM 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. ADM **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 ADM VM>`

   例: `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。

   機能ごとの移行オプション(/en-us/netscaler-application-delivery-management-software/media/migrate-options.png)

   指定した選択に基づいて、その機能のみがADMサービスに移行されます。

   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。

   移行完了(/en-us/netscaler-application-delivery-management-software/media/migrate-option-complete.png)

   管理および監視 (M&M) 機能には以下が含まれます。

   - ADC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。
   - 設定監査テンプレート、ポーリング間隔、イベントルールと設定。
   - 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。

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

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

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、すで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**機能の移行を完了した場合、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. ADM **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 ADM VM>`

   例: `python servicemigrationtool.py /var/secureclient.csv`
6. ADM 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、`servicemigrationtool_27.py` と `config_collect_onprem_27.py` の2つのバンドルスクリプトが含まれています。
   b. 2つのスクリプトをオンプレミスADMに保存します。例えば、/var ディレクトリに保存します。
   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 on-premises ADM VM>`

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

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

スクリプトを実行すると、前提条件がチェックされ、その後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ADM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することで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。

プールライセンスサーバーにサポートされていないADCインスタンスバージョンがある場合、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することで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** を選択した場合、スクリプトは移行を停止します。

オンプレミスの構成によっては、移行が完了するまで数分から数時間かかります。移行が完了すると、以下のメッセージが表示されます。

移行完了ステータス(/en-us/netscaler-application-delivery-management-software/media/migration-complete-status.png)

すべてのADCインスタンスとそのそれぞれの構成がADM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® ADMは以下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

オンプレミスADMへのロールバック

オンプレミスADM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。

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

前提条件

オンプレミスADM（ADMサービスへの移行前）が次のいずれかの場合：

- プールされたライセンスサーバーとして使用されている場合は、オンプレミスADMに必要なプールされたライセンスがあることを確認してください。
- オンプレミスADMエージェントで構成されている場合は、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、プールされたライセンスの同じ構成（移行前）が、オンプレミスADM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、これらの変更はオンプレミスADMには反映されません。

- **ADM 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。
- **79.xxより前のADM**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オンプレミスADMに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、オンプレミスADM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. ADM **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 ADM on-prem VM>` を実行します

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

   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。

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

4. 82.xxビルドより前のADMの場合:

   a. 以下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. ADM 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、以下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 ADM on-prem>`

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

   c. 76.xxビルドより前のADMの場合、スクリプトをオンプレミスADMに保存します。たとえば、`/var`の場所に保存し、以下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 ADM on-prem>`

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

   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。

よくある質問

ADMサービス

ADMサービスエージェントは、オンプレミスNetScalerエージェントと同様にオプションですか?

いいえ。ADMサービスエージェントはADMサービスに必須であり、インスタンスとADMサービス間のすべての通信はADMサービスエージェントを介して行われます。オンプレミスADMエージェントはオプションですが、帯域幅の消費を節約するためだけにオンプレミスエージェントを構成できます。

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

ADMサービスを使用する理由?

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

- オンプレミスNetScaler® ADMよりも簡単なオンボーディングと低い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、および使用状況に関する機械学習ベースの分析。
- ピークおよび閑散期の分析、WAFおよび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ADM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NetScaler ADMがHAペアの場合、移行後に何が起こりますか?

すべての構成はCitrix Cloudに移動されます。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イ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ADM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ADM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。

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。オンプレミスADMからデータを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。オンプレミスのライセンスファイルはADMサービスでは使用できません。ADM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ADMでプールライセンスを使用している場合は、ADM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NetScaler ADMから移行されないものは何ですか?

以下の機能はADMサービスに移行できません。

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

- **RBAC** – ADM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。ADM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ADM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** – ADMサービスはADC 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NetScaler ADMにアップロードされたSSL証明書/キーはADMサービスに移行されません。

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

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

移行後、インスタンスのライセンス供与や分析の有効化が再度必要になりますか?

ADM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NetScaler ADM VIPよりも多い場合、仮想サーバーは自動的にライセンス供与されます。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。

移行ツール

移行スクリプトの実行後、エラーメッセージが表示されます。何が問題でしょうか?

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、移行スクリプトを再度実行できます。一般的に、移行スクリプトを実行する前に、以下を確認してください。

- ADMサービスエージェントを構成する
- ADMサービスライセンスを取得する
- クライアントおよびセキュアCSVファイルを保存した正しいパスをコピーする

ADC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オプション「Y」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のバージョンでのみ行われます。

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

ADCインスタンスに関する構成が移行スクリプトで失敗した場合、どうなりますか?

ADCインスタンスはオンプレミスのADM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、移行スクリプトを再度実行できます。

一部のADCインスタンスがADMサービスへの移行に失敗した場合、どうなりますか。移行スクリプトを再実行すると解決しますか?

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。例えば、5つのインスタンスのうち2つが移行に失敗したとします。是正措置を講じて移行スクリプトを再実行すると、以前に正常に移行された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、以前に失敗した残りの2つのインスタンスは正常に移行されます。

移行ステータスを確認するためのログファイルはありますか?

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ADMではログファイルは `servicemigrationtool.py.log`、python2.7を使用するADMではログファイルは `servicemigrationtool_27.py.log` となります。

移行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?

移行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、移行はさらに続行されます。

ADMサービスがオンプレミスNetScaler ADM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、ライセンスが不足していることを示す提案が表示され、続行するか停止するかのプロンプトが表示されます。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NetScaler ADMがADMサービスExpressアカウントに移行された場合、どうなりますか?

ADM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ADMがこれ以上の構成を持っており、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。

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

Citrix Cloudに招待されたユーザー（Citrix Cloudアカウントを作成した管理者ユーザー以外）がオンプレミスADMセットアップの移行を試みた場合、どうなりますか?

管理者が移行スクリプトを実行することをお勧めします。招待されたユーザーは管理者権限（adminExceptSystem_group）を持っていません。その結果、グループ、ロール、およびポリシーの移行は失敗し、「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、招待された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

オンプレミスADM HAペアでロールバックスクリプトを使用した場合、どうなりますか?

オンプレミスADM 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。

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ため、一部の設定がすでにADMサービスに移行されている可能性があります。
- 移行スクリプトを実行する前に、ADMサービスで同じ設定を手動で作成した可能性があります。

次のエラーメッセージの一部を参照してください。

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

ADMサービスに追加された手動プロファイル

手動プロファイルの追加(/en-us/netscaler-application-delivery-management-software/media/manual-profile-add.png)

回避策: 移行スクリプトを実行する前にNetScaler® ADM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。

ADMサービスに追加されたNetScalerデバイス

手動ADCデバイスの追加(/en-us/netscaler-application-delivery-management-software/media/manual-adc-add.png)

回避策: オンプレミスADM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ことを確認してください。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。

StyleBookカスタムテンプレートのADMサービスへのインポート

手動StyleBookの追加(/en-us/netscaler-application-delivery-management-software/media/stylebook-import-add.png)

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 ADM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。

ADMサービスに追加された構成ジョブ

構成ジョブの手動追加(/en-us/netscaler-application-delivery-management-software/media/config-jobs-add.png)

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。

ADMサービスに追加されたIPブロック

IPブロックの手動追加(/en-us/netscaler-application-delivery-management-software/media/ip-blocks-add.png)

回避策：ADM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。

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

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

ネットワークダッシュボードの手動追加(/en-us/netscaler-application-delivery-management-software/media/network-dashboard-add.png)

回避策：ADM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 ADM) の「ハウツー記事」は、NetScaler ADM 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、分析などの人気のある NetScaler ADM 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すると、その機能のハウツー記事のリストが表示されます。

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 ADM 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

NetScaler ADMにインスタンスを追加する方法

NetScaler ADMでインスタンスグループを作成する方法

NetScaler ADMでGeomapsのサイトを構成する方法

NetScaler ADM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

NetScaler ADM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

NetScaler ADM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

複数のNetScaler VPXインスタンスを再検出する方法

NetScaler ADM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

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

NetScaler ADMでインスタンスの管理を解除する方法

NetScaler ADMからインスタンスへのルートをトレースする方法

構成管理

NetScaler ADMで構成ジョブを作成する方法

構成ジョブでSCP (put) コマンドを使用する方法

NetScaler ADM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

NetScaler ADM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/13-1/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/13-1/networks/configuration-jobs/how-to-reuse-executed-configuration-jobs.html)

NetScaler ADM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/13-1/networks/configuration-jobs/how-to-upgrade-netscaler-instances.html)

NetScaler ADMの構成ジョブで変数を使用する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/configuration-jobs/how-to-use-variables.html)

NetScaler ADM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/13-1/networks/configuration-jobs/use-configuration-templates-to-create-audit-templates.html)

NetScaler ADM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/13-1/networks/configuration-jobs/how-to-create-jobs-from-corrective-commands.html)

NetScaler ADM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/13-1/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/13-1/networks/configuration-jobs/record-and-play.html)

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

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/13-1/networks/configuration-jobs/replicate-configuration.html)

NetScaler ADM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/13-1/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/13-1/networks/configuration-audit/how-to-poll-configuration-audit-of-netscaler-instances.html)

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/13-1/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/13-1/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/13-1/networks/configuration-audit/generate-configuration-audit-diff-for-configchange-snmp-traps.html)

証明書管理

NetScaler ADMでエンタープライズポリシーを構成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-configure-enterprise-policy.html)

NetScaler ADM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(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-install-ssl-certificates-on-netscaler-instance.html)

NetScaler ADMからインストール済みの証明書を更新する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-update-an-installed-certificate.html)

NetScaler ADM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(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-link-and-unlink-ssl-certificates.html)

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

NetScaler ADMを使用して証明書署名要求 (CSR) を作成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-create-csr.html)

NetScaler ADMからSSL証明書の有効期限通知を設定する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-set-up-notificationsfor-ssl-certificate-expiry.html)

NetScaler ADMでSSLダッシュボードを使用する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-use-ssl-dashboard.html)

NetScalerインスタンスからSSL証明書をポーリングする方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/ssl-certificate-dashboard/how-to-poll-ssl-certificates-from-netscaler-instances.html)

StyleBooks

StyleBooksのさまざまなグループを表示する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-view-stylebooks.html)

独自のStyleBooksを作成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-create-custom-stylebooks.html)

NetScaler ADMでユーザー定義のStyleBooksを使用する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-create-custom-stylebooks/how-to-use-custom-stylebooks.html)

APIを使用してStyleBooksから構成を作成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks.html)

StyleBookで定義された仮想サーバーで分析を有効にし、アラームを構成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-create-custom-stylebooks/how-to-enable-analytics-on-virtual-server-defined-in-stylebooks.html)

NetScaler ADM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(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-create-custom-stylebooks/how-to-create-a-stylebook-to-upload-files-to-netscaler-mas.html)

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方法

SSL 証明書と証明書キーファイルを NetScaler ADM にアップロードする StyleBook を作成する方法

© 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構成を作成する方法

企業で Microsoft Skype for Business StyleBook を使用する方法

企業で Microsoft Exchange StyleBook を使用する方法

企業で Microsoft SharePoint StyleBook を使用する方法

分析

インスタンスで分析を有効にする方法

適応型しきい値を構成する方法

SLA 管理を構成する方法

分析のためにデータベースの要約を構成する方法

NetScaler ADM を使用してしきい値とアラートを作成する方法

NetScaler ADM から分析用の URL データ収集を無効にする方法

ストリーミングされたビデオの種類とネットワークから消費されたデータ量を表示する方法

特定の期間のピークデータレートを表示する方法https://author-p185304-e1959167.adobeaemcloud.com/ja-jp/netscaler-application-delivery-management-software/13-1/analytics/video-insight/view-peak-data-rate-specific-time-frame.html

ネットワーク効率を表示する方法

イベント管理

NetScaler ADM上のイベントのイベント期間を設定する方法

NetScaler ADM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 ADM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 ADMを使用してイベントを抑制する方法

イベントダッシュボードを使用してイベントを監視する方法

NetScaler ADM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

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

NetScaler ADMでイベントの概要を表示する方法

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

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

NetScaler ADM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ニング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

TACACS認証サーバーを追加する方法

NetScaler ADMで認証サーバーグループを抽出する方法

フォールバックローカル認証を有効にする方法

NetScaler ADMシステム

NetScaler ADMをアップグレードする方法

NetScaler ADMのパスワードをリセットする方法

NetScaler ADMのテクニカルサポートファイルを生成する方法

シングルサーバー展開でNetScaler ADMサーバーをバックアップおよび復元する方法

HAペアでNetScaler ADM構成をバックアップおよび復元する方法

NetScaler ADM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

NetScaler ADMでNTPサーバーを構成する方法

NetScaler ADMのSSL設定を構成する方法

NetScaler ADM の syslog パージ間隔を構成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/manage-system-settings/how-to-configure-syslog-purging-interval.html)

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

NetScaler ADM の監査情報を表示する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/manage-system-settings/how-to-view-auditing-information-of-mas.html)

NetScaler ADM のシステム通知設定を構成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/manage-system-settings/how-to-configure-system-settings-of-mas.html)

NetScaler ADM 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/13-1/manage-system-settings/how-to-monitor-cpu-memory-disk-usage-of-mas.html)

NetScaler ADM の暗号グループを構成する方法(/ja-jp/netscaler-application-delivery-management-software/13-1/manage-system-settings/how-to-configure-cipher-group-for-mas.html)

NetScaler ADM 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/13-1/manage-system-settings/how-to-create-snmp-traps-managers-users-mas.html)

NetScaler ADM サーバーにホスト名を割り当てる方法(/ja-jp/netscaler-application-delivery-management-software/13-1/manage-system-settings/how-to-assign-host-name-to-mas-server.html)

NetScaler ADM 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/13-1/manage-system-settings/configure-system-prune-settings-mas.html)

NetScaler ADM 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/13-1/manage-system-settings/configure-system-backup-settings.html)

NetScaler ADM 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/13-1/manage-system-settings/configure-view-system-alarms-mas.html)

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/13-1/networks/network-functions/how-to-generate-reports-for-load-balancing-entities.html)

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

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/13-1/networks/network-functions/export-or-schedule-export-of-reports.html)

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

概要

NetScaler Application Delivery Management (ADM) は、管理者に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。ADM 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。

ADM は、Citrix Hypervisor™、VMware ESXi、および Linux KVM で動作する仮想アプライアンスです。ADM 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次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
- ウェブページのパフォーマンスデータ
- サイトのADC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。

ADM 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® Application Delivery Management (ADM) 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

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 ダッシュボードは、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。たとえば、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が表示されます。App Security ダッシュボードには、検出された ADC インスタンスに対す

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

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されます。

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

ADCインスタンスのIPアドレスがADMに追加されると、ADMによってNITROコールが送信され、その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が追加されます。

イベントは、管理対象のADC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 ADM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し、未使用または間もなく期限切れになる証明書を綿密に監視できます。ADMの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ADM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

NetScaler ADMを使用すると、複数のインスタンスで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の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ADM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。

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

- 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

ADM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。

分析

ウェブインサイト

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、IT管理者がNetScalerによって提供されるすべてのWebアプリケーションを、統合されたリアルタイムのアプリケーション監視によって監視できるようにします。Web Insightは、ユーザーおよびサーバーの応答時間などの重要な情報を提供し、IT組織がアプリケーションのパフォーマンスを監視および改善できるようにします。

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。HDX Insightにより、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。

ゲートウェイインサイト

アクセスモードに関係なく、ユーザーがログオン時に遭遇する失敗の可視性を提供します。特定の時点にログオンしているユーザーのリストを、アクティブユーザー数、アクティブセッション数、および特定の時点ですべてのユーザーが使用しているバイト数とライセンス数とともに表示できます。

セキュリティインサイト

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つシングルペインソリューションを提供します。

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、セキュアなWebトランザクションの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。

TCPインサイト

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

TCP Insightは、データ伝送におけるネットワーク輻輳を回避するためにADCインスタンスで使用される最適化技術と輻輳制御戦略（またはアルゴリズム）のメトリックを監視するための、簡単でスケーラブルなソリューションを提供します。

ビデオインサイト

Video Insight機能は、顧客体験と運用効率を向上させるためにNetScalerインスタンスによって使用されるビデオ最適化技術のメトリックを監視するための、簡単でスケーラブルなソリューションを提供します。

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 ADM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/13-1/orchestration.html)

NetScaler ADMは、異なるベンダーのSDNコントローラーと統合することで、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。ADM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® Application Delivery Management (ADM) 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、証明書詳細、インスタンスに構成されたエンティティなどのインスタンス詳細のインベントリがサーバーに保存されます。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。

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

次の図は、ADM 内のさまざまなサブシステムと、ADM 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。

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

ADM のサービスサブシステムは Web サーバーとして機能し、GUI または API からポート 80 および 443 を使用して ADM 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、ADM がサポートす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、ADM と管理対象インスタンス間で転送されます。この情報はその後処理され、内部データベース (データストア) に保存されます。

NetScaler® ADM がインスタンスを検出する方法

インスタンスとは、NetScaler Application Delivery Management (ADM) から検出、管理、監視したい NetScaler ADC 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 ADM サーバーに追加する必要があります。ADM には、次の NetScaler ADC 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

インスタンスは、NetScaler ADM 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.

注

NetScaler ADM は、通信に ADC インスタンスの NetScaler IP (NSIP) アドレスを使用します。ADM 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 ADC インスタンスも検出できます。ADC インスタンスと ADM 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 ADC HA ペアを追加する場合は、ADC 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。
ADM 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。

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

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

1. NetScaler ADM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。ADC NITROコールを使用して、ADMは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ADCインスタンスであるかどうか、およびADCプラットフォームのタイプ（例：NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX、またはNetScaler Gateway）を判断します。インスタンスの検出に成功すると、ADMの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、インスタンスにライセンスが構成されていなくても、すべてのインスタンスをADMに追加できます。

2. ADMは、インスタンス上のトラップ宛先リストに自身のIPアドレスを追加します。これにより、ADMはADC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。

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

3. ADM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。

   ADM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 Application Delivery Management (ADM) 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。組織向けに、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 ADMを介してインスタンスを監視するには、NetScaler ADMは、CPU使用率、メモリ使用量、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ADC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。ADM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 ADM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。

NetScaler® ADM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 ADMは、デフォルトで定期的に自動的にポーリングします。NetScaler ADM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。

© 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
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ADC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。**Infrastructure > Instances > NetScaler** に移動します。インスタンスを選択し、**Select Action** リストから **Backup/Restore** をクリックします。
構成監査ポーリング	10時間ごと（デフォルト）	ADC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。**Infrastructure > Configuration Audit** に移動します。Configuration Audit ページで、**Settings** をクリックし、

© 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 ADMに即座に追加できます。これを行うには、**Infrastructure > Configuration Audit** 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。
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いるSSL証明書。	NITRO呼び出しとSCP	はい。**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ダッシュボードページで、**設定**をクリックしてポーリング間隔を設定します。

© 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
				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 ADM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 > SSLダッシュボード**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。
エンティティポーリング	60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。エンティティとは、ADC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。エンティティポーリングを有効にするには、「ADM機能の	NITRO呼び出し。	はい、ただし10分未満に設定することはできません。設定するには、**インフラストラクチャ > ネットワーク機能**に移動します。ネットワーク機能ページで、**設定**をクリックしてポーリング間隔を設定します。

© 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
		有効化または無効化」を参照してください。		
				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 ADM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 > ネットワーク機能**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。

注

ポーリングに加えて、管理対象ADC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 ADMによって受信されます。たとえば、システム障害や構成変更が発生し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に、SSLファイル、CA証明書ファイル、ADCテンプレート、データベース情報などがNetScaler ADMにダウンロードされます。構成監査中に、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。

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

インスタンスをポーリングするさまざまな方法

NetScaler ADM 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

インスタンスのグローバルポーリング

NetScaler ADM 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 ADM 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でレポートが生成されるまでに時間がかかり、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 ADM 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場合、またはエンティティが更新された場合、NetScaler ADM は次回のポーリングが行われるまで、新しいインスタンスまたは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することはできますが、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。NetScaler ADM では、ネットワーク全体をポーリングする代わりに、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 ADM は、管理対象インスタンスを自動的にポーリングして、1 日の特定の時間に情報を収集します。選択したポーリングにより、NetScaler ADM がこれらの選択し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 ADM で特定のインスタンスをポーリングするには:

1. NetScaler ADM で、**Infrastructure > Network Functions** に移動します。
2. **Network Functions** ページで、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** 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。

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

a. **All Instances** タブで、**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. **インスタンスの選択**タブ - リストからインスタンスを選択します

4. **ポーリングの開始**をクリックします。

ポーリングするインスタンスを選択(/en-us/netscaler-application-delivery-management-software/media/nmas-instance-polling-2-citrix.png)

NetScaler ADM 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 ADM 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 ADM はそのエンティティのみをポーリングし、NetScaler ADM 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場合、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 ADM で特定のエンティティをポーリングするには:

例として、このタスクは負荷分散仮想サーバーをポーリングするのに役立ちます。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。

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

1. NetScaler ADM で、**インフラストラクチャ > ネットワーク機能 > 負荷分散 > 仮想サーバー**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、**今すぐポーリング**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。

   今すぐポーリング(/en-us/netscaler-application-delivery-management-software/media/maservice-manual-polling-entities-citrix.png)

© 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、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。こちらに記載されている NetScaler テレメトリプログラムに準拠し続けるために、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。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 インスタンスを NetScaler Console に追加して、NetScaler の運用全体を改善および簡素化し、NetScaler の機能使用状況データを送信することで製品およびサービスの強化をサポート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、**14.1-25.53 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) を使用してアウトバウンド接続を作成し、テレメトリデータを自動的にアップロードします。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、「(/ja-jp/netscaler-application-delivery-management-software/13-1/telemetry-modes.html#automated-telemetry-collection-mode)」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 サービスへの最初のアップロードを完了する必要があります。準拠を維持するには、その後のアップロードを 90 日ごとに行う必要があります。詳細については、「(/ja-jp/netscaler-application-delivery-management-software/13-1/telemetry-modes.html#manual-telemetry-collection-mode)」を参照してください。

推奨されるのは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ですが、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し続けるためにはデータの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。

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

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、以下の構成が管理対象の NetScaler インスタンスにプッシュされました。

- 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:

最適なテレメトリ収集のため、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。

- **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®とテレメトリメトリクスプロファイルの設定に関する詳細を提供します。

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設定	テレメトリモード	必要なアクション
13.1-57.x	いいえ	自動および手動	設定はNetScalerインスタンスにプッシュされず、テレメトリメトリクスプロファイル設定が存在する場合は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

© 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設定	テレメトリモード	必要なアクション
			を使用していない場合は、`disable ns feature AppFlow` を使用してAppFlow設定を削除できます。
13.1-55.x	いいえ	自動および手動	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せん。これらの設定が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クスプロファイル設定を削除し、`disable ns feature AppFlow` を使用してAppFlow設定を削除します。
13.1-53.22	はい。AppFlowとテレメトリメトリクスプロファイル設定の両方	自動 (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

© 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設定	テレメトリモード	必要なアクション
			を実行してテレメトリメトリクスプロファイル設定を削除し、`disable ns feature AppFlow` を使用してAppFlow設定を削除します。
		自動 (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) にするか、最新の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、このコマンドが不足している場合は追加します。

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

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

- 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ています。

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	ライセンスの権利、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（14.1-25.53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 14.1-25.53以降 / 13.1–53.22以降にアップグレードした後、いずれかのテレメトリモード（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:

- **2024年9月18日**までに、最新ビルド（14.1–25.53以降 / 13.1–53.22以降）に移行する必要があります。
- 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、ただし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

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

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、これらの要件に準拠しない場合、Citrixが法律上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。

© 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、ビルド14.1-25.53以降/13.1-53.22以降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を使用すると、NetScaler Consoleオンプレミスでオプションのテレメトリパラメータを収集する**セキュリティアドバイザリ**機能を使用できます。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:

- 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、この構成が不足している場合はNetScalerインスタンスにプッシュし続けます。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、このコマンドが不足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。
- 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、論理的な資産照合の目的でのみ使用されます。

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ています。

カテゴリ	説明	用途?	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

オプションのパラメータを無効にするには：

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。

NetScaler Consoleが13.1-53.22より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、

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

ステータス、その他のメトリックに関する重要な統計情報を送信できます。Citrixは、NetScaler Consoleの使用状況を把握するために統計情報を収集します。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.

ライセンス

NetScaler Application Delivery Management (ADM) 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® ADM 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。ADM 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 edition – Express edition 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 edition ライセンスが適用されます。

Advanced edition - これにより、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。

ビルド 13.1-12.x 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 日間の猶予期間内に、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、ADM 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。
- アップグレード後、ADM の動作には以下の変更点があります。
    - ADM は 30 日間の猶予期間を適用します。

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

- 30 日間の猶予期間中、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、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 日間の猶予期間中は 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 日間の猶予期間内であれば、管理者として Advanced ADM 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。

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) Advanced with App Firewallライセンスが必要です。
	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。	NA
	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と、追加の2つの仮想サーバーの権利があります。	該当なし
	構成 > StyleBooks	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
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関連の情報には、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権利があります。	Premium (または) Advanced と App Firewall ライセンス
	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、追加の仮想サーバー2台の権利があります。	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、追加の仮想サーバー2台の権利があります。	Advanced (レポート作成 < 1時間) Premium (レポート作成 = 無制限)
	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	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
			と、追加の仮想サーバー2台の権利があります。	(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	NA
	インスタンス	無制限	無制限	NA
	SSLダッシュボード	無制限	無制限	NA
	イベント	無制限	無制限	N/A
	ネットワーク機能	無制限	無制限	N/A
	ネットワークレポート	無制限	無制限	N/A
	プールライセンス	無制限	無制限	N/A
	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
設定	RBAC & 外部認証 (インスタンスレベル)	無制限	無制限	該当なし
	RBAC & 外部認証	無制限	無制限	該当なし

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

*NetScaler ADM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できます。有効なライセンスを取得し、NetScaler ADM GUIを介してNetScaler ADMサーバーにライセンスを追加できます。

高可用性

NetScaler ADM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ADM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。また、別のADMサーバーへのライセンスの割り当ては制限されています。

ADM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、ADM高可用性展開では、NetScaler ADM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ます。

注

- NetScaler ADM 12.1.49.x以前のリリース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日間の猶予期間が与えられます。猶予期間が過ぎると、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。
- 12.1.50.x以降のリリースでは、NetScaler ADM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、12.1.50.x以降のリリースからセカンダリノードに自動的に同期されます。

ADM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?

フェー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。

- **リアルホストID** - このIDは、ADMサーバーのMACアドレスから生成されます。各ADMスタンドアロン展開には、一意のホストIDがあります。

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

- **仮想ホストID** - このIDは、HA展開中に自動生成されます。ADMプライマリサーバーのリアルホスト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は暗号化された形式でADMデータベースに保存され、このID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。

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. ADMは、ライセンス容量の二重化を避けるため、ライセンスサーバーがNode-1でのみ実行されていることを確認します。
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ADCインスタンスにロックされます。NetScaler ADM 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仮想アプライアンスの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、そのインスタンスに将来のすべてのライセンスが適用されます。ライセンスは、ライセンスをインストールしたサーバーからのみ削除できます。

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 ADMのライセンスをアップグレードして、NetScalerアプライアンス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。

アプライアンス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 ADM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する**。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

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

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する**。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がメールで送信されます。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した場合、NetScaler ADM 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 ADM 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 ADM を介して管理および監視する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。

注意点

- デフォルトでは、NetScaler ADM 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をランダムに自動的にライセンス供与します。
- NetScaler ADM 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 ADM はデフォルトで、すべての仮想サーバーにライセンスを供与します。

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

仮想サーバーを手動で選択するか、ライセンス供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供与を無効にしてから、管理する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供与を無効にする

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の自動選択**」を無効にします。

   自動ライセンス供与を無効にする(/en-us/netscaler-application-delivery-management-software/media/auto-select-vservers-citrix.png)

ライセンス供与するサードパーティ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、管理対象の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。

   サードパーティ仮想サーバーを選択(/en-us/netscaler-application-delivery-management-software/media/auto-select-vservers-2.png)

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。

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。

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

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インスタンス上の仮想サーバーの制限を個別に設定します。ADMは、指定された制限までCPXインスタンス上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、サイドカーデプロイメントタイプを除くCPXインスタンスに適用されます。

  サイドカーデプロイメントタイプの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ADCインスタンス (MPX/VPX/BLX) 上の仮想サーバーの制限を設定します。ADMは、指定された制限までADCインスタンス上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ADCインスタンスを選択します。したがって、ADM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ポリシーを編集 (/en-us/netscaler-application-delivery-management-software/media/configure-license-policy-citrix.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. **>** に移動します。
2. の セクションで、仮想サーバーの種類をクリックします。

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

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 ADM 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 ADM は、 の下にオプションを提供します。 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 ADM 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、現在、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サポートされている唯一の分析です。

仮想サーバーライセンスの有効期限チェック

NetScaler ADM で仮想サーバーライセンスの有効期限の状態を表示し、アラートを設定できるようになりました。

ライセンスのステータスを表示するには:

1. **> >** に移動します。
2. 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。
   - **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:** 有効期限が切れるまでの残り日数。

ライセンスの通知設定を構成するには:

1. **インフラストラクチャ > プールされたライセンス > 設定** に移動します。
2. **通知設定**セクションで、鉛筆アイコンをクリックしてパラメータを編集します。

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

- **メールプロファイル:** ライセンスがしきい値に達したとき、または有効期限が切れるときに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。
- **SMS (テキストメッセージ):** ライセンスがしきい値に達したとき、または有効期限が切れるときに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** - 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。
- **通知:** プールされたライセンスの何パーセントで管理者にメールまたはSMSで通知するかを設定します。
- **ライセンス有効期限しきい値:** アラートしきい値によって決定されたライセンスの数が期限切れになるまでの日数。
- **ライセンスの有効期限:** 有効期限が切れるまでの残り日数。

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

システム要件

NetScaler® Application Delivery Management (ADM) 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 ADM の要件

コンポーネント	要件
RAM	32 GB
仮想CPU	8 CPU
	注: Citrix では、NetScaler ADM 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 ADM のサイジング見積もりによって異なります。
	NetScaler ADM 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 台のみです。
	Citrix では、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お勧めします。
	詳細については、「NetScaler ADM 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 ADM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 ギガビーピーエス

注

AMDプロセッサは以下でサポートされています。

- **NetScaler ADM 13.1 build 4.43以降**。
- **NetScaler Agent 13.1 build 17.42以降**。

NetScaler ADM機能に必要なNetScalerの最小バージョン

重要

NetScaler ADM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 ADM 12.1 Build 50.39をインストールしている場合は、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 ADM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で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 ADM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
ジョブを使用した監視/レポートおよび構成	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

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

NetScaler ADMアナリティクスの要件

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

NETSCALER ADM機能	CITRIX VIRTUAL APPS AND DESKTOPSのバージョン
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.

注記

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）は、NetScalerインスタンスで利用可能である必要があります。NetScaler ADM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 ADM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

HDX InsightのためにNetScaler ADMによって収集されるデータは、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依存します。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アプライアンスに対してのみ表示されます。

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 ADM 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
シトリックス ハイパーバイザー	7.1および7.4
ヴイエムウェア ESX	6.0、6.5、6.7、および7.0
マイクロソフト Hyper-V	2012 R2および2016
汎用KVM	RHEL 7.4、RHEL 8.0、Ubuntu 16.04、およびUbuntu 18.04

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 ADM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
ウィンドウズ	4.0 スタンダードエディション
リナックス	13.0.265571以降
Mac	11.8、ビルド238301以降
HTML5	1.5
Chromeアプリ	1.5

サポートされているブラウザ

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

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

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

WEBブラウザ	バージョン
サファリ	10以降
モジラ ファイアフォックス	52以降

サポートされているポート

NetScaler ADMは、NetScalerとの通信にNetScaler IP (NSIPとして知られる) アドレスを使用します。ADCインスタンスとADM間の仲介役としてADM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。

注

NetScalerを高可用性モードで構成している場合、NetScaler ADMはNSIPを使用してNetScalerと通信し、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:

エージェントレス展開のネットワークポート(/en-us/netscaler-application-delivery-management-software/media/port-diagram-without-agent.png)

ADMエージェントを含む展開のネットワークポート図:

エージェント展開のネットワークポート(/en-us/netscaler-application-delivery-management-software/media/port-diagram-with-agent-on-prem.png)

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。

- ADMサーバー(#ports-for-the-adm-server)
- ADMエージェント(#ports-for-the-adm-agent)
- ADCインスタンス(#ports-for-adc-instances)
- 外部サーバー(#ports-for-external-servers)

ADMサーバーのポート

次の表は、ADMサーバーで開く必要があるポートについて説明しています。

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

ポート	タイプ	詳細	通信の方向
80/443/5454/22	TCP	高可用性モードのNetScaler ADM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です。**注:** このポートはNetScalerテレメトリにも使用されます。	NetScaler ADMプライマリノードからNetScaler ADMセカンダリノード
443/8443/7443	TCP	NetScalerエージェントとNetScaler ADM間の通信用のポート。	NetScalerエージェントがNetScaler ADMとの通信を開始します。その後、NetScaler ADMとエージェントが相互にやり取りします。
27000および7279	TCP	NetScaler ADMライセンスサーバーとADCインスタンス間の通信用のライセンスポート。これらのポートは、ADCプールライセンスにも使用されます。	NetScaler から NetScaler ADM
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 ADMプライマリノードからセカンダリノードへ。NetScaler ADMセカンダリノードからプライマリノードへ。
5140	UDP	NetScaler Gatewayのテレメトリデータを受信するためのポート。	NetScalerからNetScaler Consoleへの通信

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

ADMおよびADCインスタンスが通信にエージェントを使用していない場合は、ADMサーバーで次のポートを開放してください。

ポート	タイプ	詳細	通信の方向
80/443	TCP	NetScaler ADM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 ADMへのAppFlow通信用。	NetScalerからNetScalerエージェントへ
162	UDP	NetScalerインスタンスからNetScaler ADMへのSNMPイベントを受信するため。	NetScalerからNetScalerエージェントへ
514	UDP	NetScalerインスタンスからNetScaler ADMへの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 ADM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の場合）。	ネットスケーラー から ネットスケーラー ADM へ
5563	TCP	NetScalerインスタンスからNetScaler ADMへ、ADCメトリック（カウンター）、システムイベント、監査ログ	ネットスケーラー から ネットスケーラー ADM へ

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

ポート	タイプ	詳細	通信の方向
		メッセージを受信するため	

ADMエージェントのポート

次の表は、ADM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	通信の方向
80/443	TCP	NetScaler ADM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 ADMへのAppFlow通信用。	NetScalerからNetScalerエージェントへ
162	UDP	NetScalerインスタンスからNetScaler ADMへのSNMPイベントを受信するため。	NetScalerからNetScalerエージェントへ
514	UDP	NetScalerインスタンスからNetScaler ADMへの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 ADM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）。	NetScaler - NetScaler ADM

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

ADCインスタンスのポート

次の表は、NetScalerインスタンス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 ADMからNetScalerインスタンスへのNITRO通信用。高可用性モードのNetScaler ADMサーバー間のNITRO通信用。	NetScaler ADMからNetScaler、およびNetScalerからNetScaler ADMへ
22	TCP	NetScaler ADM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 ADMサーバー間の同期用。また、このポートはADMエージェントとNetScaler間のSSH通信に必要です。	NetScaler ADMからNetScalerへ。または、NetScalerエージェントからNetScalerへ。
予約ポートなし	ICMP	NetScaler ADM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 ADMサーバー間のネットワーク到達性を検出するため。	NetScaler ADMからNetScalerへ
161	UDP	ADCインスタンスからイベントをポーリングするため。	NetScaler ADMからNetScalerへ

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

ADC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く必要がある必須ポートについて説明しています。

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

注:

ADMの高可用性展開では、ADM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。

外部サーバー用のポート

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

ポート	タイプ	詳細	通信の方向
25	TCP	NetScaler ADMからユーザーにSMTP通知を送信するため。	NetScaler ADM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 ADMとLDAP外部認証サーバー間の通信用。	NetScaler ADMからLDAP外部認証サーバーへ
123	UDP	複数の時刻ソースと同期するためのデフォルトNTPサーバーポート。	NetScaler ADMからNTPサーバーへ

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

ポート	タイプ	詳細	通信の方向
1812	RADIUS	認証プロトコルのデフォルトポート。NetScaler ADMとRADIUS外部認証サーバー間の通信用。	NetScaler ADMからRADIUS外部認証サーバーへ
49	TACACS	認証プロトコルのデフォルトポート。NetScaler ADMとTACACS外部認証サーバー間の通信用。	NetScaler ADMからTACACS外部認証サーバーへ

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を構成するには、 > に移動し、 の下の を選択し、 を有効にして、IPv6構成の詳細を入力し、 をクリックします。

次の表に、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一覧を示します。

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
設定ジョブ	
設定監査	
ネットワーク機能	
ネットワークレポート	

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

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
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 Application Delivery Management (ADM) を初めて展開およびセットアップする方法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 ADM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 ADMの既存ユーザーである場合は、サーバーをNetScaler ADMの最新リリースに(/ja-jp/netscaler-application-delivery-management-software/13-1/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® ADM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管理および監視できます。ただし、ライセンスを適用しない場合、管理できる検出済みアプリは30個まで、分析情報を表示できる仮想サーバーは2台までです。30個を超えるアプリを管理したり、2台を超える仮想サーバーの分析情報を表示したりするには、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正しい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。
- **ブラウザ要件**。NetScaler ADM 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 ADM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 ADM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 ADM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 ADMをインストールする必要があります。NetScaler ADM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 ADM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 ADM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 ADM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 ADM
  - Microsoft Hyper-Vを使用したNetScaler ADM
  - VMware ESXi を使用した NetScaler ADM(/ja-jp/netscaler-application-delivery-management-software/13-1/deploy/install-mas-on-esxi.html)
  - Linux KVM サーバーを使用した NetScaler ADM(/ja-jp/netscaler-application-delivery-management-software/13-1/deploy/install-mas-on-kvm.html)
- **高可用性展開。** 2台のNetScaler ADM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 ADMノードをアクティブ/パッシブモードで、同じサブネットに、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 ADMプライマリノードでフローティングIPアドレスを構成できるため、個別のNetScalerロードバランサーは不要になります。詳細については、「」を参照してください。

  ```
  ](/ja-jp/netscaler-application-delivery-management-software/13-1/deploy/high-availability-deployment.html)
  ```

ステップ3 - NetScaler ADMにインスタンスを追加する

インスタンスとは、NetScaler ADMから検出、管理、監視したいNetScaler ADC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 ADMサーバーにインスタンスを追加する必要があります。NetScaler ADMには、次のインスタンスを追加できます。

- NetScaler

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

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

NetScaler ADM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

ステップ4 - 仮想サーバーで分析を有効にする

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Analytics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 ADMでNTPサーバーを構成する

NetScaler ADMのクロックをNTPサーバーと同期させるには、NetScaler ADM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 ADM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。

詳細はこちら

ステップ6 - NetScaler ADM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 ADMを使用してインスタンスとアプリケーションの管理および監視を開始する前に、NetScaler ADM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取りたい場合があります。

© 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 ADM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。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。
- **システムプルーニング設定を構成する**。NetScaler ADM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 ADM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時) にプルーニングされます。
- **システムバックアップ設定を構成する**。NetScaler ADMは、毎日00:30時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プルーニング設定を構成する**。NetScaler ADM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 ADM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時) にプルーニングされます。
- **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 ADM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 ADM 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。

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

NetScaler インスタンスとアプリケーションの管理。 すべての NetScaler ADM 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.

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ADMの場合、データベースは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。参照:
  - シトリックス ハイパーバイザー上のNetScaler Console
  - Microsoft ハイパーV上のNetScaler Console
  - VMware ESXi上で動作するNetScaler Console
  - Linux KVMサーバー上で動作する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、中断のない操作を提供します。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ADMには適用されません。

- **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

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

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とDirectorの統合**: 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とDirectorの統合

NetScaler® ADMインストールの前提条件

Microsoft HyperV向けにNetScaler Application Delivery Management (ADM) をダウンロードしてインストールできます。 VMware ESXi、Linux KVM、およびCitrix Hypervisor™プラットフォームに仮想アプライアンスとして。NetScaler ADMをインストールする前に、 NetScaler ADMのソフトウェア要件、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での制限事項を理解しておく必要があります。

NetScaler ADM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。

- シトリックス ハイパーバイザーを使用したネットスケーラー ADM
- マイクロソフト ハイパーVを使用したネットスケーラー ADM
- VMware ESXi環境におけるNetScaler ADM
- Linux KVMサーバーでのNetScaler ADM(/ja-jp/netscaler-application-delivery-management-software/13-1/deploy/install-mas-on-kvm.html)

NetScaler ADMの一般的な要件

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 ADM 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 ADM のサイジング見積もりによって異なります。

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

コンポーネント	要件
	NetScaler ADM 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ます。追加できるディスクは 1 台のみです。
	詳細については、「NetScaler ADM 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ギガビット/秒

注:

Citrix は、NetScaler ADM 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 内のストレージデバイスにホストされている場合、NetScaler ADM 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 ADM 展開はサポートされていません。

シトリックス ハイパーバイザー™ 上の NetScaler ADM

Citrix Hypervisor (旧称 XenServer) にNetScaler® ADMをインストールするには、まずNetScaler ADM .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 ADM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 ADMはXenMotionをサポートしていません。

前提条件

NetScaler ADM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。

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

- 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 ADM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 ADM .XVAイメージファイルをダウンロード済みであること。

XenCenterのシステム要件

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。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	Windows 7、Windows サーバー 2003、または Windows 10
.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、**コンソール**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 の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。

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

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 ADM 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 ADM 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 ADM サーバーを再起動するには、**Yes** と入力します。

> **注**
>
> NetScaler ADM 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 ADMサーバーのIPアドレスを入力することで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 ADM構成ユーティリティが表示されます。

Microsoft Hyper-V 環境での NetScaler® ADM

Microsoft Hyper-V に NetScaler ADM をインストールするには、まず NetScaler ADM イメージファイルをローカルコンピュータ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あることを確認し、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 ADM 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。
- Microsoft Hyper-V マネージャーが、最小システム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。
- NetScaler ADM 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.

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	Windows サーバー 2012 R2
.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

インストールできるNetScaler ADM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 ADM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. **操作**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. 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 ADM 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. セクションで、適切な仮想マシン名を選択します。
   c. 「**インポートタイプの選択**」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。

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

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。

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 ADM Hyper-Vイメージが右ペインに表示されます。

4. NetScaler ADM 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 ADM 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. 最初の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したい場合は、`networkconfig` と入力し、構成を更新して保存します。

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
```

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

13. 展開タイプとして **NetScaler ADM Server** を選択します。何も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。

14. NetScaler ADM 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 ADM サーバーを再起動するには、**Yes** と入力します。

> **注**
>
> NetScaler ADM 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

サーバーのインストール後、ブラウザのアドレスバーにNetScaler ADM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 ADM構成ユーティリティが表示されます。

VMware ESXi 上の NetScaler® ADM

このドキュメントでは、VMware vSphere Client を使用して、VMware ESXi に NetScaler ADM 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、以下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 (6.0、6.5、6.7、および 7.0) 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。
- NetScaler ADM セットアップファイルをダウンロードします。

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

注

- VMotion は、**NetScaler ADM 13.0 Build 47.22 以降**でのみサポートされています。vSphere High Availability および vSphere DRS のセットアップを含め、ESXi ハイパーバイザーに展開された ADM 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 ADM 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 ADM をインストールするには

VMware ESXi に ADM 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。

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 ADM 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 Client を起動します。
2. 「**IPアドレス / 名前**」テキストボックスに、接続したい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で、「**ファイルまたはURLから展開**」から.ovfファイルを選択し、「**次へ**」をクリックします。

   注

   次のテキストを含む警告メッセージが表示された場合：「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確認してください。」「**はい**」をクリックします。

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

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 ADM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. 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、ディスクフォーマットを指定します。

   注

   Citrixは**シックプロビジョニング形式**を選択することを推奨します。

9. インストールプロセスを開始するには、「**完了**」をクリックします。

10. これでNetScaler ADM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。

12. **インベントリ**メニューで、**仮想マシン**をクリックし、次に**設定の編集**をクリックします。
13. **仮想マシンのプロパティ**ダイアログボックスで、**ハードウェア**タブの**メモリ**をクリックし、右側のペインで**メモリサイズ**を32 GBに指定します。
14. **CPU**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. 要件に応じて追加ディスクを追加します。

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。**インベントリ**メニューから、**仮想マシン**をクリックし、**電源**をクリックし、次に**電源オン**をクリックします。
17. **コンソール**タブをクリックして、NetScaler ADMの初期ネットワーク構成オプションを表示します。

18. 必要なIPアドレスを指定した後、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。

© 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したい場合は、`networkconfig`と入力し、構成を更新して保存します。

20. シェルプロンプトでコマンドを入力して、デプロイスクリプトを実行します。

```
deployment_type.py
```

21. 展開タイプとして**NetScaler ADM Server**を選択します。オプションを選択しない場合、デフォルトでサーバーとして展開されます。

22. NetScaler ADM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。
23. NetScaler ADMサーバーを再起動するには、「**Yes**」と入力します。

注

NetScaler ADMをインストールした後、初期構成設定を後で更新できます。

検証

サーバーがインストールされたら、ブラウザにNetScaler ADM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 ADM構成ユーティリティが表示されます。

注

VMware ESXiでの一般的なADMの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エージェント展開の自動化

NetScaler ADMを使用すると、VMware ESXi上でNetScalerエージェントの展開を自動化できます。

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

管理者として、以下の操作を自動化できます。

- NetScalerエージェントを構成する
- 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する。

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ファイルに以下のパラメーターの値を追加します。

1. IPアドレス
2. ネットマスク
3. ゲートウェイ
4. ネームサーバー
5. ホスト名

注

.ovfファイルはエージェントイメージファイル内にあります。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

登録してデフォルトパスワードを変更する前に、NetScaler エージェントの構成で指定された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 ファイルに次のパラメータの値を追加します。

1. ADM サーバー IP
2. ADM ユーザー名
3. ADM パスワード
4. エージェントの新しいパスワード

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

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、以下を確認してください。

- 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 vSphere 8.x をインストールします。
- NetScaler® ADM 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 ADM 仮想アプライアンスをインストールする
3. 確認する

.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。以下のファイルが利用可能です。
   - .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、 `</VirtualHardwareSection>` タグの後に以下の `<ProductSection>..</ProductSection>` サンプルコードを追加します

```
<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">
```

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

```
    <Label>IPAddress</Label>

    </Property>



    <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">
```

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

```
    <Label>Hostname</Label>

    </Property>



    <Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

    ovf:key="eth0.ServerIP">

    <Label>ADM Server IP</Label>

    </Property>



    <Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

    ovf:key="eth0.ServerUname">

    <Label>ADM Username</Label>

    </Property>



    <Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

    ovf:type="string" ovf:key="eth0.ServerPassword">

    <Label>ADM Password</Label>

    </Property>



    <Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

    ovf:type="string" ovf:key="eth0.NewPassword">
```

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

```
    <Label>Agent New Password</Label>

    </Property>



</ProductSection>
```

1. 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。
     - IPアドレス
     - ネットマスク
     - ゲートウェイ
     - ネームサーバー
     - ホスト名
   - 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には、以下のパラメーターに値を追加します。
     - ADMサーバーIP
     - ADMユーザー名
     - ADMパスワード
     - エージェントの新しいパスワード

   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および変更しない場合、VMの展開後にこれらのアクションを手動で実行する必要があります。

2. 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.

VMware ESXiにNetScaler ADM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。**Login**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**Deploy OVF Template**を選択します。

3. **Deploy OVF Template**ページで、次の操作を行います。

   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、仮想マシンをデプロイする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**: デプロイ後にテンプレートを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で.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. **完了準備完了**: 設定を保存してデプロイ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テンプレートのデプロイ**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オンにしないでください。

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 ADM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。

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、次の手順を実行します。

1. NetScalerエージェントが展開されたら、ブラウザでNetScaler ADMサーバーのIP アドレスを入力して、NetScaler ADM 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® ADM

KubernetesクラスターにNetScaler ADM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

ADM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サブordinate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、ADM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ベースのサブordinateにNFSクライアントをインストールするには、以下のコマンドを入力します。

`apt-get update` `apt install nfs-common`

- ADM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 vCPU、およびNFS上に120 GBのスペースが必要です。

NFS共有

ADM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、ADM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う1つ

© 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つのフォルダは異なっていても同じでも構いません。両方のフォルダに777の権限が必要です。最初のフォルダには最低10 GBのスペースが必要です。2番目のフォルダのサイズは、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。ADCは、必要なアプリケーションサービスをKubernetesの外部で利用できるようにします。 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る必要があり、ワーカーノードはADC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。

- ADCでSNIPを構成します。ADC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できるようにするために、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クラスターにADMをインストールする

KubernetesクラスターにADM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 ADM 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 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。ADM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、サービスを外部に公開します。
   - `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と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`: ADM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、ADM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`: 少なくとも100 GB。

   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、次のコマンドを実行してADMアプリケーションをインストールします。 `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、必要なポッドもクラスターに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ADM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、ADM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ADM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

デプロイ中、ADM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ADM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® ADM

NetScaler Application Delivery Management (ADM) 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 ADM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。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 ADM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 ADM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 ADM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。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

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

コンポーネント	要件
	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 ADM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の要件に必要な領域を計算します。単一のNetScaler ADM VMには120 GBのディスク領域が必要です。

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前提として、OpenStackプラットフォームにNetScaler ADM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

Citrixは、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ています。

ネットワーク要件

NetScaler ADMは、virtIO準仮想化ネットワークインターフェイスを1つのみサポートします。NetScaler ADM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 ADMセットアップファイルのダウンロード

`www.citrix.com` からNetScaler ADMセットアップファイルをダウンロードするには：

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。

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

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、再度**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. 「**Jump to Download**」リストで、「**NetScaler MAS image for KVM, 13.0 Build xx.xx**」を選択します。
8. 「**Download File**」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にNetScaler Application Delivery Managementをインストールする

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 ADM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

MAS-KVM.qcow2
```

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

```
checksum.txt
```

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. MAS1-KVM.xmlを編集して、次のネットワーク属性を設定します。

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` - ディスクイメージの絶対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`

```
virsh define MAS-KVM.xml

Domain MAS defined from MAS-KVM.xml
```

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

vii. 次のコマンドを入力して、NetScaler ADM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 ADM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、FreeBSDゲストが複数のCPUを持つ場合、適切に再起動できないことがあります。NetScaler ADM仮想アプライアンスが再起動されると、NetScaler ADM CLIおよび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 ADM仮想アプライアンスの再起動時にNetScaler ADM CLIおよび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`
2. 次のコマンドを使用して、**APICv**を無効にし、kvm_intelモジュールを再ロードします: `modprobe kvm\_intel enable\_apicv=N`
3. KVMホスト上で仮想マシンを起動します。

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

NetScaler ADM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分間待機し、NetScaler ADM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。次に、ネットワークで機能するようにMASを構成します。パスワードはNetScaler ADMユーザーインターフェイスから変更できます。NetScaler ADM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、**Edit**をクリックして、パスワード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 ADM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。
4. NetScaler ADM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 ADMの次のパラメータを設定するためのNetScaler ADM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ます。

   a. **2** を入力して、NetScaler ADM IPv4アドレス（NetScaler ADMにアクセスする管理IPアドレス）を更新します。

   b. **3** を入力して、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）を更新します。

   c. **4** を入力して、ゲートウェイIPv4アドレス（NetScaler ADM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）を更新します。

   d. **7** を入力して保存して終了します。これにより、設定の変更が保存され、システムが終了します。

   ネットワーク構成(/en-us/netscaler-application-delivery-management-software/media/admha-initialconfig.png)

5. シェルプロンプトでコマンドを入力してデプロイスクリプトを実行します: `deployment_type.py`

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

6. 表示されるデプロイ画面で、デプロイタイプとして**NetScaler ADMサーバー**を選択します。

   デプロイサーバーとしてNetScaler ADMを選択(/en-us/netscaler-application-delivery-management-software/media/ha-deploymentconfig.png)

7. NetScaler ADMをスタンドアロンデプロイとしてデプロイするには、**Yes**と入力します。
8. NetScaler ADMサーバーを再起動するには、**Yes**と入力します。
9. NetScaler ADM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 ADMにログオンします。

   後で、ブラウザのアドレスバーにNetScaler ADMサーバーのIPアドレスを入力してNetScaler ADM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。

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。同じ構成を持つ2つのNetScaler® ADMノードをアクティブ/パッシブモードで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。

展開シナリオ

シナリオ(/en-us/netscaler-application-delivery-management-software/media/deploymentscenario.png)

注

単一のNetScaler ADM 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 ADM 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 ADMをロードバランシングするように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 ADMにアクセスするためにフローティングIPアドレスを構成します。
NetScaler ADMにおける高可用性展開の利点は次のとおりです。

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

- 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 ADM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 ADM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、インスタンスを再設定する必要がなくなります。
- 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。
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	高可用性セットアップで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。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。クライアントが高可用性ノードと単一のIPアドレスを使用して通信で

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

用語	説明
	きるため、高可用性セットアップで役立ちます。

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 ADM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.png)

高可用性展開では、1つのNetScaler ADMノードがプライマリノード（MAS 1）として構成され、もう1つがセカンダリノード（MAS 2）として構成されます。プライマリノードが何らかの理由でダウンした場合、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 ADMユーザーインターフェイスへのアクセスはプライマリノードで利用可能です。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 ADM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。

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

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。ノードの状態、健全性、プロセスなどに関する情報を交換するために、NetScaler ADMのすべてのサブシステムとデータベースを監視します。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

浮動IPアドレスは、高可用性セットアップの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 ADM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。浮動IPアドレスはプライマリノードで構成されているため、フェイルオーバーの場合でもインスタンスの再構成は不要です。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。

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 ADMノードがアクティブ/パッシブモードで展開されます。これらは同じサブネット上にあり、同じソフトウェアバージョンとビルドを使用し、同じ構成である必要があります。
- 浮動IPアドレス:
    - 浮動IPアドレスはプライマリノードで構成されます。
    - 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または浮動IPアドレスのいずれかを使用できます。

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

注意

Citrixでは、ユーザーインターフェイスにアクセスするために浮動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 ADMのアップグレード:
  - 内部プロセスにより、NetScaler ADM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

アップグレードが成功したら、フローティングIPアドレスを設定する必要があります。

- ハートビートの送受信のために、両方のノードでUDPデフォルトポート5005が利用可能です。
- MACアドレスハイパーバイザーの「MACアドレスの変更」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にフローティング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アドレスの変更を有効にしてください。 たとえば、VMware ESXiでNetScaler ADM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では、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が許可されるようになりました。

注

ESXIバージョン6.7に展開されたNetScaler ADMの場合、「**MACアドレスの変更**」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アドレスの変更**」設定に関係なく、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。

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

NetScaler ADM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は、「**MACアドレスの変更**」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 ADMノードの高可用性を設定する前に、次の前提条件に注意してください。

- NetScaler ADMの高可用性展開は、NetScaler ADM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 Application Delivery Managementイメージファイル（.xva）をダウンロードします: `<https://www.citrix.com/downloads/>`

Citrixは、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推奨します。

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	Citrixでは、NetScaler ADM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。デフォルト値は120 GBです。実際のストレージ要件は、NetScaler ADMのサイジング見積もりによって異なります。NetScaler ADM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。Citrixでは、初期展開時にストレージを見積もり、追加ディスクを接続することを推奨しています。詳細については、「NetScaler ADMへの追加ディスクの接続方法」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**

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

コンポーネント	要件
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

高可用性モードでNetScaler ADMをセットアップするには

1. 最初のサーバー（プライマリノード）を登録して展開します。
2. 2番目のサーバー（セカンダリノード）を登録して展開します。
3. 高可用性セットアップのためにプライマリノードとセカンダリノードを展開します。

最初のサーバー（プライマリノード）を登録して展開する

最初の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て、ハイパーバイザーにインポートします。

   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**Start**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. **Console**タブから、NetScaler ADM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（*nsrecover/nsroot*）を使用してログオンします。

© 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。

5. プライマリノードを展開するには、**/mps/deployment_type.py**と入力します。NetScaler ADM展開構成メニューが表示されます。

   「構成メニュー」(/en-us/netscaler-application-delivery-management-software/media/ha-deploymentconfig.png)

6. NetScaler ADMサーバーをプライマリノードとして登録するには、**1**を選択します。

   「プライマリノードの登録」(/en-us/netscaler-application-delivery-management-software/media/drstep4.png)

7. コンソールは、NetScaler ADMスタンドアロン展開を選択するように促します。高可用性としての展開を確認するには、**No**と入力します。

   「展開の確認」(/en-us/netscaler-application-delivery-management-software/media/deploystep2.png)

8. コンソールは、最初のサーバーノードを選択するように促します。ノードを最初のノードとして確認するには、**Yes**と入力します。

   ノードの確認(/en-us/netscaler-application-delivery-management-software/media/deploystep3.png)

9. コンソールはシステムの再起動を促します。**Yes** と入力して再起動します。

   システムの再起動(/en-us/netscaler-application-delivery-management-software/media/deploystep4.png)

   システムが再起動し、NetScaler ADMユーザーインターフェイスでプライマリノードとして表示されます。

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

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、ハイパーバイザーにインポートします。
2. **Console**タブから、次の図に示すようにNetScaler ADMを初期ネットワーク構成で構成します。

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

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*。

   注

   ログオン後、初期ネットワーク構成を更新したい場合は、`networkconfig`と入力し、構成を更新して保存します。

4. セカンダリノードを展開するには、**/mps/deployment_type.py**と入力します。NetScaler ADM展開構成メニューが表示されます。
5. NetScaler ADMサーバーをセカンダリノードとして登録するには、**1**を選択します。
6. コンソールは、NetScaler ADMをスタンドアロン展開として選択するように促します。高可用性としての展開を確認するには、**No**と入力します。
7. コンソールは、最初のサーバーノードを選択するように促します。ノードを2番目のサーバーとして確認するには、**No**と入力します。

   2番目のノードの確認(/en-us/netscaler-application-delivery-management-software/media/deploystep5.png)
8. コンソールは、プライマリノードのIPアドレスとパスワードの入力を求めます。

   IPアドレスを入力してください(/en-us/netscaler-application-delivery-management-software/media/deploystep6.png)
9. コンソールは、フローティングIPアドレスの入力を求めます。

   フローティングIPを入力してください(/en-us/netscaler-application-delivery-management-software/media/deploystep7.png)
10. コンソールは、システムの再起動を求めます。再起動するには「**Yes**」と入力します。

    注

    - 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。
    - 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。

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

プライマリノードとセカンダリノードを高可用性ペアとして展開する

登録後、プライマリノードとセカンダリノードの両方がNetScaler ADMユーザーインターフェイスに表示されます。これらのノードを高可用性ペアとして展開します。

注

- ノードを高可用性ペアとして展開する前に、初期ネットワーク設定後、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。
- 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 ADMユーザーインターフェイスにアクセスします。

ノードを高可用性ペアとして展開するには：

1. Webブラウザを開き、最初のNetScaler ADMサーバーノードの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. ホームページで**開始**をクリックします。
4. 展開タイプとして**高可用性モードで展開された2台のサーバー**を選択し、**次へ**をクリックします。
5. 展開ページで**展開**をクリックします。
6. 確認メッセージが表示されます。**はい**をクリックします。

   NetScaler ADMが再起動し、構成が有効になるまでに約10分かかります。

   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。

7. 管理者資格情報を使用してNetScaler ADMにログオンし、ホームページで**開始**をクリックし、必要に応じて、以下を完了します。

   a. NetScalerインスタンスを追加

   b. 顧客IDを構成

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

> **注**
>
> **スキップ**をクリックして後で完了することもできます。その後、**完了**をクリックします。

8. **設定 > 展開**に移動して、展開を検証します。

   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 ADM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 ADM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 ADM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**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. **システム**タブで、**展開**に移動し、**HAの解除**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

スタンドアロン展開への高可用性を無効にした後、高可用性モードに再度再展開できます。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、プライマリノードとセカンダリノードを高可用性ペアとして展開するを参照してください。

> **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。

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

高可用性フェールオーバーシナリオ

以下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、180秒間プライマリノードからの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 ADMのプロセスのいずれか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の表示

NetScaler ADM 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、**Sync Database**ボタンが表示されます。**Sync Database**ボタンをクリックすると、データベース同期プロセスを開始できます。

ログメッセージ(/en-us/netscaler-application-delivery-management-software/media/log-message-ha.png)

データベース同期の進行状況を表示するには、**View Logs**をクリックします。**Database Sync Logs**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。

ログメッセージの同期(/en-us/netscaler-application-delivery-management-software/media/log-message-ha-sync.png)

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

たとえば、ある企業では2つのNetScaler ADM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により、2つのNetScaler ADMノード間の通信が完全に途絶えます。180秒以上ハートビートの交換がないため、両ノードは自身をプライマリノードと見なします。両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。

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

NetScaler ADM 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、ノード間のリンクのデータ量と速度に依存します。

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。

高可用性のためのディザスタリカバリを構成する

災害とは、自然災害または人為的な事象によって引き起こされるビジネス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、災害サイト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。データセンターでのデータ損失やダウンタイムは致命的であり、事業継続性を破綻させます。

NetScaler® ADMのディザスタリカバリ（DR）機能は、高可用性モードで展開されたNetScaler ADMに対し、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 ADM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、高可用性モードで展開されたNetScaler ADM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稼働しません。
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災害が発生し、機能しなくなった場

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

用語	説明
	合、このノードが（新しいプライマリとして）稼働状態になります。

注

プライマリサイトとDRサイトはポート5454および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。

災害復旧ワークフロー

次の画像は、災害復旧ワークフロー、災害前の初期設定、および災害後のワークフローを示しています。

災害前の初期設定

初期設定(/en-us/netscaler-application-delivery-management-software/media/drpriorsetup.png)

この画像は、災害前の災害復旧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 ADM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。

リカバリサイトには、リモートで展開されたスタンドアロンのNetScaler ADM災害復旧ノードがあります。災害復旧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、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災害復旧ノードにレプリケートされます。

前提条件

災害復旧ノードを設定する前に、以下の前提条件に注意してください。

- 災害復旧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 ADMノードが必要です。
- プライマリサイトにおけるNetScaler ADMのスタンドアロン展開は、災害復旧機能をサポートしていません。

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

- NetScaler ADM 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。

Citrixは、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推奨します。

次の表は、災害復旧ノードを構成するための最小要件を示しています。

コンポーネント	要件
RAM	32 GB
仮想CPU	8 CPU
ストレージ容量	Citrixは、NetScaler ADM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。デフォルト値は120 GBです。実際のストレージ要件は、NetScaler ADMのサイジング見積もりによって異なります。NetScaler ADM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。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。詳細については、「NetScaler ADM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 イーエスエックスアイ	5.5および6.0
マイクロソフト ハイパーブイ	2012 R2
リナックス ケーブイエム	UbuntuおよびFedora

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

初回ディザスターリカバリーのセットアップ

- NetScaler ADMを高可用性モードで展開する
- NetScaler ADMディザスターリカバリー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ー設定を有効/無効にする

NetScaler ADMを高可用性モードで展開する

ディザスターリカバリー設定をセットアップするには、NetScaler ADM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 ADMを高可用性で展開する方法については、「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 ADMは、NetScaler ADM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ーリカバリー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**。

DRコンソールを使用してNetScaler ADM災害復旧ノードを展開および登録する

NetScaler ADM災害復旧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. 「**コンソール**」タブから、初期ネットワーク構成でNetScaler ADMを構成します。

   注

   災害復旧ノードは、別のサブネット上に配置できます。

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（`nsrecover` / `nsroot`）を使用してログオンします。

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

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 ADM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の入力を求めます。
7. 災害復旧ノードをプライマリノードに登録するために、フローティングIPアドレスとパスワードを入力します。

   IPアドレスを入力してください(/en-us/netscaler-application-delivery-management-software/media/agentfloatingip.png)

   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)

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したい場合は、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
```

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

NetScaler ADM 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後、NetScaler ADM GUIからDRノードを展開します。この手順により、NetScaler ADM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. **災害復旧**ページで、**DRノードの展開**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**はい**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 ADM 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状態、メモリ、CPU、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、高可用性ペア用に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 ADM災害復旧ノードを展開および登録するの手順に従って、DRノードを構成します。
3. NetScaler ADM 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。

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

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、プライマリサイトが災害に見舞われ、動作不能であ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。
3. 管理者は、要件に基づいて（リカバリサイトで）、ディザスタリカバリノードで以下のリカバリススクリプトのいずれか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を構成します。

     ```
     /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構成します。

     ```
     /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。

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

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。

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」を参照してください。

重要

- NetScaler ADM 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 ADM（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 ADM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。

設定を元のプライマリサイトに戻す

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て流れます。

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。

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

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ADC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。災害復旧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 ADMプライマリノードを介して流れます。

マルチサイト展開用のオンプレミスエージェントを構成する

以前のバージョンのNetScaler ADM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 ADM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 ADM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 ADMのCPUおよびメモリリソースが使用されます。

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。

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

- 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® ADM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。

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 ADM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のインスタンス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 ADM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 ADM 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 ADMと通信できます。

エージェントは、プライマリNetScaler ADMと、異なるデータセンターで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 ADM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 ADM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と、エージェントのフェールオーバー時にNetScalerインスタンスが再配布されます。サイト内の1つのエージェントが失敗した場合、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。

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

注

サイトごとにインストールす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。

アーキテクチャ

次の図は、2つのデータセンターにおける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 ADM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 ADM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 ADM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 ADM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 ADMサーバーに登録されます。インスタンスは、プライマリNetScaler ADM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、圧縮形式でプライマリNetScaler ADM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 ADM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。

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する
  - エージェントを登録する
  - エージェントをサイトにアタッチする
- NetScalerインスタンスを追加する
  - 新しいインスタンスを追加する
  - 既存のインスタンスを更新する

データセンターにエージェントをインストールする

エージェントをインストールして構成することで、プライマリNetScaler ADMと別のデータセンターにある管理対象NetScalerインスタンス間の通信を有効にできます。

エンタープライズデータセンターの以下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。

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

- 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 Hyper-V
- リナックス 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 ADM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揃っ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
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

ポート

通信のために、エージェントとNetScaler ADMオンプレミスサーバー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 ADM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 ADM

エージェントとNetScalerインスタンスの間で、次のポートを開放する必要があります。

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

タイプ	ポート	詳細	通信の方向
TCP	80	エージェントとNetScalerインスタンス間のNITRO通信用。	NetScaler ADMからNetScaler、およびNetScalerからNetScaler ADM
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 ADMサーバー間の同期用。	NetScaler ADMからNetScaler、およびNetScalerエージェントからNetScaler
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 ADM への接続
ICMP	予約ポートなし	NetScaler ADM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 ADM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 ADMからNetScalerへ
			ポート162 - NetScalerからNetScaler ADMへ
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 ADM への接続

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

タイプ	ポート	詳細	通信の方向
TCP	5557	エージェントとNetScalerインスタンス間のLogstream通信用。	NetScaler から NetScaler ADM へ

エージェントの登録

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 ADMを初期ネットワーク構成で設定します。
3. NetScaler ADM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。

   登録1(/en-us/netscaler-application-delivery-management-software/media/register1.png)
4. 登録が成功すると、コンソールにログオンを促すメッセージが表示されます。資格情報として *nsrecover/nsroot* を使用します。
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、次のイメージに示すように表示されます。
6. NetScaler ADM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2(/en-us/netscaler-application-delivery-management-software/media/register2.png)

登録が成功すると、エージェントが再起動し、インストールプロセスが完了します。

エージェントが再起動したら、NetScaler ADM 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** 状態で表示されます。

注

NetScaler ADM 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。Citrix は、エージェントのバージョンを NetScaler ADM のバージョンにアップグレードすることを推奨します。

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

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、**サイトをアタッチ**をクリックします。
2. **サイトをアタッチ**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。

アクションの選択で、次の機能を使用できます。

新しい証明書をインストールする: 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。

デフォルトのパスワードを変更する: 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を生成する: 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インスタンスを追加する

インスタンスとは、エージェントを介してNetScaler ADMから検出、管理、監視したいNetScaler ADCアプライアンスまたは仮想アプライアンスのことです。次のNetScaler ADCアプライアンスと仮想アプライアンスをNetScaler ADMまたはエージェントに追加できます。

- NetScaler MPX

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

- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- ネットスケーラー ゲートウェイ
- シトリックス SSL フォワードプロキシ

詳細については、「NetScaler ADMへのインスタンスの追加」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 ADM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. **インフラストラクチャ > インスタンス**に移動し、インスタンスタイプを選択します。たとえば、NetScalerです。
2. **編集**をクリックして、既存のインスタンスを編集します。
3. クリックしてエージェントを選択します。
4. **エージェント**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。

> **注**
>
> インスタンスを関連付けたい**サイト**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後、インスタンスのGUIにアクセスし、トラップの宛先が構成されているか確認します。

NetScaler ADMで、**Infrastructure > Instances**に移動します。**Instances**で、アクセスしたいインスタンスの種類 (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上でトラップの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、トラップの宛先を確認します。

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

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、インスタンスを追加する際に**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ールオーバー

エージェントのフェールオーバーは、2つ以上の登録済み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。サイト内でエージェントが非アクティブ (DOWN状態) になると、NetScaler ADMは、非アクティブなエージェントのADC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。

重要

- アカウントで**エージェントフェールオーバー**機能が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、「ADM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、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。したがって、変更されたエージェントは、エージェントのフェールオーバー後にスクリプトを実行できます。

ADM 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 ADMがそれを検出し、状態をダウンとして表示します。

サイト内のNetScalerエージェントが非アクティブ（ダウン状態）になると、NetScaler ADM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である場合、NetScaler ADM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。

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

NetScaler ADM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、特定の期間到達不能な場合、メール、Slack、PagerDuty、ServiceNowを介してエージェントステータスに関する通知を受け取ることができます。**インフラストラクチャ > インスタンス > エージェント**で、**設定**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。

Kubernetesクラスターにマイクロサービスとして ADMエージェントをインストールする

NetScalerエージェントをマイクロサービスとして展開することは、NetScaler CPXの管理に役立ちます。このドキュメントで利用できる手順は、NetScaler ADMとKubernetesクラスターが異なるネットワーク上に構成されている場合にのみ適用されます。このシナリオでは、Kubernetesクラスターがホストされている場所にADMエージェントをマイクロサービスとして構成できます。

注

また、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。

はじめに

1. NetScaler® ADM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。
    a. **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です。
    b. **Password** – CPXがエージェントを介してADMにCPXをオンボーディングするために使用するパスワードを指定します。
    c. **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

デフォルトのパスワード（`nsroot`）を使用してはいけません。

d. **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:

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 testing.yaml`

   エージェントが正常に作成されました。

NetScaler ADMで、**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 ADMへのNetScaler CPXインスタンスの追加。
- サービスグラフのセットアップ。

NetScaler® ADMシングルサーバー展開を高可用性展開に移行する

NetScaler ADMシングルサーバーを、2つのNetScaler ADMサーバーの高可用性展開にアップグレードできます。NetScaler ADMサーバーの高可用性ペアはアクティブ/パッシブモードであり、両方のサーバーは同じ構成を持っています。このタイプのアクティブ/パッシブ展開では、一方のNetScaler ADMサーバーがプライマリノードとして構成され、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。

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

NetScaler ADMシングルサーバーを高可用性ペアに移行するには、新しいNetScaler ADMサーバーノードをプロビジョニングし、それを2番目のNetScaler ADMシングルサーバーとして構成し、両方のNetScaler ADMサーバーを高可用性ペアとして展開する必要があります。

NetScaler ADMシングルサーバーを高可用性モードに移行するには、次の手順が含まれます。

1. 既存のサーバーノードを変更する
2. 2番目のサーバーノードをプロビジョニングする
3. 2つのノードをHAモードで展開する
4. 高可用性ペアを構成する

既存のNetScaler ADMサーバーノードを変更する

NetScaler ADMをシングルサーバーから高可用性モードに移行するには、サーバーノードの初期展開タイプを高可用性モードに変更する必要があります。

1. ワークステーションまたはラップトップで、既存のNetScaler ADMサーバーノードのコンソールを開きます。たとえば、IPアドレスが10.106.171.17のNetScaler ADMをスタンドアロンサーバーとして展開したと仮定します。
2. NetScaler ADMにログオンします。デフォルトの資格情報は `nsroot` と `nsroot` です。
3. シェルプロンプトで `/mps/deployment_type.py` と入力し、**Enter**キーを押します。
4. 展開タイプとしてNetScaler ADMサーバーを選択します。オプションを選択しない場合、デフォルトでサーバーとして展開されます。

5. 展開コンソールは、サーバー展開（スタンドアロンとして）を選択するよう求めます。高可用性ペアとしての展開を確定するには、**No** と入力します。
6. コンソールは、（最初のサーバーノード）を選択するよう求めます。そのノードを最初のサーバーノードとして確定するには、**Yes** と入力します。
7. コンソールは、サーバーを再起動するよう求めます。
8. 再起動するには、**Yes** と入力します。

2番目のサーバーノードをプロビジョニングする

ハイパーバイザー上に2番目のサーバーをプロビジョニングする必要があります。最初のサーバーのインストールに使用したのと同じイメージファイルを使用するか、NetScalerサイトから同じバージョンのイメージファイルを入手してください。

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

1. イメージファイルをハイパーバイザーにインポートし、その後、コンソールタブから、以下の画面で説明されている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後、シェルプロンプトで /mps/deployment_type.py と入力し、Enterキーを押します。
3. 展開タイプとして **NetScaler ADM server** を選択します。
4. 展開コンソールは、サーバー展開（スタンドアロンとして）を選択するよう求めます。高可用性ペアとしての展開を確定するには、**No** と入力します。

5. コンソールは次に、（最初のサーバーノード）を選択するよう求めます。そのノードを2番目のサーバーノードとして確定するには、**No** と入力します。

6. 最初のサーバーのIPアドレスとパスワードを入力します。

   サーバーIPアドレスを指定します(/en-us/netscaler-application-delivery-management-software/media/deploystep6.png)

7. 最初のノードのフローティングIPアドレスを入力します。

   フローティングIPアドレスを指定します(/en-us/netscaler-application-delivery-management-software/media/deploystep7.png)

8. コンソールはシステムの再起動を促します。再起動するには「**Yes**」と入力します。

2台のサーバーを高可用性モードで展開する

2つのサーバーノードを高可用性ペアとしてインストールするプロセスを完了するには、既存のNetScaler ADMサーバーノードのGUIからこれらのノードを展開する必要があります。2つのサーバーノードを展開すると、2つのサーバー間の内部通信が開始されます。

重要

高可用性ノードを展開する前に、必ずデフォルトのパスワードを変更してください。

1. Webブラウザで、既存のNetScaler ADMサーバーノードの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. **システム**タブで、**展開**に移動し、**展開**をクリックします。
4. 確認メッセージが表示されます。「**はい**」をクリックします。

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

注

NetScaler ADMを高可用性で展開した後、プライマリ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できます。バージョン12.1以降では、セカンダリノードにアクセスすることはできません。

5. 2番目のサーバーノードを設定する際にフローティングIPを入力しましたが、**システム**ページでFIPを更新するオプションがあります。**HA設定** > **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。以前に設定したフローティングIPアドレスを表示できます。新しいIPアドレスを入力して**OK**をクリックします。

NetScaler® Insight Center から NetScaler ADM 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 ADM に移行できるようになりました。NetScaler ADM 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、移行がサポートされているのは、NetScaler Insight Center のスタンドアロンインスタンスのみです。

前提条件

NetScaler Insight Center 仮想アプライアンスを NetScaler ADM に移行する前に、次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 ADM 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 ADM 12.0 build 57.24 をインストールし、その後、最新の NetScaler ADM 13.1 build 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。

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

- NetScaler ADM 13.1 の最新のビルドの .tgz イメージファイルをダウンロード済みであること。

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 Citrixでは、パフォーマンス向上のために**500 GB**の使用を推奨しています。また、NetScaler ADM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
ブイエムウェア ESX	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 ADM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 ADM 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。

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

4. **./installmas**コマンドを使用してNetScaler ADMをインストールします。

5. NetScaler ADM 12.0ビルド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 ADM 13.1ビルド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 ADMの**Infrasturcture > 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 ADMでは、デフォルトで、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 ADM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 ADMライセンス」(/ja-jp/netscaler-application-delivery-management-software/13-1/licensing.html)を参照してください。

NetScaler® ADM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 ADMと統合されます。

- ネットワーク分析は、NetScaler ADM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は展開環境におけるICAトラフィックの詳細な分析ビューを提供します。
- パフォーマンス管理は、履歴保持と傾向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、容量と健全性の傾向を含む傾向レポートを作成できます。

NetScaler ADMをDirectorと統合すると、HDX InsightレポートはDirectorで次の情報を提供します。

- ページのタブには、展開環境全体のアプリケーション、デスクトップ、およびユーザーに対する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および帯域幅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 ADMへの移行に関するハードウェア要件

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。Citrixでは、NetScaler ADM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お勧めします。
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

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 ADM仮想アプライアンスに移行する前に、次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 ADM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 for Macバージョン11.8以降、およびWindows版Citrix Workspace for Windows 14.0以降が利用可能であることを確認してください。
- NetScaler ADM バージョン 11.0 以降がインストールされていること。NetScaler ADM のインストール方法の詳細については、「NetScaler ADM 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、データは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 ADM を Director と統合する手順については、`<https://docs.citrix.com/ja-jp/xenapp-and-xendesktop/7-15-ltsr/director/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® ADM に補助ディスクを接続する

NetScaler Application Delivery Management (ADM) のストレージ要件は、NetScaler ADM 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 ADM 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、補助ディスクを接続できます。

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

注

- NetScaler ADM の初回展開時に、ストレージ要件を見積もり、サーバーに補助ディスクを接続します。
- NetScaler ADM のシングルサーバー展開の場合、デフォルトのディスクに加えて、サーバーに接続できるディスクは 1 台のみです。
- NetScaler ADM の高可用性展開の場合、各ノードに補助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。
- 以前に容量の小さい外部ディスクを接続していた場合は、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。
- 2 テラバイトを超える容量の補助ディスクを接続できます。必要に応じて、ディスクのサイズは 2 テラバイト未満でもかまいません。
- Citrix は、NetScaler ADM 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。

このドキュメントでは、補助ディスクの接続、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. 新しい補助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. 新しい補助ディスクにパーティションを作成する
4. 既存の補助ディスクのサイズを変更する
5. 追加ディスク上のパーティションを削除する

スタンドアロンのNetScaler ADMにディスクを追加する

仮想マシンにディスクを接続するには、次の手順を実行します。

1. NetScaler ADM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 ADM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 ADM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。

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

3. NetScaler ADM仮想マシンを起動します。

NetScaler ADMディスクパーティションツール

NetScaler ADMは、新しいコマンドラインツールである**NetScaler ADM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。このツールの機能は、以下に詳しく説明されています。

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

- データを失うことなく、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ことはできません。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 ADM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）の120ギガバイ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

1. PuTTYなどのSSHクライアントを使用して、NetScaler ADMへのSSH接続を開きます。
2. `nsrecover/nsroot`資格情報を使用して、NetScaler ADM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
```

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

注

高可用性展開のNetScaler ADM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。

新しい追加ディスクにパーティションを作成する

createコマンドは、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使用されます。「remove」コマンドを使用して既存のパーティションを削除した後、このコマンドを使用して既存のセカンダリディスクにパーティションを作成することもできます。

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スペースを使用します。

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、残りのスペースを使用するために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ことがあり、中断してはいけません。

作成コマンド 2(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-3.png)

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がマウントされるように仮想マシンが自動的に再起動されます。

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

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)

追加されたスワップパーティションは、「create」コマンドの出力で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

パーティションを作成した後、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最大2テラバイトまでです。

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、Citrix では、サイズ変更を試みる前に、このディスク内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)

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

「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。これにより、NetScaler ADMサブシステム、PostgreSQL DBプロセス、NetScaler ADMモニタープロセスなど、ディスクにアクセスしているプロセスが停止されます。プロセスが停止されると、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。

注

「ファイルシステムの拡張」プロセスは完了までに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変更後、ツールは仮想マシンを再起動します。 ファイルシステムの拡張 1(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-9.png)

ファイルシステムの拡張 2(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-10.png)

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。

サイズ変更完了(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-11.png)

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。サイズを増やした後の詳細を以下に示します。

変更前後の詳細(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-12.png)

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。これは、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するか、**remove**コマンドを使用して既存のパーティションを削除してから、新しいパーティションを作成できます。

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

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。

既存のパーティションを削除(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-13.png)

「remove」コマンドを実行すると確認を求められ、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 (ADMサブシステム、PostgreSQLプロセス、ADM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。

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とき、またはスワップファイルが作成されたときは、仮想マシンを再起動します。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、確認されると、すべてのプロセス (ADMサブシステム、PostgreSQLプロセス、ADM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

パーティションのサイズ変更または削除の前にNetScaler ADMデータをバックアップするには、次の手順に従います。

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

注

バックアップファイルの作成にはディスク容量が必要です。Citrixでは、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）があることを確認することをお勧めします。

1. ADM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. ADM Monitorを停止します。

```
/mps/scripts/stop_mas_monit.sh
```

4. tarballを作成します。

```
cd /var

tar cvfz /var/mps/mps_backup.tgz mps
```

注

この操作にかかる時間は、バックアップするデータのサイズによって異なります。

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. コピーされた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. ADM仮想マシンからtarballを削除します。

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

```
cd /var/mps/

rm mps_backup.tgz  mps_backup_checksum
```

その他のコマンド

前述のコマンドに加えて、ツールで次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数を提供します。スキームはMBRまたはGPTのいずれかです。MBRスキームは、NetScaler ADM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 ADM 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テラバイトより大きくすることができます。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。これはプラットフォームの既知の制限です。

Create_swapfileコマンド:

NetScaler ADM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であり、したがって、デフォルトのスワップスペースは4 GBです。NetScaler ADMのデフォルトのメモリ構成である2 GBの場合、このスワップスペースで十分です。ただし、より高いメモリ構成でNetScaler ADMを実行する場合、ディスク上により多くのスワップスペースを割り当てる必要があります。

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

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スペースとも呼ばれます。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 ADM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、デフォルトでスワップパーティションが作成されていません。「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 ADM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

「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。したがって、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チェックします。

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」と入力して**Enter**キーを押します。

高可用性で展開されたNetScaler ADMに追加ディスクを接続する

セカンダリディスクなしで高可用性セットアップにNetScaler ADM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

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

ことを確認したとします。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追加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. 再起動後、セカンダリノードを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。
8. ハイパーバイザー経由で追加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後、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状態であり、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. ADM_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. ADM_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。

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

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してください。

3. ADM_Primaryを再起動します。
4. ADM_Primaryが再起動したら、それがプライマリノードであることを確認します。
5. 次に、ADM_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、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.

設定

NetScaler® ADM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 ADM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。

構成ユーティリティとダッシュボードにアクセスするには、ワークステーション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 ADM GUIにアクセスするには：

管理者資格情報を使用してNetScaler ADMにログオンします。

NetScaler ADMにログオンした後、開始するには、以下を実行する必要があります。

- NetScaler ADM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場合は、NetScaler ADM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。アプリケーションの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 ADMでNTPサーバーを構成する。NetScaler ADMのクロックをNTPサーバーと同期させるには、NetScaler ADM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 ADM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。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 ADMを使用し始める前に、NetScaler ADMサー

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

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® ADMにインスタンスを追加する

インスタンスとは、NetScaler ADMから検出、管理、監視したいNetScaler ADC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 ADMサーバーにインスタンスを追加する必要があります。NetScaler ADMには、次のNetScaler ADCアプライアンスと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 ADM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 ADM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 ADM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 ADMの間で開いておく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 ADM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プロファイルを作成する方法

NetScalerプロファイルには、NetScaler ADMに追加するインスタンスのユーザー名、パスワード、通信ポート、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の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

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

の資格情報を変更した場合は、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時に作成できます。

注記

インスタンスプロファイルを作成するには、必ず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. **プロファイル名**: NetScalerインスタンスのプロファイル名を指定します。
   b. **ユーザー名**: 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. **パスワード**: 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ポート**: NetScaler ADMとNetScalerインスタンス間のSSH通信用のポートを指定します。
   e. **HTTPポート**: NetScaler ADM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インスタンスで設定した、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 ADMとNetScaler CPX間の通信にのみ使用できます。

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

f. **HTTPSポート**: NetScaler ADM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インスタンスで設定した、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 ADMとNetScaler CPX間の通信にのみ使用できます。

g. **NetScaler通信にグローバル設定を使用**: NetScaler ADM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**: NetScaler ADMが再起動後に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 ADMにADCインスタンスを追加する

インスタンスは、NetScaler ADM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 ADM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。

2つのNetScaler ADMサーバーが高可用性モードで設定されている場合、インスタンスが追加されると、トラフィックソースはADMフローティングIPアドレスを介して行われます。

オンプレミス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ADMエージェントを介して行われます。

NetScaler ADM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 ADM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。
   - **Enter Device IP address** - NetScalerインスタンスの場合、各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します。

     SNIPを使用してADC 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>
     ```

     例: `10.10.10.11#10.10.10.12`
   - **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新しいプロファイルを作成します。

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

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新しい場所を作成します。
6. **OK**をクリックして、NetScaler ADM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、**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、**アクションの選択**リストから**再検出**をクリックします。

NetScaler ADMにNetScaler CPXインスタンスを追加する

NetScaler ADM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 ADM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、VPXやMPXなどの他のADCタイプがADMに追加される方法と同様になりました。また、ADMでのCPXの登録も強化されました。CPXが起動すると、NetScaler ADM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ることはなくなりました。

1. **インフラストラクチャ > インスタンス > NetScaler**に移動し、**CPX**タブをクリックします。
2. **追加**をクリックして、NetScaler ADM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。

    NetScaler CPXを追加(/en-us/netscaler-application-delivery-management-software/media/add-cpx-instances-citrix.png)

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

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を作成する際に、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、ホストによって公開されたポートの範囲を、**開始ポート**と**ポート数**のフィールドで指定することもできます。

4. **OK**をクリックします。

NetScaler ADM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サーバー上で動作す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を指定し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。

   NetScaler ADM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。

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

9. 「**OK**」をクリックします。

NetScaler BLXスタンドアロンインスタンスをNetScaler ADMに追加(/en-us/netscaler-application-delivery-management-software/media/add-blx-standalone-instance-citrix.png)

NetScaler ADM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サーバーで実行されます。1つの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**」フィールドに、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**」フィールドに、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インスタンスの適切な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。

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 ADMに1つのエージェントのみが構成されている場合、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。

NetScaler ADMにNetScaler BLX高可用性インスタンスを追加(/en-us/netscaler-application-delivery-management-software/media/add-blx-ha-instance-citrix.png)

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

NetScaler ADM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. アクセスしたいインスタンスの種類を選択します (例: VPX、MPX、CPX、SDX、または BLX)。
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。

インスタンスの表示(/en-us/netscaler-application-delivery-management-software/media/view-instance-citrix.png)

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 ADMに追加する

NetScaler ADM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 ADM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 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。

以下のサンプルトポロジでは、NetScaler ADMとクラウドに展開されたNetScaler VPXインスタンス間のレイヤー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.png)

データセンターDCのNetScalerアプライアンスNS_Appliance-DCと、パブリッククラウドの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 ADM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 ADM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。
   - 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。

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

- 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間で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 ADMとクラウドに展開されている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® ADM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。

   c. **Network Address**フィールドに、コネクタを介してNetScaler ADMから静的ルートを確立する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 ADMに追加します。詳細な手順については、Add Instances to NetScaler ADMを参照してください。

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

仮想サーバーでのライセンス管理とアナリティクスの有効化

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ます。「**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。仮想サーバーをライセンスし、単一のワークフローでアナリティクスを有効にできます。

「**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、次のことができます。

- ライセンスされていない仮想サーバーにライセンスを適用する
- ライセンスされている仮想サーバーからライセンスを削除する
- ライセンスされてい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

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

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。

仮想サーバーのライセンスを管理する

仮想サーバーのライセンスを付与するには、**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。

   分析を有効にする(/en-us/netscaler-application-delivery-management-software/media/enable-analytics-citrix.png)

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

> **注**
>
> または、特定のインスタンスの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。

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 セキュリティ違反) を選択します。

b. 転送モードとして **Logstream** を選択します。

> **注**
>
> NetScaler 12.0 以前の場合、**IPFIX** が転送モードのデフォルトオプションです。
> NetScaler 12.0 以降の場合、転送モードとして **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** - 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。

© 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® ADM 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ト、認証、GSLB などの仮想サーバーの場合、分析を有効にすることはできません。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 ADM は、選択した仮想サーバーで分析を有効にする処理を行います。

「

注

」

NetScaler ADM 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 ADM 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	ソース 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：

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分析を編集することもできます。

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

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、**分析を編集**をクリックします。

2. **分析を編集**をクリックします

3. **分析構成の編集**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。

分析を無効にする

選択した仮想サーバーで分析を無効にするには：

1. 仮想サーバーを選択します
2. **分析を無効にする**をクリックします

NetScaler ADM は、選択した仮想サーバーの分析を無効にします。

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 ADM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	非対応	•
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	•	•

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

仮想サーバーでアナリティクスを有効にするための統合プロセス

既存のアナリティクス有効化プロセスとは別に、単一ペインの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済み仮想サーバー
- その後のライセンス済み仮想サーバー

設定後、この機能により、既存およびその後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® ADM の以下の動作を理解しておく必要があります。

- 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します。

  Web Insight、HDX™ Insight、および Gateway Insight を選択して、アナリティクス設定を初めて構成したとします。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。
- 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 台のライセンス済み仮想サーバーがあり、そのうち 2 台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 台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になっている仮想サーバー。

  10 台のライセンス済み仮想サーバーがあり、2 台の仮想サーバー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、この機能は残りの 8 台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になっている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ること。

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

- 後続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ること。**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。

   グローバルアナリティクス設定(/en-us/netscaler-application-delivery-management-software/media/global-analytics-configuration.png)
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。
4. 後続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。

   アナリティクス設定(/en-us/netscaler-application-delivery-management-software/media/analytics-configuration-citrix.png)

NTPサーバーを構成する

NetScaler® ADMで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 ADM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 ADMでNTPサーバーを構成するには：

1. ADM GUIから、**設定 > 管理**に移動します。**システム管理**ページで、**ネットワーク構成**の下にある**NTPサーバー**をクリックします。次に、**追加**をクリックします。
2. **NTPサーバーの作成**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のべき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のべき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。

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

- **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. **作成**をクリックします。

NetScaler ADMでNTP同期を有効にするには：

1. **NTPサーバー**のホームページに移動します。
2. **NTP同期**をクリックし、**NTP同期を有効にする**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 ADM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「**はい**」をクリックします。

システム設定を構成する

NetScaler® ADM を使用してインスタンスとアプリケーションの管理および監視を開始する前に、NetScaler ADM 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の問題を認識できるように、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を超えた場合（例: memoryUsageHigh）や、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. **>** の順に移動し、右上隅にある タブをクリックします。

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

2. 構成するアラームを選択し、 をクリックします。
3. 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、 **>** の順に移動し、 をクリックします。

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 ADM で通知サーバーをセットアップし、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. **>** の順に移動します。 ページの で、 **>** をクリックします。
2. ページで、NetScaler ADM 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。

システムプルーニング設定の構成

NetScaler ADM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 ADM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）にプルーニングされます。

システムプルーニング設定を構成するには:

1. **設定 > システム管理**に移動します。**データプルーニング**の下で、**システムおよびインスタンスデータプルーニング**をクリックします。
2. **システム**ページで、データを保持する日数を指定し、**保存**をクリックします。

インスタンスsyslogプルーニング設定の構成

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 ADM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パージ設定を構成するには:

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

1. **設定 > 管理 > データプルーニング**に移動します。
2. **システムおよびインスタンスデータプルーニング > インスタンスSyslog**をクリックします。
3. **インスタンスSyslogプルーニング設定の構成**ページで、**Syslog汎用データの保持**フィールドに1から180までの日数を指定します。
4. **保存**をクリックします。

インスタンスイベントプルーニング設定の構成

NetScaler ADM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 ADM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）にプルーニングされます。

インスタンスイベントプルーニング設定を構成するには:

1. 「**Settings > Administration**」に移動します。
2. 「**System Administration**」ページで、「**Data Pruning**」の下にある「**System and Instance Data Pruning**」をクリックします。
3. 「**Data Pruning**」ページで、「**Instance Events**」をクリックします。
4. 「**Data to keep (days)**」フィールドに、NetScaler ADMサーバーでデータを保持する期間（日数）を入力し、「**Save**」をクリックします。

システムバックアップ設定を構成する

NetScaler ADM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を保存します。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. 「**Settings > Administration**」に移動します。
2. 「**Backup**」の下にある「**Configure System and Instance backup**」をクリックします。
3. 「**System**」をクリックし、「**Configure System Backup Settings**」ページで必要な値を指定します。

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

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回復できます。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. 「**Settings > Administration**」に移動します。
2. 「**Backup**」の下にある「**Configure System and Instance backup**」をクリックします。
3. 「**Configure Instance Backup Settings**」の下にある「**Instance**」をクリックし、必要な値を指定します。

ADM機能の有効化または無効化

管理者として、「**Settings > Administration > Configurable Features**」ページで以下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。サイト内でエージェントが非アクティブ（DOWN状態）になると、NetScaler ADMサービスは、非アクティブなエージェントのADC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、ADC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 ADMは設定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ADC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。
- **インスタンス構成監査** - 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、保存されていない構成を回復します。詳細については、「監査テンプレートの作成」を参照してください。
- **インスタンスイベント** - 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。NetScaler ADM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

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

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** - グローバルレベルでインスタンスのレポートを生成できます。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 ADMは、すべての管理対象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** - すべてのSyslogメッセージをNetScaler ADMにリダイレクトするようにデバイスを設定している場合、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. 「**Enable**」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® ADMとServiceNowインスタンスの統合

NetScalerおよびADMイベントのServiceNow通知を有効にするには、NetScaler ADM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 ADMとServiceNowインスタンス間で通信します。

ADM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。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アダプターの仕組み」を参照してください。

オンプレミス展開のADMをITSMアダプターに接続するには、顧客IDを構成してください。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

ADMをServiceNowと統合する前に、以下を確認してください。

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

1. Citrix Cloudにサインアップします。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。

ADMをServiceNowと統合する方法?

ITSMコネクタを使用してNetScaler ADMをServiceNowと統合するには、次の手順を実行します。

1. Citrix Cloud™でITSMアダプターサービスをサブスクライブする。
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. ADMでServiceNowチケットの自動生成をテストする。

ステップ 1 - Citrix CloudでITSM Adapterサービスをサブスクライブする

1. **ITSM Adapter** タイルで、**Request Trial** をクリックします。

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、次に **Authenticate** をクリックします。Citrix CloudからメモしたClient IDとSecretを入力します。
4. 接続をテストします。
5. 構成を保存します。ServiceNowからの確認メッセージが表示され、接続がアクティブであることを示します。
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. Client IDとClient Secretを使用してアクセスおよび更新トークンを取得します。OAuthトークンを参照してください。

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

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. 「**テスト**」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. 接続テストが正常に完了したら、ServiceNowインスタンスを追加するために「**保存**」をクリックします。

ステップ4 - ADMでのServiceNowチケットの自動生成をテストする

1. NetScaler ADMにログインします。
2. 「**アカウント > 通知**」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. ServiceNowチケットを自動生成し、設定を確認するために「**テスト**」をクリックします。

   NetScaler ADM GUIでServiceNowチケットを表示したい場合は、「**ServiceNowチケット**」を選択します。

ADM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後、NetScaler ADM GUIで以下のイベントに対してServiceNow通知を設定できます。

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 ADMは、選択された管理対象NetScalerインスタンスからの選択された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イベントに対して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**ServiceNow通知の送信**として割り当てる必要があります。

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

ADMで、**インフラストラクチャ > イベント > ルール**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、「ServiceNow通知の送信」を参照してください。

- **アプリケーション分析**: NetScaler ADMは、指定されたしきい値を超過し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。

  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証明書およびADMライセンスイベント**: NetScaler ADMは、SSL証明書の有効期限切れイベントおよびADM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、「SSL証明書の有効期限切れ」を参照してください。

  ADM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、「NetScaler ADMライセンスの有効期限切れ」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設定

NetScaler® ADM では、選択した NetScaler ADM 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。

NetScaler ADM は、個々の ADM 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ます。これらは表示、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

ADM 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。

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

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、ADM 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、ADM 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。

    ADM レポートをエクスポートする(/en-us/netscaler-application-delivery-management-software/media/export-snapshot-citrix.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. をクリックします。

エクスポートレポートのスケジュール設定

定期的にエクスポートレポートをスケジュールするには、繰り返し間隔を指定します。NetScaler ADM 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. を選択し、以下を指定します。

    - **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** - ADM 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 、、または 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オンにし、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、 をクリックします。
    - **Slack** - チェックボックスをオンにし、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、 をクリックします。

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

3. 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. ページ右上の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、機能固有のすべて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 ADMの各リリースでは、機能が強化された新しい機能や更新された機能が提供されます。Citrixでは、新しい機能やバグ修正を利用するために、NetScaler ADM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。機能強化、既知の問題、バグ修正の包括的なリストは、すべての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。また、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 ADM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。

アップグレードパスの情報は、Citrix Upgrade Guideでも入手できます。

アップグレードする前に

NetScaler ADM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、この記事の指示に従ってシステムを最新の13.1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、ADMは再起動し、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 ADMはデータを処理しません。

重要

NetScaler ADM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 ADM 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。

13.1へのアップグレード前に注意すべき点:

- 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。

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

- 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にアップグレードしてから13.1にアップグレードします。
- 12.1からアップグレードする場合は、直接13.1にアップグレードできます。
- 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てから13.1にアップグレードしてください。

13.1-xx.xx以降へのアップグレード前に注意すべき重要な点

ADMソフトウェアをバージョン13.1-xx.xxにアップグレードすると、ADMデータベースも移行されます。このデータ移行は、ADM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

ADMソフトウェア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:

- 13.1-xx.xx以降にアップグレードする場合は、NetScaler ADM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® ADM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 ADM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。
- 13.1.9.xから13.1.30.xまでのいずれかのバージョンにアップグレードすると、NetScaler ADMは既存のStyleBooks ConfigPacksを以前のバージョンにロールバックします。

  この問題を回避するには、13.1.33.50ビルドにアップグレードしてください。
- 高可用性セットアップのNetScaler ADM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.

- アップグレード後、高可用性ペアのアクティブノードが変更される可能性があります。

単一のNetScaler ADMサーバーを13.1-12.xにアップグレードする

1. 管理者資格情報を使用してNetScaler ADMにログオンします。
2. **Settings > Administration** に移動します。**System Maintenance** の下にある **Upgrade NetScaler ADM** をクリックします。

3. **Upgrade NetScaler ADM** ページで、アップグレード後にイメージファイルを削除するには、**Clean software image on successful upgrade** チェックボックスをオンにします。このオプションを選択すると、アップグレード時にNetScaler ADM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オンにしなかった場合、イメージを手動で削除する必要があります。

4. その後、**Local** (ローカルマシン) または **Appliance** 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 ADM仮想アプライアンスに存在する必要があります。
5. **OK** をクリックします。
6. **Upgrade ADM** ページには、ファイル名、選択されたバージョン、完了までの推定時間などの詳細が表示されます。**Upgrade** 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、ADM 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ADMでの作業を続行できます。

履歴データ移行中、一部の古いデータが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。

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

ADM GUIを使用してデータベース移行を監視できます。「**View upgrade progress**」をクリックすると、「**Database Migration Status**」が表示されます。

アップグレードが完了すると、デフォルトの無料ライセンスが2つに減らされたというメッセージが表示されます。詳細については、「**View Details**」をクリックしてください。

単一のNetScaler ADMサーバーを13.1-4.xまたは13.1-9.xにアップグレードする

1. 管理者資格情報を使用してNetScaler ADMにログオンします。
2. **System** \> **System Administration** に移動します。「**System Administration**」の見出しの下にある「**Upgrade NetScaler ADM**」をクリックします。
3. **Upgrade NetScaler ADM** ページで、「**Clean software image on successful upgrade**」チェックボックスを選択して、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 ADM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、「**Local**」（ローカルマシン）または「**Appliance**」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 ADM仮想アプライアンスに存在する必要があります。
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。

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

設定が移行された後、ADM GUIにログオンできます。ログオンすると、履歴データがバックグラウンドで移行を開始し、その間もADMでの作業を続行できます。

履歴データ移行中、一部の古いデータが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。

ADM 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。

データベース移行の問題のトラブルシューティング

13.1-xx.xx以降へのアップグレードプロセス中に、Web Insightの履歴データの移行が停止しているように見える場合があります。そのような場合は、データ移行の詳細を確認するには、次の手順を実行します。

ADMシェルプロンプトにログオンし、次のコマンドを実行して進行状況の詳細を確認します。

```
cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
```

以下に出力例を示します

```
    bash-3.2# cat /var/mps/log/db_upgrade/
web_insight_mapping_migration_status

    Tue Oct  6 07:41:55 GMT 2020

    157 out of 127346 done in 54 seconds

    File

     /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
af_app_client_server_resp_second_l3p_d7_dump

    bash-3.2#
```

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

この例では、`af_app_client_server_resp_second_l3p_d7` はアップグレード中のエントリです。そして、127,346個のエントリのうち157個が54秒で移行されました。

12.1リリースから13.1リリースへの高可用性ペアのアップグレード

高可用性モードのNetScaler ADM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 ADM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 ADMディザスタリカバリ展開のアップグレード

NetScaler ADMのディザスタリカバリ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 ADMノードをアップグレードします。その後、ディザスタリカバリノードをアップグレードする必要があります。
- ディザスタリカバリ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 ADMサーバーをアップグレードしていることを確認してください。

NetScaler ADMディザスタリカバリノードをアップグレードする

1. NetScalerサイトからNetScaler ADM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` 資格情報を使用して、このファイルをディザスタリカバリノードにアップロードします。
3. `nsrecover` 資格情報を使用して、ディザスタリカバリ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

   ▢

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、次のタスクを完了していることを確認してください。

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

1. 高可用性で展開されているNetScaler ADMサーバーをアップグレードします。
2. NetScaler ADM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 ADM 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` 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` 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 ADM サーバーにディスクを追加する

NetScaler ADM のストレージ要件がデフォルトのディスク容量 (120 GB) を超える場合は、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、さらにディスクを接続できます。

NetScaler ADM をリリースバージョン 12.1〜13.1Œ からアップグレードしても、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同じままです。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。

ディスクを追加する手順は、アップグレードされたビルドでも同じです。NetScaler ADM 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成できるようになりました。このツールを使用して、既存の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 ADM 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.

StyleBookを使用してOpenStackでNetScalerインスタンスをプロビジョニングする

NetScaler ADM 12.1ビルド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 ADM 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12.1ビルド48.18からNetScaler ADM 13.1にアップグレードする場合、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
```

`os-cs-lb-mon` StyleBookと移行スクリプトの詳細については、StyleBookを使用したOpenStackでのNetScaler VPXインスタンスのプロビジョニング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® ADM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 ADM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 ADM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、および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 ADM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 ADM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 ADMへのアクセスを許可されます。

外部認証サーバー

NetScaler ADM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 ADM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 ADM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 ADM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 ADMでユーザーを認証する

NetScaler ADMでユーザーを認証する方法は2つあります。

- NetScaler ADMで構成されたローカルユーザー

  構成後、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。

  1 – ユーザーがNetScaler ADMにログオンします

  2 – NetScaler ADMは、認証のためにユーザーに資格情報を要求し、資格情報がADMデータベースと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

  設定後、外部の認証、認可、および監査サーバーにおけるユーザー認証のワークフローは次のとおりです。

  1 – ユーザーがNetScaler ADMに接続します

  2 – NetScaler ADMがユーザーに資格情報の入力を求めます

  3 – NetScaler ADMは、外部の認証、認可、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。

NetScaler® ADM で外部認証サーバーを構成する

LDAP、RADIUS、またはTACACSサーバーを構成した後、これらのサーバーをNetScaler ADMに追加できます。

LDAP認証サーバーを追加する

LDAPプロトコルをRADIUSおよびTACAS認証サーバーと統合すると、ADM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. **設定 > 認証** に移動します。
2. **LDAP** タブを選択し、**追加** をクリックします。
3. **LDAPサーバーの作成** 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

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

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. **セキュリティタイプ** – 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、Transport Layer Security (TLS) またはSSLのいずれかを選択して暗号化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も指定できます。

e. **サーバータイプ** – LDAPサーバーのタイプとして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® ADM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** – LDAP証明書の検証チェックボックスを選択し、証明書に入力するホスト名を指定します。

認証 オプションをクリアし、SSH公開鍵を指定します。鍵ベースの認証を使用すると、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鍵のリストを取得できるようになります。

- [ ]

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** – パスワードの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ている検索フィルターに従って、2要素認証用の外部ユーザーを構成します。たとえば、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)`。

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

注

デフォルトでは、検索フィルターの値は角かっこで囲まれています。

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、認証が成功したとき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。

注

ユーザーがActive Directoryグループのメンバーである場合、NetScaler ADM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、次のパラメーターを指定します。

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。デフォルトポートは1812です

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

d. **タイムアウト (秒)** – NetScaler® ADM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** – 確認のためにもう一度キーを指定します

詳細で、次のパラメーターを指定します。

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グループ抽出を使用するためのベンダー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

v. **グループ区切り文字** – RADIUSグループ抽出のために、RADIUS属性内で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サーバーへ送信される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

アプライアンスでRADIUSサーバーの監査情報をログに記録する場合は、 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。

© 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を有効にするを参照してください。

TACACS認証サーバーの追加

1. **Settings > Authentication** に移動します。
2. **TACACS** タブを選択し、**Add** をクリックします。
3. **Create TACACS** ページで、次のパラメータを指定します。
   a. **Name** – TACACSサーバー名を指定します
   b. **IP address** – TACACS IPアドレスを指定します
   c. **Port** – 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
   d. **Time-out (seconds)** – NetScaler® ADM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）
   e. **TACACS Key** – 認証用のTACACSキーを指定します
   f. **Confirm TACACS Key** – 確認のため、TACACSキーを再度指定します
   g. **Group Attribute Name** – グループ名を指定します

   アプライアンスでTACACSサーバーに監査情報をログ記録する場合は、**Accounting** を選択します。
4. **Create** 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。

NetScaler® ADMのユーザー

認証サーバー上のユーザーを補完するために、NetScaler ADMでローカルにユーザーアカウントを作成できます。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、認証サーバーにそれらのユーザーのエントリを作成することなく、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。

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

ユーザーの設定の詳細については、「ユーザーの設定」(/ja-jp/netscaler-application-delivery-management-software/13-1/access-control/role-based-access-control/rbac-configuring-groups.html)を参照してください。

注

ユーザーがActive Directory上にいる場合は、NetScaler ADMのグループ名が、外部サーバー上のActive Directoryグループのグループ名と同じであることを確認してください。

NetScaler ADMのユーザーグループ

NetScaler ADMでは、グループを作成し、そのグループにユーザーを追加することで、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付与でき、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 ADMでは、次のようになります。

- 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つまたは複数の役割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 ADMでローカルグループを作成し、その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 ADM上のグループを、内部ネットワーク内の認証サーバーで構成されているグループと一致するように設定します。ユーザーがログオンして認証されると、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 ADM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 ADMで構成されているグループに追加します。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」(/ja-jp/netscaler-application-delivery-management-software/13-1/access-control/role-based-access-control/rbac-configuring-groups.html)を参照してください。

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

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 ADM 13.0**からサポートされています。

NetScaler® ADM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する。
- 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る。

利点:

- ユーザーは外部サーバーで管理されるため、NetScaler ADMでユーザーを作成する必要はありません。
- NetScaler ADM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へのアクセスに対してグループ権限を割り当てることにより、ユーザーの認証を実行します。

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® ADM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 ADM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、次の手順を実行します。

- 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以外のユーザーはNetScaler ADM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 ADM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 ADM は、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。 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

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

合、NetScaler ADM 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 ADM 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任意の種類の外部認証サーバー (RADIUS、LDAP、TACACS) 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 ADMは、設定に基づいて外部サーバーで認証を試行します。この例のシナリオでは、NetScaler ADMは次のことを試行します。

- 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 ADMでは、最大32台の外部認証サーバーを設定できます。

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** に移動します。
2. 「**認証**」ページで、「**設定**」をクリックします。
3. 「**認証構成**」ページで、「**サーバータイプ**」リストから「**EXTERNAL**」を選択します（外部サーバーのみカスケードできます）。
4. 「**挿入**」をクリックし、「**外部サーバー**」ページで、カスケードする認証サーバーを1つまたは複数選択します。
5. 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、「**フォールバックローカル認証を有効にする**」チェックボックスをオンにします。
6. 外部ユーザーグループ情報をシステム監査ログに記録したい場合は、「**外部グループ情報をログに記録**」チェックボックスをオンにします。
7. ページを閉じるには、「**OK**」をクリックします。

   選択したサーバーは「外部サーバー」の下に表示されます。

   「外部サーバー」(/en-us/netscaler-application-delivery-management-software/media/external-servers-citrix.png)

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

サーバー名の横にあるアイコンを使用してサーバーをリスト内で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。

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

アクセス制御

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® Application Delivery Management (ADM) 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 ADM は RADIUS、LDAP、および TACACS プロトコルによる外部認証をサポートしています。ユーザーが外部認証用に構成された NetScaler ADM へのアクセスを試みると、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を行います。認証が完了すると、必要なプロトコルを使用して NetScaler ADM 上でユーザーを識別します。

アクセス制御とは、特定のリソースに必要なセキュリティを適用するプロセスです。これは、コンピューティング環境で誰がリソースを表示または使用できるかを規制するために使用できるセキュリティ技術です。アクセス制御の目的は、コンピューターシステムの正当なユーザーが実行できるアクションまたは操作を制限することです。アクセス制御は、ユーザーが直接できること、およびユーザーに代わって実行されるプログラムが許可されていることを制限します。このように、アクセス制御はセキュリティ侵害につながる可能性のある活動を防ぐことを目指します。アクセス制御は、参照モニターを介したアクセス制御の適用に先立ち、ユーザーの認証が正常に検証されていることを前提としています。NetScaler ADM は、管理者が企業内の個々のユーザーの役割に基づいてユーザーにアクセス許可を提供できる、きめ細かなロールベースのアクセス制御 (RBAC) を可能にします。NetScaler ADM における RBAC は、アクセスポリシー、ロール、グループ、およびユーザーを作成することによって実現されます。

ロールベースのアクセス制御

NetScaler® ADM 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ロールに基づいてアクセス権限を付与できます。このコンテキストでは、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機能です。ロールは、企業内のユーザーの権限と責任に従って定義されます。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することを許可される場合がありますが、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。

ロール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、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、ユーザーにロールを割り当てます。ユーザーのグループにロールを割り当てることもできます。

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

グループとは、共通の権限を持つユーザーの集まりです。たとえば、特定のデータセンターを管理しているユーザーはグループに割り当てることができます。ロールとは、特定の条件に基づいてユーザーまたはグループに付与されるIDです。NetScaler ADM では、ロールとポリシーの作成は NetScaler の RBAC 機能に固有のものです。ロールとポリシーは、企業のニーズの変化に応じて、各ユーザーの権限を個別に更新することなく、簡単に作成、変更、または廃止できます。

ロールは、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:

ADC グループの責任者であるクリスは、彼の組織における NetScaler ADM のスーパー管理者です。クリスは、セキュリティ管理者、アプリケーション管理者、ネットワーク管理者の3つの管理者ロールを作成します。

セキュリティ管理者であるデイビッドは、SSL 証明書の管理と監視に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スティーブは、特定のアプリケーションと特定の構成テンプレートのみに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グレッグは、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。

クリスはまた、ローカルユーザーか外部ユーザーかに関わらず、すべてのユーザーに RBAC を提供する必要があります。

NetScaler ADM 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係なく、すべてのユーザーに適用される必要があります。

次の図は、管理者およびその他のユーザーが持つ権限と、組織内での彼らのロールを示しています。

制限事項

RBACは、以下のNetScaler ADM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.

- **アナリティクス** - アナリティクスモジュールでは、RBAC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のアナリティクスモジュールでは、アプリケーションレベルでは適用されません。例:

例1: インスタンスベースのRBAC (サポート対象)

いくつかのインスタンスを割り当てられた管理者は、**Web Insight** \> **Instances**の下にあるそれらのインスタンスのみを表示でき、**Web Insight** \> **Applications**の下にある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)

いくつかのアプリケーションを割り当てられた管理者は、**Web Insight** \> **Applications**の下にある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はサポートされていないためです。

- **StyleBooks** – StyleBooksではRBACは完全にサポートされていません。
    - NetScaler ADMでは、StyleBooksと構成パックは別個のリソースとして扱われます。表示、編集、またはその両方のアクセス権限は、StyleBookと構成パックに対して個別に、または同時に付与できます。構成パックに対する表示または編集の権限は、構成パックの詳細を取得し、構成パックを作成するために不可欠なStyleBooksの表示をユーザーに暗黙的に許可します。
    - 特定のStyleBookまたは構成パックに対するアクセス権限はサポートされていません例: インスタンスに構成パックがすでに存在する場合、ユーザーはそのインスタンスへのアクセス権がなくても、ターゲットのNetScalerインスタンス上の構成を変更できます。
- **オーケストレーション** - オーケストレーションではRBAC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® Application Delivery Management (ADM) には、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 ADM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ち、すべてのNetScaler ADM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。

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

2. **readonlypolicy**。読み取り専用権限を付与します。ユーザーはNetScaler ADM上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 ADMのアプリケーション機能にアクセスするための管理権限を付与します。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、無効化の操作は実行できません。

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 ADM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 ADM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 ADM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 ADMで有効化または無効化のアクションを許可する**ネットワーク機能**の機能でのみ利用できます。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。

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

- **編集:** このオプションは、ユーザーにフルアクセスを付与します。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、より多くの構成オプションを表示します。

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。

ロール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-citrix.png)

表示権限は、**仮想サーバー**機能に対してユーザーに付与されます。ユーザーはNetScaler ADM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。

有効化/無効化権限は、**サービス**機能に対してユーザーに付与されます。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**アクションを実行することもできます。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、次のページではサービスに対する有効化または無効化のアクションが制限されます。

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。 このページでは、「**Enable**」または「**Disable**」を選択すると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。この権限により、「**View**」および「**Enable-Disable**」権限が付与されている完全なアクセスが許可されます。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

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

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。

注:

他のStyleBook権限を付与すると、View権限が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 ADM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、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ときに、グループにロールを割り当てたり、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たり、グループにユーザーを割り当てたりできます。そのグループ内のすべてのユーザーには、NetScaler® ADMで同じアクセス権が割り当てられます。

NetScaler ADM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 ADM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)** - 負荷分散 (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** - 負荷分散およびGSLBサービス
- **サービスグループ** - 負荷分散およびGSLBサービスグループ
- **サーバー** - 負荷分散サーバー

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

ユーザーグループを作成する

1. NetScaler ADMで、**設定 > ユーザーとロール > グループ** に移動します。
2. **追加** をクリックします。

   システムグループの作成 ページが表示されます。
3. **グループ名** フィールドに、グループの名前を入力します。
4. **グループの説明** 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. 「**役割**」セクションで、1つ以上の役割を「**構成済み**」リストに追加または移動します。

   注:

   「**利用可能**」リストで、「**新規**」または「**編集**」をクリックして役割を作成または変更できます。または、「**設定 > ユーザーと役割 > 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。

   システムグループの作成(/en-us/netscaler-application-delivery-management-software/media/external-server-group-extraction-2-citrix.jpg)
6. 「**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。

   - 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
   - コンフィグパック
   - 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-citrix.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することもできます。

   Autoscale グループ:

   ユーザーが表示または管理できる特定のAutoscaleグループを選択する場合は、次の手順を実行します。

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

a. **すべてのAutoscaleグループ**チェックボックスをオフにし、**Autoscaleグループの追加**をクリックします。

b. リストから必要なAutoscale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)

アプリケーション:

アプリケーションの選択リストでは、必要なアプリケーションへのユーザーアクセスを許可できます。

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。アプリケーションは、ユーザーアクセスを許可するためにインスタンスとは独立しているためです。

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、そのユーザーはそのアプリケーションのみにアクセスする権限が与えられます。

このリストには、次のオプションがあります。

- **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 ADMに存在するすべてのアプリケーションが追加されます。
- **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が追加されます。
- **特定のアプリケーション:** このオプションを使用すると、ユーザーがアクセスしたい必要なアプリケーションを追加できます。 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を選択:** 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。

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

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て を選択すると、NetScaler ADM 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。

注:

バインドされたエンティティを承認する場合は、1つのエンティティタイプのみを選択していることを確認してください。

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 ADM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. 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。

次の図は、 オプションを選択した場合に、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。

次の図は、 オプションを選択した場合に、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にのみ一致し、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。

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

承認スコープを更新するために、正規表現は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 ADM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したい場合は、次の手順を実行します。

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を選択したい場合は、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、StyleBookを承認するためのフィルタークエリを指定できます。

   個々のStyleBookを選択したい場合は、**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を検索したい場合は、**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。

   値として正規表現を使用して、グループの正規表現条件を満たすStyleBookを検索して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。

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

- 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。これは、名前が`lb-mon`または`lb`であるStyleBookを返します。
- `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。

カスタムフィルター(/en-us/netscaler-application-delivery-management-software/media/custom-filter-query.gif)

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、ADM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。

コンフィグパック:

Configpacksで、次のいずれかのオプションを選択します。

- **All Configrations**: このオプションはデフォルトで選択されています。ADMにあるすべての構成パックを追加します。
- **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、必要な構成パックを追加できます。

  グループを作成し、そのグループにユーザーを追加するときに、必要な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。

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

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。

7. **グループの作成**をクリックします。
8. **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。

   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。

   システムグループを作成する例(/en-us/netscaler-application-delivery-management-software/media/assigning-users-citrix.png)
9. **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 ADM 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。

開始する前に、グループを作成してください。詳細については、「NetScaler ADM 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、ホスト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 ADM 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「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、「アプリケーションの選択」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クリアされていることを確認します。そうしないと、NetScaler ADM 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、エンティティタイプごとに正規表現 (regex) を指定できます。正規表現は、ユーザーの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 ADM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許可できます。

ユーザー権限を動的に付与するには、スーパー管理者は**承認設定**タブで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はアプリケーションエンティティタイプに対して`App*`を正規表現として追加し、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*`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、彼のアクセスはアプリケーションのみに限定され、ホストされているサーバーにはアクセスできません。

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、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、ADM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。

ポリシー1とポリシー2の2つのポリシーを持つグループに割り当てられたユーザーを考えます。

- **ポリシー1** – アプリケーションへの表示のみの権限。
- **ポリシー2** – アプリケーションへの表示および編集権限。

ユーザーはポリシー1で指定されたアプリケーションを表示できます。また、このユーザーはポリシー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。グループ1のアプリケーションへの編集アクセスは、グループ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 ADMを12.0からそれ以降のリリースにアップグレードする場合のRBACのマッピング

NetScaler ADMを12.0から13.1にアップグレードすると、グループの作成時に「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、これにより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	偽	`admin`
管理者 読み書き	真	`appAdmin`
管理者 読み取り専用	偽	`readonly`
管理者 読み取り専用	真	`appReadonly`

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

役割を構成する

NetScaler® Application Delivery Management (ADM) では、各役割は1つ以上のアクセスポリシーにバインドされます。ポリシーと役割の間で、1対1、1対多、多対多の関係を定義できます。1つの役割を複数のポリシーにバインドすることも、複数の役割を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、ある役割が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 ADM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機能の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 ADMには、次の4つの事前定義された役割があります。

- **admin**。すべてのNetScaler ADM機能にアクセスできます。(この役割は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。(この役割はreadonlypolicyにバインドされています。)
- **appAdmin**。NetScaler ADMのアプリケーション機能のみに管理者アクセス権があります。(この役割は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。(この役割はappReadOnlyPolicyにバインドされています。)

注：

事前定義された役割は編集できません。

独自の（ユーザー定義の）役割を作成することもできます。

役割を作成し、ポリシーを割り当てるには：

1. NetScaler ADMで、**Settings > Users & Roles**に移動します。
2. **Add**をクリックします。
3. 「**ロール名**」フィールドにロールの名前を入力し、「**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）。

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

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-citrix.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® Application Delivery Management (ADM) には次の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 ADM 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 ADM 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。1人のユーザーを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 ADM でユーザーを構成するには:

1. NetScaler ADM で、 **>** に移動します。
2. 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 ADM にログオンするためのパスワード

4. オプションで、 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ます。
5. グループを作成しており、ユーザーをグループに割り当てたい場合は、 セクションで、1つ以上のグループを リストから リストに移動します。

   システムユーザーの作成(/en-us/netscaler-application-delivery-management-software/media/create-system-user-citrix.png)

6. をクリックします。

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

推奨事項を表示し、ADCとアプリケーションを効率的に管理する

数百もの検出されたNetScalerインスタンスがあり、各ADC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）を構成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、即座に注意が必要なインスタンスやアプリにも焦点を当てる必要があるかもしれません。NetScaler® ADMのタスク機能は、サブスクリプションと現在の利用状況に基づいて、以下の推奨事項を提供します。

- 管理者が、実用的な「ガイドミー」ワークフローを使用して、NetScaler ADMがどのように効率的な展開を提供できるかを知るのに役立ちます。
- タスクを完了するか、後で完了するために承認することで、管理者の重要な時間と労力を削減します。
- 管理者がNetScaler ADMのすべての機能を活用し、製品が推奨する製品検出と機能を有効にして、展開を効率的に管理できるようにします。

「**セットアップタスク**」ページでは、次のタブを表示できます。

- **To Do** – 推奨事項のリストを表示できます。確認して**ガイドミー**をクリックしてタスクを完了するか、**承認**をクリックしてこのタスクをスキップできます。
- **アーカイブ** – 完了または承認されたすべてのタスクのリストを表示できます。また、「ガイドミー」オプションを使用して、繰り返し発生する要件を完了することもできます。

次の表は、NetScaler ADM GUIで表示できるタスクまたは推奨事項について説明しています。

推奨事項名	タスクはいつGUIに表示されますか？
ADCを追加する	NetScaler ADMにオンボーディングした後、ADCインスタンスが検出されない場合。
アプリケーション分析は非常に重要です！ライセンスされた仮想サーバーで有効にし、ア	複数のライセンスされた仮想サーバーがあるが、分析が有効になっていない場合。

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

推奨事項名	タスクはいつGUIに表示されますか？
プリケーションの問題をより迅速にトリアージします	
ADCの帯域幅を再割り当てしたいですか？簡単です！	プールされたライセンスがADC GUIで割り当てられており、それらのADCインスタンスがNetScaler ADMで検出されている場合、NetScaler ADMを使用して再割り当てを行うことができます。
仮想IPエンタイトルメントからより多くの価値を引き出しましょう！残りの検出された仮想サーバーで、より多くの仮想IPライセンスを有効にしてください	必要なライセンスを持っているが、すべての仮想サーバーにライセンスが適用されていない場合。
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のアクセスを有効にする	NetScaler ADMでロールベースのアクセス制御 (RBAC) がまだ構成されていない場合。
ルールを構成し、ADCインスタンスで重要なイベントを見逃さないようにします	カスタムイベントルールがまだ構成されていない場合。
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構成されていない場合。
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証明書について警告または通知が構成されていない場合
セキュリティアドバイザリ - CVEと緩和策でADCを最新の状態に保つ	ADC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ADCに適用します	**Config Job**タスクがまだ構成されていない場合。
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	タスクはいつGUIに表示されますか？
選択した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	アプリケーションダッシュボードの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。
時間を節約！StyleBooksでアプリケーションの展開と管理を簡素化します	デフォルトのStyleBookがまだ構成されていない場合。
AppSec違反をリアルタイムでSplunkにサブスクライブしてエクスポートします	NetScaler ADM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、単一または二重のしきい値がサービスに適用されていない場合。
通知プロファイルを事前に設定し、通信先に通知を受け取ります。	通知プロファイルがまだ設定されていない場合。
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設定されていない場合。
ServiceNowをお持ちで、ADMとの統合を検討していますか？	NetScaler ADMでServiceNow統合がまだ設定されていない場合。

デフォルトでは、上位5つの推奨事項を表示できます。すべての推奨事項を表示するには、**Show All** をクリックします。カテゴリリストを使用してカテゴリを選択し、選択に基づいて特定の推奨事項をフィルタリングできます。

カテゴリを選択してください。(/en-us/netscaler-application-delivery-management-software/media/set-up-task-categories.png)

または、検索バーを使用して最初の数文字を入力し、タスクを絞り込むこともできます。

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

ガイドミーワークフローを使用してタスクを完了する方法?

すべてのライセンスされた仮想サーバーで分析を有効にしたいとします。次のタスクで **Guide me** をクリックします。

ユースケース(/en-us/netscaler-application-delivery-management-software/media/set-up-task-use-case.png)

ワークフローは、タスクを完了するために必要な提案を提供します。この例では、**Guide me** をクリックした後、提供されるツールチップの提案に従ってください。

1. ☐
2. ☐
3. ☐

分析タイプを選択し、**Save Analytics**をクリックすると、タスクは完了します。このタスクは**Archived**タブに移動されます。

同様に、**Archive**タブで繰り返し発生する要件に対しても、同じワークフローを使用できます。

Popular Featuresでは、NetScaler ADMの重要な機能を確認でき、機能をクリックすることでこれらの機能を探索できます。

よくある質問

1. **Guide me**がツールチップを表示せず、UIのリダイレクトのみを行いますか？これを修正するにはどうすればよいですか？

   この問題は、ファイアウォールがPendo FQDNをブロックしている場合に発生する可能性があります。Enable Pendo for your enterpriseを参照し、ファイアウォールでFQDNが許可されていることを確認してください。Pendo FQDNを許可すると、**Guide me**がツールチップを表示できるようになります。Pendoが利用可能な場合にのみ、**Guide me**ワークフローを最大限に活用できます。

2. 管理者にはどのような種類のタスクが提示されますか？

   現在、推奨事項は、展開を効率化するための構成やセットアップタスクに関して管理者をより支援する展開に特化しています。また、製品の発見を促進し、管理者は、事前の知識がなくても、またはADMにその機能が存在するかどうかを知らなくても、タスクが何を行い、どのように役立つかを知ることができます。

3. **Archive**から**To Do**にタスクを戻すことはできますか？

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

アーカイブ内のタスクは、特定の条件に基づいてのみ**To Do**に戻ります。例えば、イベントルールがすべて削除された場合や、すべてのADCが削除された場合、アーカイブされたタスクは管理者の注意を引くために、再びTo-Doタスクに移動します。

4. 承認した場合、進捗バーは完了しますか？

   はい！ただし、これらのタスクを完了することをお勧めします。しかし、後で実行したい場合は、製品の推奨事項を認識していることを承認し、後で完了するためにアーカイブに戻ることができます。

5. ガイドミーを開始して途中で中断した場合、タスクはアーカイブに移動しますか？

   いいえ、アクションが保存または完了されない限り、タスクは引き続きTo Doで利用可能です。

6. 検索またはフィルタリングを実行できますか？

   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。

7. ADCメモリの急増、アプリのダウン、LB仮想サーバーのダウンなどの動的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？

   これらはすべて機能強化の一部であり、今後のリリースで利用可能になる予定です。

8. これはオンプレミスADMで利用可能になりますか？

   この機能は現在、ADMサービスでのみ利用可能です。

9. NetScaler ADMにADCが追加されていない場合でも、私の20以上のタスクがすべて表示されますか？

   いいえ。これらすべてのタスクを表示するには、NetScaler ADMでADC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。

10. タスクはどれくらいの頻度で更新されますか？

    ```
    When you click **Tasks** from the left navigation pane, they are
    refreshed and available at the latest status. The details for each task
    are fetched and updated. The tasks are automatically refreshed every 24
    hours. For better administrative control, you can also do a manual
    refresh of tasks to get the latest status.
    ```

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

アプリケーション

NetScaler® ADM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 ADMにNetScalerインスタンスを追加していることを確認してください。
- 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。
- 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てください。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

アプリケーションは次のいずれかです。

- 個別アプリケーション
- 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)

個別アプリケーション

ライセンスが付与されているすべての仮想サーバーは、個別アプリケーションと呼ばれます。

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

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ADC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、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。

注意事項

- カスタムアプリケーションに追加された個別アプリケーションは、個別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 ADMでは最大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個別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® ADM 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。

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。

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

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、関連する仮想サーバー、関連する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

- 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、ADM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、:

  - 過去1日、1週間、1ヶ月の期間を選択した場合、Jan 4, 2020にダッシュボードには削除されたアプリケーションが引き続き表示されます。
  - 過去1週間および1ヶ月の期間を選択した場合、Jan 5, 2020にダッシュボードには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。

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

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：

-ADC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。
-ADC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

アプリの詳細(/en-us/netscaler-application-delivery-management-software/media/manage-applications-citrix.png)

- **アプリケーション名** – 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または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。
  - **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総数と、すべての仮想サーバーの現在の状態を示します。マウスカーソルを合わせると、仮想サーバーの総数、仮想サーバーのタイプ、仮想サーバーの状態などの詳細が表示されます。

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

仮想サーバーの状態(/en-us/netscaler-application-delivery-management-software/media/virtual-server-status.png)

- **Services/state** – 設定されているサービス総数とすべてのサービスの現在のステータスを示します
- **Service Goups/state** – 設定されているサービスグループ総数とすべてのサービスグループのステータスを示します
- **Servers/state** – アプリケーション用に設定されているサーバー総数とすべてのサーバーの現在のステータスを示します
- **Actions** – 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. 新しいアプリケーションを作成するには、**New Application** をクリックします

   Define Application ページが表示されます

   注:

   Applications をクリックし、その後、**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。
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。「アプリケーションカテゴリ」ページを表示するにはクリックします。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。

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

フィールド	説明
	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。たとえば、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。たとえば、10.102.29.20、10.102.43.10-60、10.216.43.45と入力できます。
StyleBookから新しい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。

3. 「**OK**」をクリックします。

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

注:

現在、アプリケーションダッシュボードは負荷分散と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表示され、カテゴリとともに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® ADM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**と**アドレス指定できない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 ADM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 ADMでは、ユーザー定義の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。

   StyleBookの選択ページが表示されます。このページには、NetScaler ADM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ーの値を入力します。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。

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

選択したNetScalerインスタンスでNetScaler ADM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。

アプリケーション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 ADMでは、現在のアプリケーション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。頻繁に、アプリケーション管理者はこれらのレポートを使用して、アプリケーション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 ADMの他のレポートエクスポートオプションとは異なり、アプリケーション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。アプリケーションダッシュボードおよびアプリケーションセキュリティダッシュボードページから、セカンドレベル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。

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。

ダッシュボードには、次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.

- **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、**重大、良好、普通、該当なし**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、**稼働中、停止中、部分的に稼働中、サービス停止中、NA**などのように示します
  - **稼働中** – 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稼働中です。
  - **停止中** – 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停止中です。
  - **部分的に稼働中** – 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停止中か、サービス停止中です。
  - **サービス停止中** – 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エラーカウントが最大の問題を示します
- **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。

- **総リクエスト数** – アプリケーションが受信した総リクエスト数を示します
- **スループット** – アプリケーションの総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総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

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

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** という名前の支払い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、**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** 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。
  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、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。

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

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。

- 次に、**PaymentApp**を使用し、**ComABC**および**ComCDE**に関連付けることができます。

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. **ComABC**アプリを見つけて、**編集**をクリックします。

c. **参照されるアプリケーション**の下で、**カスタムアプリケーションの追加**をクリックし、**PaymentApp**を選択します。

d. **PaymentApp**が**参照されるアプリケーション**の下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。

1 – 1時間、1日、1週間、1ヶ月など、選択した期間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。

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

5 – アプリケーションを表示するための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。

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仮想サーバーが設定されていません

    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、**100 - 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**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)**、および **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
- 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
- その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。

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

注記

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。

すべてクリアをクリックして、適用されたフィルターをクリアします。

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総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総ネットワークスループット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総データ量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レスポンス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数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数を表示するヒストグラム
- **送信パケット** – アプリケーションによって送信された総パケット数を表示するヒストグラム
- **受信パケット** – アプリケーションによって受信された総パケット数を表示するヒストグラム
- **仮想サーバーの健全性** – スコア範囲0%から100%の間のアプリケーションの総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た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。

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

アプリケーションの詳細

ダッシュボードからアプリケーションをクリックして、さらに詳細な情報をドリルダウンします。

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、**Service Graph**をクリックします。詳細については、Service Graph for Applications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、**Transaction Logs**をクリックします。
- 詳細な監査ログ情報を表示するには、**Audit logs**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、**Configure**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、**Service**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。

- **App Score** – 選択した期間のアプリケーションスコア。最終スコアは**100 minus total penalty**として計算されます。

  このダッシュボードでは、アプリの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。

- **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は、**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。

  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

  詳細の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。

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

- **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

  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

- **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	設定	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	不適切な永続化タイプ
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
低いセッション再利用率		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、および詳細などの詳細を確認します。

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ページの以前の表示です。

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**問題**セクションで閲覧できるようになりました。

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

- **現在の**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。
- **すべて**の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。**現在の**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。

すべてのタブには、1日間の期間で検出された合計問題が表示されます。

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、App Score の計算に使用するコンポーネントを選択し、しきい値を設定できます。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
- アプリケーションが応答性の面で良好に動作しているか

Applications > Dashboard に移動し、設定アイコンを選択します。

App Score の構成ページで、最終的な App Score を決定するためのコンポーネントを選択し、しきい値を設定できます。

App Score コンポーネントの図(/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	ユーザーが設定したしきい値	説明
ADC メモリ使用量	はい	NetScaler インスタンスにおける合計メモリ使用量の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、応答を必要とするサージリクエストの合計に対する低および高しきい値。
ADC CPU使用率	はい	NetScalerインスタンスにおける総CPU使用率に対する低および高しきい値。

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

APP SCORE コンポーネント	ユーザーが設定したしきい値	説明
応答時間	はい	リクエストパケットの送信から、仮想サーバーで構成されたサービスからの最初の応答パケットの受信までの時間間隔。
アプリCPU使用率	はい	アプリケーションによる総CPU使用率に対する低および高しきい値。
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	なし	仮想サーバーでの永続性使用率が低いかどうかを示します。
サーバーエラー (5xx)	なし	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	なし	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え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	なし	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、遅延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	なし	一定期間にわたるセッションの蓄積を示します。これにより、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可能性があります。

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

APP SCORE コンポーネント	ユーザーが設定したしきい値	説明
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総数を示します。
TCP再構成キュー制限ヒット	いいえ	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® ADM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、**設定 > 分析設定**に移動し、**アプリスコアの設定**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して、さらに詳細な情報をドリルダウンします。

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：

- 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
- **サービスグラフ**をクリックして、選択したアプリケーションのサービスグラフを表示します。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。
- **トランザクションログ**をクリックして、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します
- **監査ログ**をクリックして、詳細な監査ログ情報を表示します

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

期間を選択すると、以下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、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から合計ペナルティを引いた値**として計算されます。

  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ネームスペース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する問題を示します

  このダッシュボードでは、アプリスコアに影響し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** – サービス名
  - **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
  - **名前空間** – サービスに割り当てられた名前空間
  - **サービスラベル** – サービスに割り当てられたサービスラベル

- **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に割り当てられた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

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

- **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、サーバー接続、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値**として計算されます。

  選択した期間の次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、選択した期間は1か月です。202.66 MBという値は1か月の期間の合計データ量で、8.13 MBという値は差分値です。グラフでは、最初の値は14.11で、最後の値は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。次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	設定	システムリソース
応答時間	平均CPU使用率	高い5xx応答	不適切な永続化タイプ
セッション再利用率の低さ	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再構成キューの制限ヒット	
SSLリアルタイムトラフィック			

  各問題をクリックして、次の情報を表示します。

  - 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)

    - **現在の**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。
    - **すべての**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。

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

次の例は、1日間のアプリケーションの問題です。**現在の**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日間の期間に検出された合計問題が表示されます。

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® ADM 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を監視およびトラブルシューティングするための、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すべてのレベルを監視し、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改善します。

一般的な展開では、数千台のサーバーがユーザーのデータニーズに対応しています。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。

- 停止時やその他のイベント時に監視、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、アプリケーションが最適なパフォーマンスを達成するために必要に応じて構成を変更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は、**Applications** > **Dashboard** に移動し、アプリケーションを選択して、下にスクロールして **Issues** セクションで問題を表示することで確認できます。

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

インテリジェントアプリ分析を構成する

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 ADM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。デフォルトでは、インスタンスをNetScaler ADMに追加する際に、NetScalerで**Metrics Collector**が有効になっています。

Metrics Collector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 > NetScaler**に移動し、監視するインスタンスの種類（例: NetScaler VPX）を選択します。
2. NetScalerインスタンスを選択します。
3. **アクションの選択**リストから、**Metrics Collector**を選択します。

4. **Metrics Collector設定の構成**ページで、**有効にする**オプションがデフォルトで選択されています。このオプションが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。

注

サーバーエラーとその**詳細なWebトランザクション**の異常を表示するには、仮想サーバーで分析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、ADCインスタンスで分析とメトリックコレクターを有効にする必要があります。

分析とメトリック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
- アクティブなサービス
- 平均CPU使用率
- メモリ使用量

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

- NICカード飽和
- サービスフラップ
- セッション再利用率の低下
- 不適切な永続性タイプ
- 不安定なサーバー (5xx)
- SSLリアルタイムトラフィック
- 異常に大きいHTTPパケット
- TCP再構成キュー制限ヒット
- サージキューの蓄積

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。**レスポンスタイム**タブをクリックして、問題の詳細を表示します。

レスポンスタイム(/en-us/netscaler-application-delivery-management-software/media/pi-response-time.png)

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
- 低、中、高などの問題の重大度
- 合計トランザクション応答時間が設定されたしきい値を超えていること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よりも小さい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。

アクティブサービス(/en-us/netscaler-application-delivery-management-software/media/pi-active-services.png)

で、以下を表示できます。

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

- 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
- 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

平均CPU使用率

この問題は、このアプリケーションのADC 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。

詳細の下で、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
- 低、中、高などの問題の重大度
- ADC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ADC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。**メモリ使用量**タブをクリックして、問題の詳細を表示します。

詳細では、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
- ADC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

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

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すると、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DOWNステータスになっているサービスを把握する
- 特定の期間にUPまたはDOWN状態になっているサービスの数を把握する

サービスフラップの詳細を表示するには、**サービスフラップ**タブをクリックします。

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：

- **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があります。

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

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。

不安定なサーバー(/en-us/netscaler-application-delivery-management-software/media/unstable-server.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。

- 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、中などの異常の深刻度
- 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トランザクションに関する詳細については、サーバーエラーのWebトランザクション分析を参照してください。

セッションの蓄積

すべての保護されたトランザクションに対して、NetScalerは最初のトランザクションでSSLオフロードプロセスを実行し、**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基づいて、セッションの蓄積が一定期間にわたって発生する可能性があり、これにより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警告し、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。

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

詳細の下で、以下を表示できます。

- セッション蓄積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。

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。

セッション再利用率の低下

NetScalerインスタンスは、サーバーからの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。**セッション再利用率の低下**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、**セッション再利用率の低下**タブをクリックします。

セッション再利用率の低下(/en-us/netscaler-application-delivery-management-software/media/iaa-low-session.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、セッション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。

- セッション再利用率が低いアプリケーションの総数
- セッション再利用率の低下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

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

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ることになります。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発生してい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)

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刻
- 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。

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

- トラフィックを確認して、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追加します。

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
- 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

不適切な永続性タイプ

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）、仮想サーバーで永続性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は同じクライアントから同じサーバーに転送します。

永続性は、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に効果的です。永続性セッションの再利用率が低い場合、ADC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。

不適切な永続性タイプインジケーターを使用して、仮想サーバーでの永続性の使用率が低いかどうかを判断できます。**不適切な永続性タイプ**タブをクリックして、問題の詳細を表示します。

不適切な永続性タイプ(/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、永続性タイプを確認するか、永続性を無効にすることです。詳細については、「永続性設定」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
- 未使用セッションの割合を示す検出メッセージ

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

TCP再構成キュー制限ヒット

TCPは、TCP通信における順序不同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。キューサイズが長い場合、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、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。

TCP再構成キュー制限ヒットインジケーターを使用すると、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過しているかどうかを確認できます。

TCP再構成キュー制限ヒットタブをクリックして、問題の詳細を表示します。

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。

- 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追加します。
- この動作が予期されるネットワーク動作である場合は、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、それ以上の措置は不要です。

詳細の下で、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トラフィックを処理するために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、レイテンシー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。

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

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ー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。

- 異常が発生した時刻
- 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設定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、数分以内（約10〜15分）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の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、記載された期間（10〜15分）が経過した後でも、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（**適用不可**ステータス）で表示されている。

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

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

アプリケーションがライセンスされている

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。**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ます。アプリケーションがライセンスされていない場合は、以下を参照してください。

- **ADMサービス** - 仮想サーバーでのライセンス管理と分析の有効化。
- **ADMオンプレミス** – 仮想サーバーでのライセンス管理と分析の有効化。

メトリックコレクターが有効になっている

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。

NetScalerバージョン13.0以降では、ADCインスタンスがADMに正常に追加されると、メトリクスコレクターはデフォルトで有効になります。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

ネットスケーラーで：

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。

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

`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® ADM 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。

   b. インスタンスを選択し、**Start Polling** をクリックします。

   ポーリングが失敗した場合は、ADM から ADC インスタンスを削除し、再度 ADC インスタンスを追加します。ADC インスタンスを追加すると、コレクターが ADC に追加されます。

コレクターが**ダウン**状態を示している場合:

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. ADC インスタンスが ADM 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。

NetScaler インスタンスの後のビルド

NetScaler ADM で、メトリクス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 > ロードバランシング > サービス** に移動します。
2. 検索バーで、**Instance: (IP address)** と **Name: ADM** 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、ADM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、コレクターサービスがNetScalerの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。

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

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
   ```

コレクターが**Down**ステータスを示している場合：

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. ADCインスタンスがADM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)
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てください。

   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。ファイアウォールによるブロックの問題を解決する必要があります。

NetScalerで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、コレクターは空白として表示されます。

コレクターサービスなし(/en-us/netscaler-application-delivery-management-software/media/no-collector.png)

NetScaler ADM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(/en-us/netscaler-application-delivery-management-software/media/polling.png)

   ポーリングが失敗した場合、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
   ```

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

```
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。

「コレクターサービスを更新」(/en-us/netscaler-application-delivery-management-software/media/update-adc.png)

上記で述べたトラブルシューティング手順をすべて実行しても問題が解決しない場合は、**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なメトリックは、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偏差が発生する可能性があります。こ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場合があります。

NetScaler® ADM はこのような異常を検出し、必要な詳細情報を提供します。**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 ADM 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 ADM 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)

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。以下の例は、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。

- 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**
- **詳細**の下にある時間と異常の詳細

© 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。

改良された**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**タブに次の情報が表示されます。

- 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と使用状況のメトリックを関連付ける。

注

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の最大遅延。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、**Client Network Latency**は644ミリ秒と表示されます。
- 選択した期間にわたって、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。

Usageタブから表示できるWeb Insightメトリックは次のとおりです。

- **Clients** – アプリケーションにアクセスしているクライアントに関するインサイトを表示します。
  - **Total Clients** – 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。
  - **Client Network Latency** – クライアントからNetScalerまでのネットワーク遅延を表示します。**Client Network Latency**タブをクリックして、以下を表示します。
    - **Client** – クライアントのIPアドレス。

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

- **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です。
- **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です。
- **リクエスト** – クライアントからの合計リクエスト数です。

◦ **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** – クライアントのIPアドレスです。
- **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です。
- **リクエスト** – クライアントからの合計リクエスト数です。

• **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。

> **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。

- **合計サーバー数** – アプリケーションにアクセスしている合計サーバー数を表示します。
- **サーバーネットワーク遅延** – サーバーからNetScalerへの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アドレスです。
  - **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です。
  - **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。
- **サーバー応答時間** – 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。**サーバー応答時間**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。
  - **サーバー応答時間 (平均)** – サーバーからの平均応答時間。
  - **サーバー応答時間 (最大)** – サーバーからの最大応答時間。
  - **リクエスト** – サーバーからの合計リクエスト。

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

- **帯域幅** – サーバーによって消費された合計帯域幅を表示します。**帯域幅**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。
  - **帯域幅** – サーバーから消費された合計帯域幅。
  - **リクエスト** – サーバーからの合計リクエスト。

- **地理的位置** – 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。

  - **合計ロケーション** – 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。
  - **応答時間** – クライアントの場所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。

- **URL** – 負荷とレンダリング時間が高い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。
  - 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。
  - **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。

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

    - **Render Time (avg)** – URLのレンダリングにかかった平均時間。
    - **Requests** – URLからのリクエストの合計。

- **HTTP Response Status** – 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。

    - **Response Status** – 2xx、4xx、5xxなどの応答コードを表示します。
    - **Response Status Reason** – 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。
    - **No of Occurrences** – 発生総数を表示します。

- **Operating system** – アプリケーションにアクセスしているOSに関するインサイトを表示します。

    - **Requests** – 各オペレーティングシステムからのリクエストの合計を表示します。
    - **Bandwidth** – 各オペレーティングシステムが消費した合計帯域幅を表示します。
    - **Load Time** – 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。

- **Browsers** – 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の種類に関する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エラーに関する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SSLエラーの合計数を表示します。「**フロントエンド**」タブをクリックすると、SSLエラーの種類と合計発生回数を表示できます。

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

- **バックエンド** – バックエンドサーバーからのSSLエラーの合計数を表示します。「**バックエンド**」タブをクリックすると、SSLエラーの種類と合計発生回数を表示できます。

- **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** – SSL証明書の合計数を表示します。「**証明書**」タブをクリックすると、証明書名と合計ヒット数を表示できます。
  - **プロトコル** – SSLプロトコルの合計数を表示します。「**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を表示できます。
  - **暗号** – 暗号の合計数を表示します。「**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を表示できます。
  - **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を表示できます。

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。

グラフィカル形式(/en-us/netscaler-application-delivery-management-software/media/web-insight-1.gif)

「**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表示できる詳細は次のとおりです。

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る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

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

インサイト名	メトリック	説明
	リクエスト	クライアントからの合計リクエストを示します
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	場所	クライアントの場所を示します
	応答時間	クライアントの場所からの合計応答時間を示します
	帯域幅	場所から消費された合計帯域幅を示します
	リクエスト	場所からの合計リクエスト数を示します
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

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

インサイト名	メトリック	説明
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	レスポンス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
ブラウザ	ブラウザ	ブラウザ名（Mozilla Firefox、Chromeなど）を示します。
	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示します。
	帯域幅	ブラウザが消費した合計帯域幅を示します。

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

インサイト名	メトリック	説明
	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	エラー名（CLIENTAUTH FAILUREなど）を示します。
	発生回数	SSLエラーの合計発生回数を示します。
SSL使用状況	プロトコル名とバージョン（TLS、SSLなど）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」を参照してください。

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

Web Insight ダッシュボード

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）をクリックすると、次のメトリックが表示されます。

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
		ブラウザ

各メトリックで、上位5つの結果を表示できます。クリックするとさらにドリルダウンして、問題を分析し、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。

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

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 ADMはRTT値を次のように表示します。

- **NA** – ADC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** – ADC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ミリ秒です。

たとえば、1か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：

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。

   選択したサーバーのメトリック詳細が表示されます。
2. 「**サーバーネットワーク遅延**」タブを選択して、遅延を分析します。

   サーバーネットワーク遅延(/en-us/netscaler-application-delivery-management-software/media/app-wi-serverlatency.png)

   平均遅延は10.01秒を示しており、グラフから過去1ヶ月間のサーバーネットワーク遅延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往復を必要とせずに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、「**サーバー**」の下に表示され、ADC仮想サーバーのIPアドレスの横にIC通知が表示されます。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、「**サーバーメトリクス**」に統合キャッシュヒットとミスのタブが表示されます。

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

グラフビュー：

- 「**統合キャッシュヒット**」タブでは、NetScalerアプライアンスがキャッシュから提供する応答の合計数を表示できます。

  統合キャッシュヒット(/en-us/netscaler-application-delivery-management-software/media/web-insight-server-integrated-cache.png)
- 「**統合キャッシュミス**」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応答の合計数を表示できます。

  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」を参照してください。

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

サービスグラフ

NetScaler® ADM 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に監視できます。この機能を使用すると、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で表示できます。

- 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(#service-graph-for-applications-across-all-citrix-adc-instances)
- Kubernetesアプリケーション(#service-graph-for-kubernetes-applications)
- 3層Webアプリケーション(#service-graph-for-3-tier-web-applications)

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。この単一ペインのサービスグラフビューから、管理者として以下を実行できます。

- 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把握する
- 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どこで発生しているかを把握する
- 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

Applications > Service Graph に移動し、**Global** 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、および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」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以下を表示します。

- エンドツーエンドのアプリケーション全体的な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
- パフォーマンスの問題に寄与する要因を確認する
- 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 ADM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、「Setting up service graph」を参照してください。

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。

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

- 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）の詳細

  GSLBアプリケーションの場合、データセンター、ADC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 ADM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 (red)** - 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 の場合を示します
  - **良好 (緑)** - エラーがなく、平均サービス応答時間 < 200 ms の場合を示します
- **重大**、**レビュー**、**良好**などのクライアントステータス。NetScaler ADM は、クライアントネットワークの遅延とエラー数に基づいてクライアントステータスを表示します。
  - **重大 (赤)** - 平均クライアントネットワーク遅延 > 200 ms かつエラー数 > 0 の場合を示します
  - **レビュー (オレンジ)** - 平均クライアントネットワーク遅延 > 200 ms またはエラー数 > 0 の場合を示します
  - **良好 (緑)** - エラーがなく、平均クライアントネットワーク遅延 < 200 ms の場合を示します
- **重大**、**レビュー**、**良好**などの仮想サーバステータス。NetScaler ADM は、アプリスコアに基づいて仮想サーバステータスを表示します。
  - **重大 (赤)** - アプリスコア < 40 の場合を示します
  - **レビュー (オレンジ)** - アプリスコアが 40 から 75 の間の場合を示します
  - **良好 (緑)** - アプリスコア > 75 の場合を示します

注意点:

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

- 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、負荷分散、コンテンツスイッチング、GSLB 仮想サーバ、サービスなどの構成データに基づいてのみ、サービスグラフの詳細を表示できます。
- アプリケーション構成に変更が加えられた場合、サービスグラフに反映されるまでに10分かかることがあります。

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アプリ用サービスグラフ

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
- サービスグラフでの詳細表示
- サービスグラフでのしきい値の設定
- サービス詳細の表示
- 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
- 分散トレース
- 診断の表示

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

サービスグラフの設定

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 ADM バージョン	NETSCALER AGENT 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クラスターをさまざまな展開トポロジで構成でき、以下の表は、サービスグラフでサポートされているトポロジを示しています。

トポロジ	サービスグラフでサポート
シングルティアまたは統合イングレス	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
NodePortタイプのサービス	いいえ

NetScaler® ADM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

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

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 ADMとKubernetesクラスターが同じネットワーク上にある場合（例：NetScaler ADMとKubernetesクラスターが同じCitrix Hypervisor™上でホストされている場合）。
- NetScaler ADM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。

- シングルティアまたは統合イングレストポロジでKubernetesクラスターを構成しました。
- NetScaler ADMに(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-unified-single-ingress-topology.html#add-vpx-or-sdx-or-mpx-or-blx-instance-in-citrix-adm)を追加し、**Web Insight**を有効にしました。
- NetScaler ADMに(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-unified-single-ingress-topology.html#add-kubernetes-cluster-in-citrix-adm)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クラスターを構成しました。
- NetScaler ADMとNetScaler CPX間の通信を有効にするために、NetScaler ADMで(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#configure-static-routes-in-citrix-adm-agent)を構成しました。

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

注

同じクラスターにNetScaler ADM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。

- GitHubリポジトリから(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#download-the-sample-deployment-files-from-github)をダウンロードしました。
- NetScaler ADMへのCPXの登録を成功させるために、CPX YAMLファイルに(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-parameters-in-cpx-yaml-file)を追加しました。
- NetScaler ADMに(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-vpx-or-sdx-or-mpx-or-blx-instance-in-citrix-adm)を追加しました。
- NetScaler ADMに(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-kubernetes-cluster-in-citrix-adm)を追加しました。
- (/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#deploy-a-sample-microservice-application)を展開しました。
- NetScaler CPXを展開し、(/ja-jp/netscaler-application-delivery-management-software/13-1/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#deploy-cpx-and-register-cpx-in-adm)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トランザクションとTCPトランザクションの設定を**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

以下が完了していることを確認してください。

- Kubernetesクラスターバージョン `1.14.0` が、以下のいずれかのサービスメッシュトポロジで構成されていること。

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

- 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が有効になっていること。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ます。

  ```
  admissionregistration.k8s.io/v1beta1
  ```

- Istio `istio v.1.3.0`がインストールされていること。
- Helmバージョン3.xがインストールされていること。
- NetScaler ADMとNetScaler CPX間の通信を有効にするために、NetScaler ADMで静的ルートが構成されていること。

  注記

  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デプロイしている場合、この手順は無視できます。

- サービスメッシュトポロジデータを設定するために、必要なパラメータ を構成しました。
- サンプルアプリケーション を展開しました。
- NetScaler ADM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。

  注記

  CPXがサービスメッシュ展開で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。

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

サービスグラフで詳細を表示

NetScaler® ADM 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/サービスメッシュライトトポロジ	単一層/統合イングレストポロジ
2層アーキテクチャの図(/en-us/netscaler-application-delivery-management-software/media/two-tier-sg.png)	その他のトポロジの図(/en-us/netscaler-application-delivery-management-software/media/other-topologies.png)

- **Tier 1 イングレス** – Kubernetes クラスター内の NetScaler Ingress Controller は、Kubernetes クラスター外の NetScaler インスタンス (VPX/MPX/SDX/BLX) を構成します。
- **Tier 2 イングレス** – 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。
- **イングレス** – その他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

サービスグラフの詳細(/en-us/netscaler-application-delivery-management-software/media/details-service-graph.png)

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のネットワークマップ

2 – 特定の期間における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時間リスト

5 - サービスを表示するためにフィルターを適用する

6 – 設定アイコン

7 – 拡大・縮小表示

8 – グラフ表示または表形式表示

選択した時間に基づいて、サービスグラフを表示できます。

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

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、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、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、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。

注

サービスに警告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。詳細情報をさらにドリルダウンするには、ヒット数を示すグラフから期間を選択します。

注

NetScaler ADM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、サービスで使用されるプロトコルが表示されます。次の図に示すように、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。

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

注

Orchestration > **Kubernetes** > **Clusters** に複数のクラスターを追加した場合、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。

  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への主要メトリック

  主要メトリック(/en-us/netscaler-application-delivery-management-software/media/key-metrics-tabular.png)

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。

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

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。

- **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 ADM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 ADMはクライアントの場所を認識できます。NetScaler ADM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 ADMは、IPアドレスがNetScaler ADM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City 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 ADMは、このクライアントのトラフィックがCity Aから発信されていると認識します。

プライベートIPブロックを作成する

NetScaler ADMは、クライアントのプライベートIPアドレスがNetScaler ADMサーバーに追加されている場合、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City 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 ADMは、このクライアントのトラフィックがCity 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 ADMで、 > > の順に移動し、 をクリックします。
2. ページで、次のパラメータを指定します。
    - **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、地域を選択することもできます。
    - **市**。地域に基づいて市が自動入力されますが、市を選択することもできます。
    - **市の緯度**と**市の経度**。選択した市に基づいて、緯度と経度が自動入力されます。
3. 完了するには**作成**をクリックします。

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

パブリックIPブロック

NetScaler ADM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 ADMには、クライアントの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、**Insightの構成**ページから**地理データ収集を有効にする**を有効にすることです。

注

NetScaler ADM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。

イングレスメトリックの表示

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インスタンスが稼働中 (Up)、停止中 (Down)、またはステータス不明 (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**イングレス**のみを表示できます。

詳細をさらに掘り下げるには、**イングレス**をクリックします。詳細については、「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する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。

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

- **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データの合計
- **TCPサーバーリセット** – サーバーから開始されたTCPリセットの合計

SSLメトリック

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メトリックが表示されます。

- **SSLサーバーエラー** – サーバーからのSSLエラーの合計を示します。(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
- **SSLクライアントエラー** - クライアントからのSSLエラーの合計を示します。(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。

例えば、遅延が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。

「**Service Info**」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。

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

注

Kubernetesサービス定義YAMLでサービス用に構成されたラベルによっては、さらに多くのフィルターオプションを表示することもできます。

「**Clear All**」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

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後、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。

サービスビュー(/en-us/netscaler-application-delivery-management-software/media/services-views.png)

4 – サービスをどのように表示するか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かのオプション。

エラーを分析する

エラーを示す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エラー(/en-us/netscaler-application-delivery-management-software/media/sg-tcp-error.png)	**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クライアントエラー(/en-us/netscaler-application-delivery-management-software/media/sg-tcp-client-error.png)	**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。

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

エラー	説明
SSLエラー(/en-us/netscaler-application-delivery-management-software/media/sg-ssl-error.png)	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 (プロトコルタイプに関係なく) は、クライアントエラー数が**1以上**の場合、任意のサービスに表示されます。
- 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。

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**のメトリックの詳細を表示できます。

NetScaler ADMでは、Ingressとサービス間のトランザクションの詳細を表示することもできます。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。

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

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 Protocol – SSLプロトコルバージョンを示します。

Ingress と **service** の間の矢印をクリックして、詳細なトランザクションを表示します。

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® ADM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**デフォルトのしきい値**（サービス応答時間 = 200ミリ秒、エラー数 = 0）を表示できます。

注

デフォルトのしきい値は削除できません。

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**をクリックして、新しいしきい値を設定します。

   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**シングル**または**ダブル**を選択します
   d. しきい値を指定します。

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

注記

二重しきい値を選択した場合は、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**ページでしきい値の詳細を表示できます。

単一しきい値

単一しきい値を構成すると、NetScaler ADM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
- 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 ADM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、**詳細の表示**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)

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

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サービス主要メトリックをグラフ形式で表示 (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)。

  サービスの詳細(/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すると、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。

- **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応答時間を示します

メトリクスの詳細

メトリクス	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

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

メトリクス	説明
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

サービスに関連付けられているバックエンドPodを表示するには、**Pods**タブをクリックします。

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

Poll Nowオプションを使用してPodのステータスを取得する

Poll Now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。

1. **インスタンスの詳細**をクリックして、詳細を表示します。
2. 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。
   - **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。

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

- **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。

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**

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（**稼働中**、**停止中**、**サービス停止中**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 – ADC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スペース使用率。

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

- **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リクエスト/秒** – 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接続** – 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トランザクション** – 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。

- **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。	- CPU使用率が高い
		- メモリ使用量が多い
		- ディスク使用量が多い
		- SSLカードの障害
		- 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

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

問題カテゴリ	説明	問題
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
容量の問題	ADCの容量の問題を表示します。ADMは、ADC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します。たとえば、インスタンスに選択した期間の次のエラーがあるとします。

- 「**現在の**」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ADC運用上の問題が表示されます。

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

- 「**すべて**」タブには、選択した期間に検出されたすべてのインフラ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。

- 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より前**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性を減らすことができます。

  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。

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

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG:

    distributed_tracing:

      enable: 'true'

      samplingrate: 100

    endpoint:

      server: <ADM-AgentIP> / <ADM-AppserverIP>

    timeseries:

      port: 5563

      metrics:

        enable: 'true'

        mode: 'avro'

      auditlogs:
```

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

```
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
```

注

`Samplingrate` の値は 0 から 100 の間で指定できます。NetScaler ADM 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
```

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

```
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
```

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

```
        enable: 'true'
    transactions:
      enable: 'true'
      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する

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。

- サジェスト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期間を選択できる期間リスト (2)。
- ドラッグして選択することで特定の期間の結果を表示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対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

トランザクションをクリックして詳細情報をドリルダウンします。選択したサービスに対して、以下のようなトランザクションの詳細を表示できます。

- 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。

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

トレースの詳細(/en-us/netscaler-application-delivery-management-software/media/trace-details.png)

「トレースの詳細」ページが表示されます。

トレーストランザクション(/en-us/netscaler-application-delivery-management-software/media/trace-transactions.png)

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。

トランザクションをクリック(/en-us/netscaler-application-delivery-management-software/media/trace-click-transaction.png)

`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。

フィルターパネル(/en-us/netscaler-application-delivery-management-software/media/filters-panel.png)

- **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**: データ転送サイズと、サービスとの間で転送が行われる速度。
- **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情報に基づくクライアントOS。

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

- **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。
- **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。
- **SSL暗号強度**: SSL証明書のキーサイズに基づく暗号強度（高、中、低など）。
- **SSLキー強度**: SSL暗号強度はSSL証明書の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的なデータまたはデータなしの場合の診断の詳細を表示

必要なサービスグラフの構成を完了し、NetScaler ADMにKubernetesクラスターを追加すると、サービスグラフがデータの入力を開始します。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をいくつか示します。

- 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
- 必要な分析構成が設定されていないため、サービスグラフがすべてのデータをロードできません

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が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を使用すると、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® ADMで、**Applications** > **Service Graph**に移動し、**Microservices**タブをクリックします。

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

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。

>をクリックして詳細を表示します。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。

See Moreをクリックして問題の詳細を表示します。

詳細を見る(/en-us/netscaler-application-delivery-management-software/media/more-details.png)

- **問題の種類** – 設定、分析設定、またはライセンスから発生してい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。

部分的なデータの診断

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、**Show Diagnostics**ボタンをクリックして診断情報を表示します。

以下の例は、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、**Settings > Analytics Settings**に移動して、**TCP Transaction Settings**を**All**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 ADMは定期的に診断チェックを自動的に実行します。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、**Run Diagnostics**をクリックし、**CPX instances**を選択して、**Run Diagnostics**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)

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

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。

   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、ADC、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、ADC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

  ネットワーク機能ビュー(/en-us/netscaler-application-delivery-management-software/media/ga-sg-networkview.png)

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。

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

ネットワーク機能ビュー(/en-us/netscaler-application-delivery-management-software/media/sg-gslb-nf.png)

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

ADC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のみを表示します（クライアントとADCなし）。

構成ビュー(/en-us/netscaler-application-delivery-management-software/media/ga-sg-configview.png)

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。

メトリックなし(/en-us/netscaler-application-delivery-management-software/media/ga-no-metrics.png)

メトリックを分析する

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のいずれかでメトリックの詳細が表示されます。

クライアントメトリック

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/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ック

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、メトリックの詳細が表示されます。

ネットワーク機能メトリック(/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。
- **ADC処理時間** – ADCインスタンスによる平均処理時間を示します。

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

- **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。

サービスメトリック

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。
- **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）

ADC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。

ADC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ADCスコアが表示されます。スコアは、さまざまなNetScalerの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。
- **ADC処理時間** – ADC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：

ホスト名の代わりにNetScaler IPアドレスが表示されます。
メトリックでは、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)

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

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リージョン

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

> **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

クライアントリージョン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**」 - クライアント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SSLエラーの合計数を示します。

NetScalerの詳細を表示

サービスグラフでは、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
- 各データセンターからスコアの低い上位4つのNetScalerインスタンスのみ

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

ADCグループ(/en-us/netscaler-application-delivery-management-software/media/adc-group.png)

「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。

その他のADC(/en-us/netscaler-application-delivery-management-software/media/all-adcs.png)

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。

ADCの詳細(/en-us/netscaler-application-delivery-management-software/media/adc-details.png)

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。
- **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、ADCインスタンスに関連する問題などのインスタンス詳細を表示します。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」(/ja-jp/netscaler-application-delivery-management-software/13-1/hybrid-multi-cloud-deployments/infrastructure-analytics-instance-details.html#instance-score)を参照してください。

個別のアプリケーションを表示する

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
アプリ 3	10.102.32.40	49 (確認)	アップ
アプリ4	10.102.113.208	92 (良好)	ダウン

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

アプリ名	NETSCALER	アプリスコア	アプリステータス
アプリ5	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 (レビュー)	稼働中

このシナリオでは、App1、App3、App6、App7をサービスグラフ内のスコアの低い上位4つのアプリケーションとして表示できます。

同様に、**カスタム**アプリケーションと**マイクロサービス**アプリケーションのスコアの低い上位4つのアプリケーションも表示できます。

サービスにマウスポインターを合わせると、メトリック情報を表示できます。

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** – 稼働中または停止中など、アプリケーションの現在のステータスを示します
- **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** – 全体的なアプリケーションスコアに影響を与える上位の問題を示します

その他をクリックして、すべての個別アプリケーションを表示します。次の図に示すように、個別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** – 個別アプリケーションの合計数
- **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。

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

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、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。

マイクロサービスアプリケーションの表示

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。

以下を表示できます。

- サービス名
- サービスで使用されるプロトコル（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合計数
- **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 = Client RTT + リクエスト最終バイト – リクエスト初回バイト)
- **エラー** – 4xx、5xxなどのエラーの合計
- **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エラーの合計

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)

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

結果をフィルタリングするための検索バー

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、この検索バーを使用すると、次の場合に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、フィルター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)

たとえば、特定のADC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。

検索結果(/en-us/netscaler-application-delivery-management-software/media/search-results-gsg.png)

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

StyleBook

StyleBook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ようにStyleBookを設計することもできます。

StyleBookは、構成が宣言的でバージョン管理されているDevOpsチームによって実践されているInfrastructure-as-codeの原則によく適合します。構成は繰り返し可能であり、全体として展開されます。StyleBookには次の利点があります。

- **宣言的**: StyleBookは、命令型ではなく宣言型の構文で記述されます。StyleBookを使用すると、特定のNetScalerインスタンスでそれ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 Application Delivery Management (ADM) 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。StyleBook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 ADM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**: StyleBook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が常に一貫した状態に保たれることが保証されます。
- **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、この一意の特性を維持するために、そのバージョン番号（またはその名前または名前空間）を更新する必要があります。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が定義された後、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。一般的な構成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。StyleBookはバージョン管理されているため、既存のStyleBookへの変更は新しいStyleBookをもたらし、したがって依存するStyleBook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**: StyleBook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、パラメータを使用して抽象化できます。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.

StyleBook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に展開でき、インスタンス間を移動することもできます。

- **自動生成UI**: NetScaler® ADMは、NetScaler ADM GUIを使用して構成を行う際に、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 ADM 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、StyleBook APIは、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。各構成は構成パック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、それをNetScalerインスタンスで実行できます。この構成は構成パック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。この構成用に新しい構成パックが作成されます。構成パックは、NetScaler ADMと、構成が実行されるNetScalerインスタンスの両方に保存されます。

展開用の構成を作成するには、NetScaler ADMに付属のデフォルトのStyleBookを使用するか、独自のStyleBookを設計してNetScaler ADMにインポートすることができます。StyleBookを使用して構成を作成するには、NetScaler ADM 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/13-1/stylebooks/business-application-stylebooks.html)
- カスタムStyleBook(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/how-to-create-custom-stylebooks.html)
- スタイルブック内のAPI
- StyleBookの文法(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar.html)

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

StyleBookのカテゴリ

NetScaler® Application Delivery Management (ADM)には、2つのStyleBookカテゴリがあります。これらはデフォルトのStyleBookとカスタムStyleBookです。デフォルトかカスタムかにかかわらず、StyleBookはパブリックまたはプライベートのいずれかです。NetScaler ADMでは、種類や可視性の状態に関係なく、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 ADM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。
- ADMのデフォルトStyleBookを非表示にします。
- NetScaler ADM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StyleBook**は、NetScaler ADM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StyleBookを削除することはできませんが、ADM GUIから非表示にすることはできます。
- **カスタムStyleBook**は、NetScaler ADMにインポートした独自のStyleBookです。

デフォルトとカスタムの両方のStyleBookは、パブリックまたはプライベートのいずれかです。

パブリックおよびプライベートStyleBook

構成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 ADM GUIおよびAPIから構成を作成するために直接使用できます。

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 ADM GUIから構成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 ADMに表示して確認することはできます。カスタムStyleBook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 ADM APIを使用して構成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 ADM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、両方の種類のStyleBookを個別に表示したい場合もあります。

NetScaler ADM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表示されます。

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表示されます。

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、次の画像に示すように、異なるアイコンが表示されます。

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

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。

ページ右上に、表示するStyleBookの種類を選択するオプションが表示されます。「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 ADMからカスタムStyleBookをダウンロードするには、**Applications** > **StyleBooks** > **Configurations**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チェックします。**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、ダウンロードされるバンドルに依存StyleBookを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:

NetScaler ADMのデフォルトStyleBookはダウンロードできません。そ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を削除

Delete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 ADMからStyleBookを削除するかどうかを確認するメッセージが表

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

示されます。StyleBookが他のカスタムStyleBookを使用している場合、チェックボックスを選択してそれらのStyleBookを削除することを選択できます。

注:

NetScaler ADMに依存StyleBookがある場合、カスタムStyleBookを削除しないでください。そうしないと、既存のStyleBookが破損します。

StyleBookの依存関係を表示

StyleBookの重要かつ強力な機能は、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 ADM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されるかを学ぶことができます。

NetScaler ADMでは、StyleBookが相互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 ADMで、**アプリケーション** > **StyleBook**に移動します。StyleBookページには、NetScaler ADMで使用可能なすべてのStyleBookが表示されます。下にスクロールして、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。**依存関係の表示**をクリックします。

順方向の依存関係

順方向の依存関係タブでは、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。矢印のいずれか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。

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

逆方向の依存関係

逆方向の依存関係タブでは、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が自分のStyleBookを指していることがわかります。一部のStyleBookはStyleBookを直接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。

構成パックに対するADC構成の監査

StyleBook構成パックによって行われた変更を現在のADC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構成パックとADC構成の間の構成のずれを検出します。
- 構成パックによって行われた変更を反映していない、ADC上の変更されたオブジェクトと削除されたオブジェクトを特定します。

構成パックの変更をADCの構成と比較するには、次の手順を実行します。

1. 「**アプリケーション**」>「**StyleBooks**」>「**構成**」に移動します。
2. 「**構成監査**」をクリックします。

   構成監査ページには、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ADC構成の監査(/en-us/netscaler-application-delivery-management-software/media/configuration-audit-configpack.png)

StyleBookのタグを作成する

NetScaler ADM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 ADM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. 「**アプリケーション**」>「**StyleBooks**」に移動します。
2. タグを追加するStyleBookで「**タグ**」を選択します。

   StyleBookのタグ(/en-us/netscaler-application-delivery-management-software/media/adm-tags-stylebooks-new-citrix.png)

   すべての種類のStyleBookにタグを追加できます。

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

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、キー=team、値=bizdata

   StyleBookのタグを作成する(/en-us/netscaler-application-delivery-management-software/media/adm-create-tags-stylebook-citrix.png)

   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。

タグを使用してStyleBookをフィルタリングするには、検索バーで「**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。

タグの使用方法(/en-us/netscaler-application-delivery-management-software/media/use-tags-stylebook-citrix.png)

以下は、`key=team`および`value=bizdata`のタグを持つStyleBookの検索例です。

タグの例(/en-us/netscaler-application-delivery-management-software/media/example-adm-tag-citrix.png)

StyleBookタグをその構成パック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構成パックを検索できます。

構成パックを作成するときは、「**タグの関連付け**」セクションで次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。
- **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、構成パックに関連付けることができます。

StyleBookタグをその構成パックに関連付ける(/en-us/netscaler-application-delivery-management-software/media/associate-tags-stylebook-configuration-pack-citrix.png)

CLIコマンドを使用してStyleBookを構成するには

CLIコマンドを使用してStyleBookを構成したい場合は、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 ADM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StyleBookのいずれかを使用して構成を作成します。

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

- NetScalerで`show ns runningConfig`コマンドを再度実行します。

2つの出力の違いは、NetScaler CLIを使用して任意のStyleBookを設定するために利用できるCLIコマンドを示しています。

GitHub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を考えてみましょう。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で管理しているシナリオを考えてみましょう。

GitHub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を作成しているかもしれません。これらのStyleBookは、Citrix Applications and Delivery Management (ADM) でも必要です。これで、これらのStyleBookをNetScaler ADMに直接インポートできます。GitHubから手動でコピーしてNetScaler ADMにアップロードしたり、ADMとGitHub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。

NetScaler® ADMで、GitHubリポジトリを表すリポジトリを定義できるようになりました。GitHubリポジトリのURLと、GitHubで作成したユーザー名とパスワード（またはAPIトークン）を指定します。つまり、GitHubで有効なアカウントを持つ認証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。

リポジトリを作成したら、NetScaler ADMをGitHubリポジトリと同期できます。NetScaler ADMはGitHub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、ADMはStyleBookを検証し、NetScaler ADMのStyleBookリストに追加します。検証に失敗したStyleBookはNetScaler ADM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リポジトリにコミットしてください。後で、それらをNetScaler ADMに再度インポートまたは同期を試すことができます。

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

注

- StyleBookファイルは、GitHub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。
- GitHubリポジトリからのStyleBookの同期は、NetScaler ADM GUIまたはAPIから手動で開始する必要があります。つまり、現在、StyleBookのインポートと同期は、GitHubのコミットアクティビティに基づいて自動的に行われるわけではありません。

リポジトリを追加し、GitHubリポジトリからStyleBookをインポートする

開始する前に、GitHubに有効なアカウントがあることを確認してください。

GitHubリポジトリ内の任意のフォルダーからADMにStyleBookファイルをインポートできます。

1. NetScaler ADMで、**Applications** > **StyleBooks** > **Repositories** の順に移動します。
2. **Add** をクリックします。**Add Repository** ウィンドウで、次のパラメーターを入力します。
   - **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リポジトリのURLを入力します。
   - **ユーザー名とパスワード**。GitHub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にアクセスする際のパスワードの代わりに使用できます。GitHubリポジトリのAPIトークンの作成方法については、GitHubドキュメントの個人アクセストークンの作成を参照してください。

3. **作成**をクリックします。

   リポジトリがNetScaler ADMに作成されます。

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

4. StyleBookをインポートまたは同期するには、**リポジトリ**ページでリポジトリを選択し、**同期**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。
- **削除**。リポジトリと、以前にそのGitHubリポジトリからインポートされたNetScaler ADMに存在するすべてのStyleBookを削除できます。

  注

  ConfigPackが関連付けられているStyleBookがある場合、NetScaler ADM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のすべての構成パックを削除します。その後、NetScaler ADM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 ADM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 ADM内のすべてのStyleBookを削除できます。
- **ファイルの一覧表示**。GitHubリポジトリから取得されたNetScaler ADMに存在するすべてのStyleBookのリストを表示できます。

デフォルトのStyleBookを使用する

NetScaler Application Delivery Management (ADM) 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、StyleBook内のパラメータの値を指定し、構成を実行する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 ADMは指定し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StyleBookから構成を作成するには

1.**Applications** > **Configurations > StyleBooks** に移動します。StyleBooksページには、NetScaler ADM内のすべてのStyleBookが表示されます。このリストには、デフォルトのStyleBookとカスタムStyleBookの両方が含まれます。検索フィールドにStyleBookの名前を入力して**Enter**キーを押すか、リストをスクロールしてStyleBookを見つけることができます。

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。

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

注:

構成パラメータと値は、選択したStyleBook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 ADM > **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 ADM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。

NetScalerインスタンスで構成を実行する前にテストまたは検証する場合は、**Dry Run** を選択し、**Create** をクリックします。構成が有効な場合、指定した値に基づいて作成されるオブジェクトが表示されます。

4.**Dry Run** チェックボックスをオフにし、**Create** をクリックして構成を作成し、NetScalerインスタンスで構成を実行します。作成したStyleBook構成は、以下に示すように構成リストに表示されます。

注

NetScaler ADMで最近検出されたNetScalerインスタンスを、このウィンドウで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。

これで、NetScaler® ADMを使用して、この構成パックを検査、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、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脅威を含む）からWebアプリケーションとサイトを保護するWebアプリケーションファイアウォール（WAF）です。

NetScaler ADMでは、NetScalerインスタンス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。

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

アプリケーションファイアウォール構成の展開

次のタスクは、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とIPレピュテーションポリシーを含む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 ADMで、**Applications** > **Configurations** > **StyleBooks** の順に移動します。StyleBooksページには、NetScaler ADM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。`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、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。

2. 次のパラメータの値を入力します。

   - **負荷分散アプリケーション名**。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を含む負荷分散構成の名前。
   - **負荷分散アプリケーション仮想IPアドレス**。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。
   - **負荷分散アプリケーション仮想ポート**。ユーザーが負荷分散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。
   - **負荷分散アプリケーションプロトコル**。リストからフロントエンドプロトコルを選択します。
   - **アプリケーションサーバープロトコル**。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、**高度なロードバランサー設定**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します(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-2-citrix.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-citrix.png)

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

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します(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-4-citrix.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名を作成します(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-5-citrix.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します(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-6-citrix.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します(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-7-citrix.png)
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。

   そのVIP上のすべてのトラフィックにアプリケーションファイアウォール設定を適用する場合は、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設定を有効にします(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-8-citrix.png)
10. 必要に応じて、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. 必要に応じて、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。

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

12. 次に、StartURL設定、DenyURL設定など、そ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、「アプリケーションファイアウォール」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 ADM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。

14. **IPレピュテーションチェック**を有効にして、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。

    ヒント

    Citrixでは、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。

    各サーバーで作成されたオブジェクトを次の図に示します。

    WAFによってADCインスタンスに作成されたオブジェクト(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-12.png)

16. NetScaler® ADMで作成されたConfigPackを表示するには、**Applications** > **Configurations**に移動します。

    WAF構成パック(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-13-citrix.png)

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

StyleBookを使用してWAFおよびBOTプロファイルを作成する

API GatewayでAPIリソースにポリシーを選択すると、APIリクエストを認証するためのトラフィック選択基準を定義できます。また、APIトラフィックにAPIセキュリティポリシーを設定することもできます。

APIリソースにWAFおよびBOTポリシーを設定できます。ポリシーを設定する前に、NetScaler® Application Delivery Management (ADM) でそのプロファイルを作成してください。プロファイルを作成するには、以下のデフォルトのStyleBookを使用します。

- API WAF 検出 StyleBook
- API BOT 検出 StyleBook

StyleBookを使用してWAFプロファイルを作成する

WAFプロファイルを作成するには、以下を実行します。

1. NetScaler ADMで、**Applications** > **Configurations** > **StyleBooks** に移動します。`api-waf-profile`として名前を入力してStyleBookを検索します。**Create Configuration** をクリックします。

   StyleBookはユーザーインターフェー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. 次のパラメーターの値を指定します。

   - **API WAFプロファイル名** - WAFプロファイルを識別するための名前。
   - **アプリケーションタイプ** - プロファイルにアプリケーションタイプを追加します。WAFプロファイルはJSONおよびXMLアプリケーションタイプをサポートしています。
3. オプションで、**セキュリティ設定**を有効にして、HTTP、JSON、またはXMLの保護チェックを指定します。NetScaler Web App FirewallにエラーURLを指定することもできます。詳細については、「Web App Firewallプロファイルの作成」を参照してください。
4. この構成を展開するターゲットのNetScaler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。
5. **作成**をクリックします。

WAFポリシーを設定するには、API展開にポリシーを追加するを参照してください。

StyleBookを使用してBOTプロファイルを作成する

BOTプロファイルを作成するには、次の手順を実行します。

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

1. NetScaler ADMで、**Applications** > **Configurations** > **StyleBooks**の順に移動します。名前を `api-bot-profile` と入力してStyleBookを検索します。**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ページとして開きます。
2. **BOT Profile Name**で、BOTプロファイルを識別する名前を指定します。
3. オプションで、要件に基づいて次のオプションを有効にします。

   - **Enable IP reputation check** - このオプションは、不要な要求を送信しているIPアドレスを識別します。IPレピュテーションリストを使用して、評判の悪いIPからの要求を事前に拒否できます。
   - **Enable BOT Signatures** - BOTシグネチャ名を指定します。指定されたシグネチャからの要求をブロックします。
   - **Allow List** - IPv4またはサブネット（CIDR）アドレスを指定します。このオプションにより、BOTプロファイルは指定されたIPv4またはサブネットアドレスからの要求をバイパスできます。
   - **Deny List** - IPv4またはサブネット（CIDR）アドレスを指定します。このオプションにより、BOTプロファイルは指定されたIPv4またはサブネットアドレスからの要求をブロックできます。
4. この構成を展開するターゲットのNetScaler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。
5. **Create**をクリックします。

BOTポリシーを設定するには、API展開にポリシーを追加するを参照してください。

すべてのデフォルトStyleBookを非表示にする

NetScaler® ADMは、NetScaler ADM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。ユーザーが作成した、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できるようにすることができます。

NetScaler ADMを使用すると、カスタムStyleBookを表示し、NetScaler ADMに付属するすべてのデフォルトStyleBookを非表示にできます。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。

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

すべてのデフォルトStyleBookを非表示にするには：

1. NetScaler ADMで、**Applications** > **Configurations > Settings** 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。

RBAC機能を使用してページを非表示にすることを選択しなかった場合、**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 ADMで、**アカウント** \> **ユーザー管理** \> **アクセスポリシー** に移動します。
2. ポリシーを作成するには、**Add** をクリックします。
3. ポリシー名を入力します。
4. **Permissions**セクションで、**All** > **Applications** > **Configuration** > **Settings**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、ロールをユーザーグループに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、「Configuring Role-Based Access Control」を参照してください。

StyleBooks Configuration Builder を使用した NetScaler アプリケーション構成の移行

注

この機能はテクニカルプレビュー版です。

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

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、ある NetScaler インスタンスから別のインスタンスへのアプリケーション構成の移行も自動化します。

Configuration Builder を使用すると、カスタマイズされた StyleBook を作成する要件を簡素化できます。この機能により、StyleBooks の文法や構成要素に関する深い知識がなくても StyleBook を作成できます。そうでない場合、StyleBook を作成するには StyleBooks の文法と構成要素の知識が必要です。

Configuration Builder は、新しい ADC インスタンスで同じ ADC 構成を反映する ConfigPack も作成します。この ConfigPack を使用すると、ある ADC インスタンスの初期 ADC 構成を別の ADC インスタンスに複製できます。初期構成ソースは次のいずれかです。

- **NetScaler インスタンス:** 複製したいアプリケーション構成がホストされているインスタンスを指定します。

  ターゲットインスタンスを指定しなくても、Configuration Builder は ADC 構成を StyleBook と ConfigPack に変換します。後でこの ConfigPack を使用して、ADC 構成を他の ADC 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。

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 は選択され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。

- **展開属性** - 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。
- **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ら、ターゲット ADC 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 ConfigPack が NetScaler® ADM に作成されます。この ConfigPack は、ターゲット ADC 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 ConfigPack を表示するには、**Applications** > **StyleBooks** > **Configurations** に移動します。

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

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。

- コンテンツスイッチング
- ロードバランシング
- モニタリング
- SSLオフロード
- レート制限
- リライト
- レスポンダー
- 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 ADMでNetScalerアプリケーションの移行を行うStyleBookを作成する手順は次のとおりです。

1. **Applications** > **StyleBooks** > **Configurations** に移動します。
2. **Migrate ADC Configuration** をクリックします。
3. **Get Started** をクリックします。
4. 「**Specify Configuration**」で、構成ソースを選択します。
    - 「**Import from an ADC**」：このオプションは、選択したADCインスタンス上のアクティブなアプリケーションを検出します。
    - 「**Import using CLI Commands**」：このオプションは、CLIコマンドを分析し、CLIコマンドからアプリケーションを抽出します。
5. アプリケーション構成を移行または複製する**Source ADC Instance**を指定します。
6. アプリケーション構成を移行または複製する**Target ADC Instance**を指定します。
7. 「**アプリケーションの定義**」で、,
    a. 「**Application Name**」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. 「**Next**」をクリックします。

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

8. 「**Equivalent CLI Commands**」で、コマンドを確認し、「**Next**」をクリックします。

   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です。

9. 「**Deployment Attributes**」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アドレスとポートを表示および編集できます。

   IPアドレスとポートを編集するには、フロー図で仮想サーバー、サービス、またはサービスグループメンバーの編集アイコンをクリックします。

   デプロイ属性を編集します(/en-us/netscaler-application-delivery-management-software/media/edit-deployment-attributes.png)

   このタブは、次の場合にのみ表示されます。

   - ソースインスタンスとターゲットインスタンスが異なります。
   - CLIコマンドを使用して構成をインポートします。

10. **Configuration Attributes**で、必要な詳細を指定し、**Next**をクリックします。

    このタブには、パスワードや証明書を復号化するためのキーなどのシークレットが一覧表示されます。

    注

    移行を開始する前に、見つからない構成またはサポートされていない構成が、次のいずれかのタブに表示されます。

    サポートされていない構成
    サポートされていないグローバル構成
    これらの構成を正常に移行するには、見つからない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。そして、**Next**をクリックします。

11. **Migrate**で、必要なStyleBookの詳細を指定します。**Migrate**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に発生します。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 StyleBook

NetScaler® ADM は、特定のビジネスアプリケーション向けに ADC 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 proxy スタイルブック
- Oracle e-business スタイルブック
- Webアプリケーションファイアウォール StyleBook
- StyleBook を使用した WAF および BOT プロファイルの作成

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 ADM 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、ユーザーがGoogle Appsにアクセスするための認証を行うSAML IDプロバイダーとしてNetScalerインスタンスを構成します。

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

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
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、それ以降の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、認証リクエストを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® ADMで、**Applications** > **Configurations** > **StyleBooks** に移動します。StyleBooksページには、NetScaler ADM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. **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。

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

b. **認証仮想IPアドレス**。GoogleアプリSAML IdPポリシーがバインドされている認証、承認、および監査仮想サーバーによって使用される仮想IPアドレス。

c. **SAMLルール式**。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.HEADER("Referrer").CONTAINS("google")。要件が異なる場合は、このフィー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、および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認証リクエストを受け入れます。

c. **アサーションコンシューマーサービスURL**。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。

d. このセクションには、他にもオプションの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」プロファイルです）。

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」です）。

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」です）。

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されているため、Citrixではデフォルト設定を維持することをお勧めします。

e. また、「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の詳細を入力することもできます。

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

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

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が発行す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、以下を構成する必要があります。

a. **LDAP (Active Directory) ベース**。認証を許可する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) バインド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) バインド 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。

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。

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

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. **証明書名**。SSL 証明書の名前を入力します。
   b. **証明書ファイル**。ローカルシステムまたは NetScaler ADM のディレクトリから SSL 証明書ファイルを選択します。
   c. **証明書キー形式**。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. **証明書キー名**。証明書の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 ADMから、証明書の秘密キーを含むファイルを選択します。
   f. **秘密キーパスワード**。秘密キー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. 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には、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。
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は、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、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 (公開キー) を指定するために、SAML SP SSL証明書を選択できます。
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 ADM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。

また、,

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

ヒント

Citrixは、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。

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。

- 管理者による管理コンソールへのサインインを含む
- エンタープライズ資格情報を使用して、すべてのMicrosoft Office 365サービスに一度サインオンする。

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、次の手順を実行します。

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. インスタンスでLDAP認証サーバーとポリシーを構成する
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。

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。この統合プロセスは、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

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

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。

SSO Microsoft Office 365 StyleBookを展開するには

1. NetScaler® Application Delivery Management (ADM)で、**Applications** > **StyleBooks**に移動します。**StyleBooks**ページには、NetScaler ADM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. **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証明書 設定**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鍵をロードするために、秘密鍵のパスワードを入力することもできます。

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。

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

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、次のように構成します。

   - **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
   - **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を追加します（設定を容易にするためにメールアドレスを使用）。例: cn=Manager,dc=netscaler,dc=com
   - **LDAP (Active Directory) Bind DNパスワード**。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。
     - 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。
     - 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名のいずれか少なくとも1つを指定する必要があります。

     - 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）。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証明書の検証に使用されます。
     - 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、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。

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

- **CertKey形式**。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。
- **証明書キー名**。証明書の秘密鍵の名前を入力します。
- **証明書キーファイル**。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。
- **秘密鍵パスワード**。秘密鍵ファイルを保護するパスフレーズを入力します。

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。

10. 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は、**SAML IdP CA証明書**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。
11. **SAML SP証明書**セクションで、Office 365 SSL公開証明書について、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します。

    - **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形式**。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。
    - **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。

12. **SAML IdP設定**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で、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`
    - **名前識別子式**。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」）。

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

- **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メソッドを選択します（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。
- **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属性のフレンドリ名**。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

  Citrixは、これらの設定がMicrosoft Office 365アプリで動作することがテストされているため、デフォルト設定を保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。

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

ヒント

Citrixでは、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。

Microsoft Skype for Business 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 の展開では、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が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。

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

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する必要がある場合、Skype for Business 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、認証済みおよび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 エッジサーバーには、次の4種類の役割があります。

- アクセスエッジ。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。
- 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するウェブ会議
- A/V会議パケットを処理し、外部ユーザーにオーディオとビデオ、アプリ共有、ファイル転送を拡張するA/V会議
- 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するXMPPプロキシ。

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、セキュリティが強化されます。

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連絡先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、ネットワーク内のSkypeサーバーの展開を模式的に示しています。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/stylebook-skype-topology-diagram.jpg)

エンタープライズ環境での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。

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

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

フロントエンドサーバーを構成するには

1. NetScaler® Application Delivery Management (ADM) で、**Applications** > **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 ADM 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の値を入力できます。
2. 「**Edge Server**」セクションで、次の仮想IP（VIP）アドレスと、ネットワーク内のすべてのEdgeサーバーのIPアドレスを入力します。
    a. アクセスエッジ、Web会議エッジ、およびA/Vエッジに使用される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. ネットワーク内の外部Edgeサーバー2台と内部Edgeサーバー2台。
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アドレスも入力します。
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アドレスも入力します。高可用性のために、少なくとも2台のDirectorサーバーを作成してください。
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。

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

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、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。
AutoDiscover内部ポート	4443	HTTPS	HTTPS (リバースプロキシから) およびAutoDiscoverサインインのための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)	フロントエンドサーバーがすべての内部SIP通信に使用します。
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。

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

ラベル	ポート	プロトコル	説明
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アプリ共有ポート	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（つまり、ダイヤルイン会議用）に使用されます。
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（つまり、ダイヤルイン会議用）に使用されます。
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コールアドミッション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アドミッ

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

ラベル	ポート	プロトコル	説明
			ションコントロールに使用されます。
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における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。

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

ラベル	ポート	プロトコル	説明
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アウトバウンドで流れる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	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ディレクターのプー

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

ラベル	ポート	プロトコル	説明
			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. **Target Instances**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。

注

更新アイコンをクリックして、NetScaler ADM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。

7. 選択したNetScalerインスタンスに構成を作成するには、「**Create**」をクリックします。

ヒント

Citrixでは、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、**Dry Run**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個の負荷分散仮想サーバーを作成します。つまり、各ポートに対して1つの負荷分散仮想サーバーが定義され、1つのサービスグループが関連付けられ、そのサービスグループが負荷分散仮想サーバーにバインドされます。この構成では、フロントエンドサーバーもサービスグループメンバーとして追加され、サービスグループにバインドされます。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。

Microsoft Exchange スタイルブック

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。

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

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主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サーバー向けに次のNetScaler機能を有効にし、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
- 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サーバーの展開を図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ポートがアクセス可能であることを確認してください。

Microsoft Exchange スタイルブックの構成

ビジネスエンタープライズでMicrosoft Exchange StyleBookを構成して、NetScaler構成を展開します。

NetScaler® ADM で Microsoft Exchange アプリケーションを構成するには

1. NetScaler ADM で、**アプリケーション** > **StyleBooks** の順に移動します。
2. **Microsoft Exchange 2016 StyleBook** を検索し、**構成の作成**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。

   マイクロソフト エクスチェンジ スタイルブック の構成(/en-us/netscaler-application-delivery-management-software/media/microsoft-exchange-2016-create-configuration-citrix.png)
3. 次のパラメータの詳細を入力します。

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

- **Exchange アプリケーション名** - 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 IP** - 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つの Exchange サーバーが構成されています。

4. **Exchange 証明書**セクションで、Exchange 証明書を NetScaler ADM 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 ADM 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、**高度な証明書設定**を選択します。

5. **Exchange Active Directory 認証設定**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内のLDAPベース文字列。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」。

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

- **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。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。

   注

   最近検出されたNetScalerインスタンスを表示するには、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。

   Citrixでは、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し、セキュリティを確保する 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 ADM、バージョン 12.0 以降
- NetScaler、バージョン 10.5 以降

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

Microsoft SharePoint 2016 StyleBook によって構成される NetScaler の機能

Microsoft SharePoint 2016 StyleBook を使用して、Microsoft SharePoint 2016 用に以下の NetScaler 機能を有効にして構成できます。

- 負荷分散
- コンテンツスイッチング
- レスポンダー
- 書き換え
- 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、12個のロードバランシング仮想サーバーを構成します。これらはそれぞれ、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に対するリクエストのロードバランシング専用です。

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に設定されています。

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、要求された特定の種類の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一致する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、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ビデオに適用したい場合があります。

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

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。

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インラインで動作し、そのため、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、リライト機能はユーザーリクエストから不要なヘッダーを削除するために使用されます。

圧縮

NetScaler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一方で、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。

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

次の図は、NetScaler ADM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化されたネットワークにおけるSharePointサーバーの展開を図式的に示しています。

(/en-us/netscaler-application-delivery-management-software/media/stylebook-sharepoint-topology.jpg)

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。

Microsoft SharePoint 2016 StyleBookを展開するには:

1. NetScaler® ADM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 ADM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 ADM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。

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

> **注**
>
> SSLを選択する場合は、このStyleBookのSharePoint詳細設定セクションでRewrite Configuration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。

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ーから該当する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 ADM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。負荷分散機能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ますが、レスポンダー構成、書き換え構成、圧縮構成、統合キャッシュ構成など、インスタンスで構成したい他の機能を選択できます。

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 ADM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。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/nmas-sharepoint-ssl-support-service-4-citrix.png)

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

注

Citrix は、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の負荷分散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、それらを負荷分散仮想サーバーにバインドします。どのポリシーが作成されるかは、構成パックの作成時に 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 ADM で構成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。**アプリケーション** > **管理** > **構成** に移動し、**作成されたオブジェクトの表示** をクリックします。次の図は、「NetScaler ADM から SharePoint StyleBook 構成を展開する」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。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/stylebook-sharepoint-defined-objects.jpg)

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 リソースの例としては、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サーバーへの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、通常は組織のペリメータネットワーク（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、安全な接続、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 Application Delivery Management (ADM) のMicrosoft ADFSプロキシStyleBookを使用すると、NetScalerインスタンス上でADFSプロキシサーバーを設定できます。

次の図は、企業DMZにおけるADFSプロキシサーバーとしてのNetScalerインスタンスの展開を示しています。

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

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します
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します
3. 事前認証のための豊富な方法をサポートします
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します
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します
    a. アクティブプロトコルアプリの例は、Microsoft Outlook、Microsoft Skype for Businessです
    b. パッシブプロトコルアプリの例は、Microsoft Outlook Web App、Webブラウザです
6. DMZベースの展開のための強化されたデバイス
7. 追加のコアNetScaler ADC機能を使用することで価値を付加します。
    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、後で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ためのNetScalerのセットアップ方法について説明します。

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

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® ADM 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。

Microsoft ADFS プロキシ StyleBook を展開するには

1. NetScaler ADM で、**Applications** \> **StyleBooks** に移動します。**StyleBooks** ページには、NetScaler ADM 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。また、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ロードすることもできます。

© 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。

5. オプションで、SSL証明書にNetScalerへのCA公開証明書のインストールが必要な場合は、「**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。

   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プロキシアクティブ認証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。

   ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/nmas-adfs-proxy-stylebooks-4-citrix.png)
8. 対応するオプションを有効にし、LDAP設定を構成して、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、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.

b. **LDAP (Active Directory) バインド 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) バインド 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 サーバー (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サーバーFQDN 名**。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名を入力してください。

f. **LDAP サーバー Active Directory ポート**。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) ログインユーザー名**。「sAMAccountName」としてユーザー名を入力します。

h. **ADFS プロキシ パッシブ認証 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サーバーのDNS VIPを設定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。

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

注記

Citrix は、実際の構成を実行する前に、**ドライラン**を選択することを推奨します。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、複数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。

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ー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、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。

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

Oracle E-Business Suite 12.2の構成を作成するには

1. NetScaler Application Delivery Management (ADM)で、**Applications** > **Configuration** > **StyleBooks**に移動します。**StyleBooks**ページには、NetScaler ADM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**構成の作成**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。ここでは、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. ロードバランシング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。さらにサーバーIPアドレスを追加するには、**+**をクリックします。
6. **SSL証明書設定**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。**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。

   構成を作成するターゲットNetScalerインスタンスを選択し、**作成**をクリックします。

   ヒント

   更新アイコンをクリックして、NetScaler ADM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。更新アイコンは現在、NetScaler ADM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、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、ユーザーが利用可能なアプリやデスクトップへのセルフサービスアクセスを可能にします。

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

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® ADM GUIで、**アプリケーション > StyleBook**に移動します。
2. 検索バーで、**名前**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 ConfigPack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要求のリダイレクト先となるHTTPS URLを指定します。

   NetScalerインスタンスでStoreFrontサーバーを構成するための詳細を指定します(/en-us/netscaler-application-delivery-management-software/media/storefront-stylebook-configuration-citrix.png)
5. **SSL証明書設定**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ーから該当するファイルを選択します。秘密キーのパスワードを入力して、PEM形式の暗号化された秘密キーを指定することもできます。

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証明書にNetScalerへのCA公開証明書のインストールが必要な場合は、「**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。

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

10. 「**Target Instances**」をクリックし、StoreFrontサーバーを構成する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の作成と使用

独自のStyleBookを作成して展開し、NetScaler® Application Delivery Management (ADM) 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。

はじめる前に

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 の作成時に注意すべき 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。
- YAML には適切なインデントが必要です
- 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みます。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ます。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off、TRUE/true/truthy/FALSE/False/false/falsely などの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、引用符で囲みます。例:
  - 「YES」
  - 「いいえ」

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

- "真"
- 「False」など。

注

NetScaler ADMにStyleBookファイルを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。Citrixは、YAMLコンテンツを検証およびインポートするために、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を宣言できます。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。
- **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で必要なパラメーターを定義できます。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）を定義できます。このセクションはStyleBookのコアと見なされます。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適応させます。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性が促進されます。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の属性の値を指定したい場合に使用できます。

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

- **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に公開する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 ADM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。

次の図は、StyleBook の簡単な概要を示しています。

次の例は、StyleBook の文法と構造、および複雑さのレベルを上げて StyleBook を記述する方法について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
- 基本的な負荷分散構成を作成するためのStyleBook
- 複合StyleBookを作成する
- GUI属性を使用してStyleBookをカスタマイズする

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は、ユーザー定義の値を受け入れます。つまり、これらはStyleBookのパラメータです。

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"
```

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

```
version: "0.1"
```

ヘッダーセクションには、次の詳細が含まれています。

- **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® ADMに表示されます。
- **display-name**: NetScaler ADMに表示されるStyleBookの記述的な名前。
- **namespace**: 名前衝突を避けるために、StyleBookの一意の識別子の一部を形成する名前空間。
- **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。

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 ADM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の名前空間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:

 -
```

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

```
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、名前空間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を参照するために名前空間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以降の任意の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するために使用できるようにするため、Citrixは、最大限の互換性のために、Nitro組み込みStyleBookを直接使用するStyleBook（名前空間：netscaler.nitro.config、バージョン：10.5）にNitro 10.5名前空間をインポートすることを推奨します。

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バージョンのNitroに基づいている必要があります。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名前空間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なく、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、その依存関係の階層内で常に最高のNitroバージョンを取得するため、そのバージョン以降のNetScalerを構成するために使用できます。

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

パラメータ

パラメータセクションでは、StyleBookで必要となるすべてのパラメータを宣言できます。StyleBook開発者として、StyleBookのユーザーにどのような入力を指定してもらいたいか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が提供する必要があるようにStyleBookを構築しています。

パラメータセクションは次のようになります。

```
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
```

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

```
  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
```

注

パラメータのラベルを指定しない場合、NetScaler ADMはこのパラメータを表示する際にname属性を使用します。NetScaler ADMでの表示方法を制御できるように、パラメータには常に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、パラメータはその名前で指定されます。
このセクションでは、**name** 属性値で示される3つのパラメータを宣言しました。仮想サーバー名には **name**、仮想サーバーのIPアドレスには **ip**、ロードバランシング方式には **lb-alg** です。

- **type**。これらのパラメータが取りうる値の型。例えば、nameとlb-algは文字列値を取ることができ、ip値はIPアドレス型である必要があります。StyleBookのパラメータは、以下のいずれかの組み込み型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属性を使用して、文字列型の長さを制限できます。
- **number**。整数。min-value属性とmax-value属性を使用して、この型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も注意してください（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。

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

- **password**。不透明/秘密の文字列値。NetScaler ADMがこのパラメータの値を表示する場合、アスタリスク（*****）として表示されます。
- **certfile**。証明書ファイル。
- **keyfile**。証明書秘密鍵ファイル。
- **file**。この型のパラメータは、ユーザーがファイル（例：証明書ファイルやキーファイル）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、これらの各要素はパラメータです。この型は、複数の関連するパラメータを1つの親パラメータ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、そのパラメータは必須であり、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はオプションです。この例では、**name** と **ip** は必須パラメータであり、**lb-alg** はオプションパラメータで、そのデフォルト値は「ROUNDROBIN」です。

default 属性を使用して、オプションパラメータ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 ADMはこれら3つのパラメータを含むフォームを表示します。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、ROUNDROBINがデフォルト値として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必要があ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。

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

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: HTTP

   ipv46: $parameters.ip

   port: 80

   lbmethod: $parameters.lb-alg
```

この例には、コンポーネントが1つだけ含まれています。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2つ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るため、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。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。
- **複合タイプ**。このタイプは、NetScaler ADMに作成およびインポートしたStyleBook、またはNetScaler ADMに付属しているデフォルトのStyleBookです。複合StyleBookの作成で、複合StyleBookの詳細を確認できます。

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ネームスペース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」はこのネームスペース内の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。

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

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、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、「ns」プレフィックスは「import-stylebooks」セクションでNetScaler Nitroネームスペース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でも同じ慣例を使用することを推奨しています。

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。Citrixは、StyleBooks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推奨しています。

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
```

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

```
   version: "10.5"
   prefix: ns
  -
   namespace: com.citrix.adc.stylebooks
   version: "1.0"
   prefix: stlb


parameters:
 -
   name: name
   label: "Application Name"
   description: "Give a name to the application configuration."
   type: string
   required: true
  -
   name: vip-ipaddress
   label: "Load Balancer IP Address"
   description: "The Application VIP that clients access"
   type: ipaddress
   required: true
  -
   name: lb-alg
```

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

```
  label: LB Algorithm

  description: Load Balancing Algorithm

  type: string

  default: ROUNDROBIN

  allowed-values:

   - ROUNDROBIN

   - LEAST-CONNECTION



components:

 -

  name: lbvserver-comp

  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler load balancing virtual server configuration object.

  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 ADM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。

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

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、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。

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、まずヘッダーセクションを更新する必要があります。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を適切に記述するために**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セクションは変更されません。Nitro構成オブジェクトを使用するために、netscaler.nitro.config名前空間を参照します。

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

```
import-stylebooks:

 -

 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

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は同じままです。

```
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
```

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

```
  -

   name: lb-alg

   type: string

   label: LoadBalancing Algorithm

   description: Choose the load balancing algorithm used for load
balancing client requests between the application servers.

     allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

      default: ROUNDROBIN

  -

   name: svc-servers

   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.
```

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

```
    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**が追加されています。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。

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
```

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

```
  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)
   servicegroupname: $parent.properties.name
```

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

この例では、元のコンポーネント**lbvserver-comp**（前の例から）に、**svcg-comp**という子コンポーネントが追加されました。そして、**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。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は、親コンポーネントの属性を参照して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オブジェクトごとに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、servicetypeに静的な値を指定し、nameは入力パラメーターから値を取得します。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。

最初のサブ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) の間に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に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**コンストラクトを使用して、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**コンストラクトではsrvとして参照されます）に対して**servicegroup_servicegroupmember_binding**タイプの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。

一般に、コンポーネント内で**repeat**および**repeat-item**コンストラクトを使用すると、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**コンストラクトに変数名（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。

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

上記の例では、この構成を簡単に構築するために、コンポーネントを相互にネストして使用しました。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、ネストせずに同じ結果を達成することもできました。

```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup\_servicegroupmember\_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   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:
```

© 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:
   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にあり（つまり、ネストされていません）、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、コンポーネント**svcg-comp**と**lbvserver-comp**は、最後に宣言されていますが、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。

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

出力

新しいStyleBookに追加できる最後のセクションは、outputsセクションです。ここでは、構成の作成に使用された後、このStyleBookがユーザー（または他のStyleBook）に何を公開するかを指定します。たとえば、outputsセクションで、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指定できます。

```
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のoutputs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を作成する際にわかるように、このStyleBookをインポートするすべてのStyleBookに柔軟性をもたらします。

注

outputsセクションでは、コンポーネントの単一のプロパティだけでなく、StyleBookのコンポーネント全体を公開することをお勧めします（たとえば、$components.lbvserver-comp.properties.nameという名前だけでなく、$components.lbvserver-comp全体を公開するなど）。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。

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

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。Citrixは、StyleBooksページの組み込み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推奨しています。

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"

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
```

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

```
  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true

 -

  name: lb-alg

  type: string

  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
```

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

```
  description: The IP addresses of all the servers of this application
  required: true


components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP


 -
  name: lbvserver-svg-binding-comp
```

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

```
  type: ns::lbvserver_servicegroup_binding

  properties:

   name: $components.lbvserver-comp.properties.name

   servicegroupname: $components.svcg-comp.properties.servicegroupname

 -

  name: members-svcg-comp

  type: ns::servicegroup_servicegroupmember_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

   ip: $srv

   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
```

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

```
  description: The component that builds the Nitro servicegroup
configuration object
```

構成を作成するためにStyleBookの使用を開始するには、NetScaler ADM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にインポートして、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組み込みStyleBookと同様に、2番目のStyleBookのコンポーネントによって使用される**タイプ**として参照できます。

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を作成する

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
```

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

```
    version: "10.5"
    prefix: ns
  -
    namespace: com.example.stylebooks
    version: "0.1"
    prefix: stlb
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: svc-servers
    type: ipaddress[]
```

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

```
    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true



  -

    name: response-code

    type: string[]

    label: List of Response Codes

    description: List of Response Codes - Provide a list of response codes
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
```

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

```
    type: ns::lbmonitor

    description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.

    properties:

      monitorname: $parameters.name + "-mon"

      type: HTTP

      respcode: $parameters.response-code

      httprequest: "'GET /'"

      lrtm: ENABLED

      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、「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、

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

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、および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 ADM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 ADM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。

Citrixでは、YAMLコンテンツを検証およびインポートするために、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

StyleBookのパラメータセクションにGUI属性を追加すると、NetScaler® Application Delivery Management (ADM) に表示されるフィールドを直感的にすることができます。

例。label属性を使用してパラメータの記述的な名前を追加し、description属性を使用してこのパラメータのツールヒントを追加できます。

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.

type: ipaddress
```

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

```
required: true
```

例。タイプがオブジェクト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列で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:

 collapse_pane: true

 columns: 2
```

例。NetScaler ADM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。StyleBookをプライベートとしてマークして、NetScaler ADM 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します。

```
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"
```

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

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® Application Delivery Management (ADM)にインポートする必要があります。NetScaler ADMでは、単一のStyleBookをYAML形式でインポートするか、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 ADM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 ADMには、StyleBook 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エディターも搭載されています。YAMLエディターを使用すると、NetScaler ADM GUI自体から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 ADM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。

- **色分け表示**。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、ADM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。コードの正確性や誤植は検証しません。

StyleBookをインポートするには

1. NetScaler ADM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。

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

- **バンドル** - NetScaler ADM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。

  StyleBookバンドルをインポート(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebooks-yaml-editor-5-citrix.png)

  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、次の操作を行います。

  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`ファイル内でStyleBookとアイコンを次のようにマッピングします。

  ```
  <StyleBook file name> : <icon file name>
  ```

  以下はStyleBookバンドルの例です。

  アイコン付きStyleBookバンドル(/en-us/netscaler-application-delivery-management-software/media/stylebook-icons-bundle.png)

  `resources`フォルダには必要なアイコンが含まれています。

  リソースフォルダ内のアイコン(/en-us/netscaler-application-delivery-management-software/media/stylebook-resources-folder.png)

  この例では、`sharepoint.yaml`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"

  }
  ```

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

`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が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

  独自のStyleBookの作成方法の詳細については、「独自のStyleBookを作成する方法」を参照してください。

- **リポジトリの同期** - このオプションには、ADMに追加されたリポジトリが一覧表示されます。ADMと同期するリポジトリを選択します。

注

StyleBook YAMLファイルからYAMLエディターにコンテンツをコピーして貼り付けることもできます。

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。

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

NetScaler ADM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 ADM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 ADM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が検証テストに失敗した場合でも、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はユーザーインターフェイスページとして開かれ、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。

6. パラメーターに必要な値を指定します。

   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「**負荷分散アルゴリズム**」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) 構成オブジェクトをテストする場合は、「**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。

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

この例では、StyleBookはタイプ `lbvserver` 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、「**構成**」ページに新しい構成パックが表示されます。

「

注

」

リフレッシュアイコンをクリックすると、NetScaler ADMで最近検出されたNetScalerインスタンスを、このウィンドウで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の検索

NetScaler ADM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 ADM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、次にサブリストから **Custom** を選択します。
4. NetScaler ADMには、ユーザー定義のStyleBookのみが表示されます。

構成パックを作成および編集する

NetScaler® Application Delivery Management (ADM) 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 に関連付けられています。構成パックへの更新は、関連付けられている StyleBook を介して行われます。

構成パックを作成する

StyleBook から構成パックを作成するには、次の手順を実行します。

1. **Applications > StyleBooks > Configurations** に移動します。
2. **Add** をクリックします。

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

3. **Choose StyleBooks** で、構成パックを作成するのに必要な StyleBook を選択します。

   このページでは、StyleBook をデフォルトとカスタムの StyleBook に分類しています。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、必要な詳細を指定します。

   GUI フィールドは StyleBook ごとに異なります。

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**
   >
   > 必要に応じて複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 > Configurations** 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。

構成パックの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。古いStyleBookを使用して構成パックをすでに作成している場合は、新しい更新されたStyleBookを使用するように更新したい場合があります。新しいStyleBookを使用するには、構成パックの既存のStyleBookを変更します。

ADC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から構成パック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は、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。

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

StyleBookを作成したら、既存の構成パック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を変更する構成パックを選択します。

   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。

   設定パックのStyleBookを変更すると、新しいStyleBookのパラメータは、既存のStyleBookとは異なる構造を持つ場合があります。パラメータ構造が以前のStyleBookと類似している場合、パラメータの値はそれぞれのフィールドに自動的に保持されます。それ以外の場合、2つのStyleBook間で同じ構造を持つパラメータのみが転送されます。例えば、同じパラメータ名、タイプ、パラメータの親などです。

   - 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の設定ページに表示されるパラメータは次のとおりです。

   - 新しい**example-lb-mon** StyleBookの設定ページに表示されるパラメータは次のとおりです。

   - 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設定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。
8. **OK**をクリックします。

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

StyleBook > 構成ページで、**StyleBook名**列には、選択した設定パックの新しいStyleBook名が表示されます。この場合、**example-lb-mon**と表示されます。

複数の設定パックを持つStyleBookを変更する

複数の設定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ADM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構成パックのStyleBookを変更します。

   選択した構成パックが同じ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。

   同じStyleBookに関連付けられている構成パックを選択します(/en-us/netscaler-application-delivery-management-software/media/change-sb-multiple-citrix.png)

   選択した構成パックの場合、ADMは次の条件が満たされたときに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。

   選択した構成パックの進行状況を確認するには、**構成**ページで**進行中/失敗した構成**を選択します。

   構成パックの進行状況ステータス(/en-us/netscaler-application-delivery-management-software/media/configuration-pack-progress-failed-citrix.png)

3. すべての構成パックが新しいStyleBookに紐付けられたら、古いStyleBookをADMから削除します。

構成パックのエクスポートまたはインポート

StyleBookと同様に、構成パック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ADMサーバーに簡単に共有できます。構成パック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、構成パック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。

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

構成のエクスポート

構成パック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. エクスポートする構成パックを選択します。
3. 「**Select Action**」で、「**Export Configuration**」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-citrix.png)
4. 「**Export Configuration**」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、ターゲットインスタンスの情報がエクスポートバンドルに含まれます。
   - **構成に関連付けられている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。
   - **圧縮ファイルタイプ**: **ZIP**または**TGZ**ファイルタイプを選択します。

   構成パックのエクスポート(/en-us/netscaler-application-delivery-management-software/media/export-configuration-options-citrix.png)
5. 「**Export**」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ADMサーバー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。

1. 「**Applications > StyleBooks > Configurations**」に移動します。
2. 「**設定のインポート**」を選択します。

   設定のインポートオプション(/en-us/netscaler-application-delivery-management-software/media/import-configuration-citrix.png)
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。

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

5. オプションで、で、**すべての構成オブジェクトがADCにすで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、ADCインスタンスにすでに作成されているオブジェクトを変更しません。

   同じADCインスタンスを2つのADMサーバーに追加したとします。そして、あるADMサーバーから別のサーバーに構成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、ADCインスタンス上の構成オブジェクトを変更せずに構成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、指定された構成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。構成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、構成を移行します。
6. 「**インポート**」をクリックします。

設定のインポート(/en-us/netscaler-application-delivery-management-software/media/import-configuration-options-citrix.png)

構成パックをインポートすると、ADM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ADMにない場合、構成パックとともに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構成を展開します。ADMに記載されているADCインスタンスがない場合、構成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ADM**: 同じADMサーバーで構成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構成パックを更新します。

構成パックからターゲットインスタンスをデタッチする

構成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 > 構成 > 設定パック** に移動します。
2. 削除するターゲットインスタンスを含む構成パックを選択します。
3. **Select Action** で、**Detach Targets** を選択します。
4. **Detach Targets** ペインで、構成パックから削除するターゲットインスタンスを選択します。

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

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重複構成パックの作成を確認するメッセージが表示されます。

StyleBook を構築する

example-lb StyleBook の全内容は、参考として以下に示します。

```
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:

  -

    name: lb-comp

    type: stlb::lb
```

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

```
    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、参考として以下に示します。

```
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

    prefix: stlb

    version: "1.0"

  -
```

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

```
    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

    properties-default-sources:

      - $parameters

  -
```

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

```
    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-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

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

NetScaler® ADM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 ADM) StyleBookを使用すると、NetScaler ADM 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インスタンスに任意の種類のファイルをアップロードする際に、NetScaler構成を作成できます。これらのファイルは、証明書ファイルや地理位置情報ファイルなどの例です。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て静的近接性を定義するためのGSLB構成で使用されます。

StyleBookを作成する - 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

 version: "11.1"

 prefix: ns
```

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

```
parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
ADM

 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)
```

注

この例で使用されているパラメータはファイルタイプです。このStyleBookをNetScaler ADM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 ADM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 ADMにすでにコピーしている場合など）。NetScaler ADMファイルシステムに最初にコピーせずにNetScaler ADMを介してNetScalerにファ

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

イルをアップロードしたい場合は、2つの「string」パラメータを持つ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、もう1つはファイルの内容を指定するためのもので、これらの2つのパラメータをupload-file-compコンポーネントで使用します。以下は、地理位置情報ファイルをアップロードするための代替StyleBookです。

StyleBookを作成する - 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



parameters:

 -

  name: filename

  label: Location Filename

  description: The name of the location file on the NetScaler
```

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

```
    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: $parameters.filename
      filelocation: "/var/NetScaler/inbuilt_db/"
      filecontent: base64.encode($parameters.filecontents)
```

ファイルをアップロードするための構成の作成

次の手順では、上記で説明した最初のStyleBookを使用して地理位置情報ファイルをアップロードする構成を、選択したNetScalerインスタンス上に作成します。

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：

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

1. NetScaler ADM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 ADM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、インポートしたStyleBookを選択します。

   StyleBook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。
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 ADMでは、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 ADM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

Citrixでは、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/

注

更新アイコンをクリックして、NetScaler ADMで最近検出されたNetScalerインスタンスを、このウィンドウで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。

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

NetScaler ADM APIを使用して構成パックを作成する

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ために、NetScaler ADM 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、「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ためのAPIの使用方法」を参照してください。

NetScaler ADM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 ADM 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 ADM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ために、NetScaler ADM APIを使用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 - **Load Balancing Virtual Server (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 ADM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

 -

  name: ip

  type: ipaddress
```

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

```
  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"

  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。

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

- 「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。「stlb」プレフィックスは、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と、「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 ADM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

   lbmethod: $parameters.lb-alg

 -

  name: lbvserver-certificate-comp

  type: stlb::vserver-certs-binds
```

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

```
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 ADM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 ADM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 ADM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

次の手順では、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 ADM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。

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 ADMで、**Applications** > **Configuration > StyleBooks** に移動します。**StyleBooks** ページには、NetScaler ADMで利用可能なすべてのStyleBookが表示されます。
2. スクロールダウンして **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。

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

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 ADM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 ADM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。

NetScaler ADMでは、NetScaler ADM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証明書を使用する独自のStyleBookを作成することもできます。

StyleBookを構築する

ファイルlb-vserver-ssl.yamlの全内容は以下のとおりです。

```
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"
```

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

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
```

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

```
   type: string

   allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

   default: ROUNDROBIN

  -

   name: certificate

   label: "SSL Certificate File"

   description: "The file name of the SSL certificate file"

   type: certfile

  -

   name: key

   label: "SSL Certificate Key File"

   description: "The file name of the server certificate's private key
file"

   type: keyfile



components:

  -

   name: my-lbvserver-comp

   type: ns::lbvserver

   properties:
```

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

```
    name: $parameters.name

    servicetype: SSL

    ipv46: $parameters.ip

    port: 443

    lbmethod: $parameters.lb-alg

-

 name: lbvserver-certificate-comp

 type: stlb::vserver-certs-binds

 description: Binds lbvserver with server certificate

 properties:

  vserver-name: $ components.my-lbvserver-comp.properties.name

  certificates:

   -

    cert-name: $parameters.name + "-lb-cert"

    cert-file: $parameters.certificate

    ssl-inform: PEM

    key-name: $parameters.name + "-key"

    key-file: $parameters.key
```

NetScaler ADM API を使用して構成パックを作成する

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ために、NetScaler ADM 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。

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

NetScalerインスタンスで定義されたオブジェクトの表示

NetScaler ADMでStyleBook構成パックが作成された後、ターゲット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するには、**作成されたオブジェクトを表示**をクリックします。

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

オペレーションコンストラクトを使用すると、NetScaler ADMアナリティクスが、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トラフィックトランザクションのすべてまたは一部でAppFlowレコードを収集するように構成できます。このコンストラクトを使用して、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ためにアラームを構成することもできます。

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:
```

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

```
      target: $outputs.lbvserver

      email-profile: $parameters.emailprofile

      sms-profile: "NetScalerSMS"



    rules:

     -

      metric: "total_requests"

      operator: "greaterthan"

      value: 25

      period-unit: $parameters.period

     -

       metric: "total_bytes"

       operator: "lessthan"

       value: 60

       period-unit: "day"
```

The attributes in the analytics section are used to instruct NetScaler ADM analytics feature to collect appflow records on a virtual server component identified by the target property. You can also optionally specify a filter property that accepts a NetScaler policy expression to filter requests for which appflow records are collected on the virtual server.

When a configuration pack is created from this StyleBook, the NetScaler ADM analytics feature is configured to collect appflow records on the virtual servers that were specified when these are created in the process of creating a configuration pack.

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-

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

profileおよびsms-profileプロパティを使用して、通知の送信先を指定します。ルール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の場合、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際に、次の演算子を使用できます。

- 「>」には「greaterthan」を使用します
- 「<」には「lessthan」を使用します
- 「greaterthanequal」は「>=」に対応する
- 「lessthanequal」は「<=」に対応する

StyleBookは、メトリックにAPI名を使用し、NetScaler ADMアナリティクスGUIに表示される名前ではない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 ADMアナリティクスドキュメントを参照してください。

インスタンスの役割

NetScaler Application Delivery Management (ADM)では、単一のアプリケーションに対して複数のNetScalerインスタンスを構成する必要がある一方で、各ADC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。

StyleBook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ADC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。

StyleBookの「インスタンスの役割」機能を使用すると、非対称構成、つまり複数のADCインスタンスに適用できるが、異なるADCインスタンスには異なる構成を持つ構成パックを作成できます。

インスタンスの役割機能を持つ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ADCインスタンスに異なる役割を割り当てることができます。この役割によって、ADC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が決まります。

注意点:

- StyleBookにおけるインスタンスの役割のセットは、StyleBookの作成時に定義されます。

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

- 役割は、構成パックの作成または更新時に特定のADC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「ターゲットロール」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役割が宣言されます。

このセクションは通常、StyleBookの「import-StyleBooks」セクションの後、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、「ターゲットロール」セクション内で2つの役割（AとB）が定義されています。

```
target-roles:



  -

   name: A

   name: B

     min-targets: 2

     max-targets: 5
```

役割Bには、オプションの2つのサブプロパティ、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役割を割り当てる必要があるADC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役割を割り当てることができるADC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、その役割に構成できるADCインスタンスの数に制限はありません。min-targets = 0の場合、その役割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ADCインスタンスがその役割に構成される必要があります。

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

ロール「default」

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。構成パックを作成する際、ADC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構成オブジェクトを受け取ります。

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、それらのロールは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ADC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ロール属性を指定できます。コンポーネントの以下の例で示します。

```
-

  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。コンポーネントのロール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。

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

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構成オブジェクトは、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。この機能を効果的に使用して、構成パックのすべてのインスタンスに適用できる構成オブジェクトを作成できます。

ロールAとBの2つのロールが定義されており、4つのコンポーネントを含むStyleBookがあると仮定します。

- 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
- 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
```

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

```
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
```

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

```
      name: lb4

      servicetype: HTTP

      ipv46: 14.14.14.14

      port: 80
```

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、コンポーネントが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を使用して構成パックを作成し、5つのADCインスタンスにデプロイするとします。この段階で、次のようにインスタンスにロールを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まとめたもので、各ADC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。

設定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ADCインスタンスで作成される設定オブジェクトを表示および確認することもできます。

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"
```

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

```
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
```

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

```
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
```

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

```
    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
```

次の図は、サンプル設定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、設定パックの作成または更新時に、各ADC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。

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

```
"targets": [

            {

             "id": "<ADC-UUID>",

             "roles": ["A"]

            },

           ]
```

完全なサンプルREST APIを参考として提供します。

POST /`<ADM-IP`>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]

        },

        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",

          "roles": ["A", "B"]
```

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

```
        },
        {
          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
        },
        {
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```

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により、NetScaler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。これは、「望ましい状態」を指定するときに行われます。

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

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

きます。同様に、NetScaler certkey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」操作をサポートしています。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、非CRUD操作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、certkey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。

非CRUD操作のサポート

「properties」コンストラクトと同じレベルのコンポーネントに、「meta-properties」と呼ばれる新しいコンストラクトが追加されました。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
```

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

```
    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netscaler.nitro.config名前空間とバージョン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は最初にStyleBookによって作成され、その後「enable」操作が実行されます。

メタプロパティ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。

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の構成パックを別のStyleBookに移行する

NetScaler® Application Delivery Management (ADM)では、構成パックは常に作成元のStyleBookにバインドされます。構成パックへの更新は、その構成パックがバインドされているStyleBookを介してのみ実行できます。NetScaler ADMでは、既存の構成パックを新しいStyleBookに移行できるようになりました。新しいStyleBookは、構成パック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、構成パックをまったく異なる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インスタンス上に構成パック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。

これで、構成パック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、構成にモニターを追加するために、構成パックCP1を削除し、新しいStyleBookから構成パックCP2を作成する必要がありました。CP1を削除すると、1つ以上のNetScalerインスタンス上の構成パック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を介して新しい構成パックを再作成する必要がありました。

代わりに、既存の構成パック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。構成パックが展開されたNetScalerイ

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

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。

構成パックの移行

example-lb StyleBookを使用して作成された構成パックをexample-lb-mon StyleBookに移行するには

1. NetScaler ADM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構成パックが表示されます。
2. 以前に作成した**example-lb**構成パック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 ADM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、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、次の画像はexample-lb StyleBookのパラメーターを示しています。

   次の画像は、構成パックを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。ただし、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。必要に応じて複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。

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

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規作成、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 ADMでのみ利用可能です。

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。この場合も、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かもしれません。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。ただし、NetScaler ADM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、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"
```

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

```
import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

example-lb-mon StyleBookの全内容は、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
```

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

```
schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

  -

    namespace: com.citrix.adc.commontypes

    prefix: cmtypes

    version: "1.0"

parameters-default-sources:

  - stlb::lb

parameters:

  -

    name: monitors

    label: "List of Monitors"

    description: "List of Monitors to monitor Application Servers"

    type: cmtypes::monitor[]
```

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

```
substitutions:

  mon-name(appname, monname): $appname + "-mon-" + $monname

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    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,
```

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

```
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

API を使用して StyleBook から構成を作成する

StyleBook を構築したら、NetScaler ADM または NetScaler ADM API を使用して、NetScaler® Application Delivery Management (ADM) にインポートする必要があります。NetScaler ADM は、インポート時に StyleBook を検証し、検証が成功すると、StyleBook は NetScaler ADM 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 ADM 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 を検討します。この StyleBook から REST API を使用して構成パックを作成するには、次のようにします。

```
POST



https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/lb-vserver/configpacks
```

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

```
Content-Type: application/json

Accept: application/json

{

  "configpack":

  {

    "parameters": {

      "name": "lb1",

      "ip": "10.102.117.31"

    },

    "target_devices":

    [

      {

        "id": "deecee30-f478-4446-9741-a85041903410"

      }

    ]

}

}
```

この HTTP リクエストでは、id (例: 「deecee30-f478-4446-9741-a85041903410」) 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 が作成される NetScaler インスタンスのインスタンス ID です。NetScaler インスタンスのインスタンス ID は NetScaler ADM から取得されます。

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

NetScaler ADM 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 ADM API を使用できます。たとえば、IP アドレスが 192.168.153.160 の 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。

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address:192.168.153.160
```

```
Accept: application/json
```

応答にはペイロード内の ID が含まれています。

```
200

OK

Content-Type: application/json

{

  "errorcode": 0,

  "message": "Done",

  "operation": "get",

  "resourceType": "ns",

  "username": "nsroot",

  "tenant_name": "Owner",

  "resourceName": "",

  "ns":

  [

    {

    "is_grace": "false",

    "hostname": "",
```

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

```
    "std_bw_config": "0",
    "gateway_deployment": "false",
    …"id": "deecee30-f478-4446-9741-a85041903410",
    ...
   }
 ]
}
```

構成パックが正常に作成されると、次の HTTP 応答が受信されます。

```
200 OK
Content-Type: application/json
{
  "configpack":
  {
    "config_id": "1460806080"
  }
}
```

id 1460806080 を使用して一意に識別される最初の構成パックを作成しました。この ID を使用して、構成を照会、更新、または削除できます。

例 2

同じ StyleBook を使用して別の構成パックを作成し、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、別の構成を作成し、仮想サーバーに異なる名前と IP アドレスを指

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

定し、ロードバランシング方法として LEASTCONNECTION を指定します。この構成を 2 つの NetScaler インスタンスに展開します。

HTTP リクエストは次のとおりです。

```
POST



https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/lb-vserver/configpacks
```

```
Content-Type: application/json

Accept: application/json

{

  "configpack":

  {

    "parameters":

    {

      "name": "lb2",

      "ip": "10.102.117.32",

      "lb-alg": "LEASTCONNECTION"

    },

    "target_devices"

    [

     {"id": "deecee30-f478-4446-9741-a85041903410"},

     {"id": "debecc60-d589-4557-8632-a74032802412"}
```

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

```
    ]

  }

}
```

この HTTP リクエストでは、IP アドレス 10.102.117.32 を持つロードバランシング仮想サーバー lb2 が、ID 「deecee30-f478-4446-9741-a85041903410」と「debecc60-d589-4557-8632-a74032802412」で表される 2 つの NetScaler インスタンス上に作成されます。

構成パックが正常に作成されると、次の HTTP 応答が受信されます。

```
200 OK

Content-Type: application/json

{

   "configpack":

  {

     "config_id": "1657696292"

  }

}
```

この新しい構成パックには、異なるID 165769629 があります。このIDを使用して、この構成を更新または削除できます。

例 3

StyleBook to Create a Basic Load balancing Configuration で作成した「basic-lb-config」StyleBook を検討してください。このStyleBookからREST APIを使用して構成パックを作成するには、次のようにします。

```
POST
```

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

```
http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/basic-lb-config/configpacks
```

```
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

    },

    "target_devices":

    [

     {

      "id": "deecee30-f478-4446-9741-a85041903410"

     },

     {

      "id": "debecc60-d589-4557-8632-a74032802412"
```

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

```
     }

    ]

  }

}
```

このHTTPリクエストでは、ロードバランシング構成が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

Create a Composite StyleBook で作成した複合StyleBook **composite-example** を検討してください。このStyleBookからREST APIを使用して構成パックを作成するには、次のようにします。

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/composite-example/configpacks
```

```
Content-Type: application/json

Accept: application/json

{

  "configpack":

  {

    "parameters": {

      "name": "myapp",

      "ip": "2.2.2.2",

      "svc-servers": ["10.102.29.52","10.102.29.53"]

    },

    "target_devices":
```

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

```
    [
    {
      "id": "deecee30-f478-4446-9741-a85041903410"
    },
    {
      "id": "debecc60-d589-4557-8632-a74032802412"
    }
    ]
 }
}
```

このHTTPリクエストでは、構成は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オンすると、「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構成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。

構成パックが正常に作成されると、次のHTTP応答が受信されます。

```
200 OK
Content-Type: application/json{
  "configpack": {
    "config_id": "4917276817"
  }
}
```

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

構成の更新

この構成を更新するには、たとえば、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をロードバランシング仮想サーバー myapp に追加する場合、構成パックを更新するためのAPIを次のように使用します。

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
Content-Type: application/json

Accept: application/json

{

  "configpack": {

    "parameters": {

      "name": "myapp",

      "ip": "2.2.2.2",

      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]

  },

  "target_devices":

  [

    {

    "id": "deecee30-f478-4446-9741-a85041903410"

    },

  {

    "id": "debecc60-d589-4557-8632-a74032802412"

  }
```

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

```
]

}

}
```

構成パックが正常に更新されると、次のHTTP応答が受信されます。

```
200 OK

Content-Type: application/json

{

   "configpack": {

     "config-id": "4917276817"

  }

}
```

構成の削除

この構成（すべてのNetScalerインスタンスから）を削除するには、構成パックを削除するためのAPIを次のように使用します。

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/
com.example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
Accept: application/json
```

構成パックが正常に削除されると、次のHTTP応答が受信されます。

```
200 OK

Content-Type: application/json

{
```

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

```
   "configpack": {

     "config_id": "4917276817"

  }

}
```

NetScalerインスタンスにログオンして、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できます。

すべてのNetScaler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したい場合は、上記の構成パック更新操作を使用し、JSONペイロードの「target_devices」属性を変更して、特定のNetScalerインスタンスIDを削除します。

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

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® Application Delivery Management (ADM)にHTTPリクエストを送信できます。

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ための StyleBookを作成する方法で作成した、証明書ファイルとキーファイルをアップロードするStyleBookの例を検討してください。このStyleBookからREST APIを使用して構成パックを作成するには、次の手順に従います。

```
POST



https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/
com.citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
```

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {
```

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

```
        "lb-appname": "lbmon",
        "lb-virtual-ip": "13.1.11.10",
        "lb-virtual-port": "80",
        "lb-service-type": "HTTP",
        "svc-service-type": "HTTP",
        "svc-servers": [
            {
                "ip": "14.1.1.15",
                "port": "80"        }
    ],
        "certificates": [
            {
                "cert-name": "server_cert",
                "cert-file": "server_cert.pem",
                "ssl-inform": "PEM",
                "key-name": "server_key",
                "key-file": "server_key.pem",
                "cert-password": "secret",
                "cert-advanced": {
                    "is-ca-cert": false,
                    "skip-ca-name": false
        }
```

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

```
        }
    ],
        "lb-advanced": {
            "flush-on-state-down": "ENABLED",
            "auth-params": {
                "authentication": "OFF",
                "authentication-http-401": "OFF"
        },
            "appflow-log": "ENABLED",
            "algorithm": "LEASTCONNECTION"
    },
        "svcg-advanced": {
            "svc-client-ip": "DISABLED",
            "svc-use-source-ip": "NO",
            "svc-use-proxy-port": "NO",
            "svc-surge-protection": "OFF",
            "svc-client-keepalive": "NO",
            "svc-tcp-buffering": "NO",
            "svc-compression": "NO",
            "svc-state": "ENABLED",
            "svc-downstate-flush": "DISABLED",
            "svc-enable-health-monitor": "NO"
```


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

```
      }

    },

       "targets": [

           {

               "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"

      }

    ]

  }

}
```

この構成パックは、ID 8c158e7a-0087-423f-91b0-0ccf16de552a 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、証明書ファイルとキーファイルはNetScaler ADM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、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

NetScaler Application Delivery Management (ADM) 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。

NetScaler MA ServiceにファイルをアップロードするStyleBookを作成する方法で、任意の種類の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。上記のトピックの例と同様に、構成パックを作成し、パラメーター「locationfile」の値をNetScaler ADM上のロケーションファイルのファイルパスとして指定します。 このStyleBookからREST APIを使用して構成パックを作成するには、次の手順に従います。

```
POST
```

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

```
https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/
com.citrix.adc.stylebooks.samples/1.0/upload-geolocations/configpacks
```

```
Content-Type: application/json

Accept: application/json

{

   "configpack":

   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ /
custom_geolocations.csv"

    },

      "targets": [

         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"

      }

    ]

  }

}
```

APIを使用してカスタムStyleBookをインポートする

StyleBook APIを使用して、カスタムStyleBookをNetScaler Application Delivery Management (ADM) にインポート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、REST APIを使用してこのStyleBookから構成パックを次の

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

ように作成します。例えば、NetScalerインスタンス上でロードバランサー構成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/v1/config/stylebooks

Headers:

Content-Type: application/json

Accept: application/json

RequestBody:

{

       "stylebook":

  {

     "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（例: `<https://www.browserling.com/tools/file-to-base64>`）に貼り付けて、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された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、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。

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

ツールでAPIが正常に実行されると、StyleBookがNetScaler® ADM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:

```
{


  "stylebook":
{


    "name": "example-lb",


    "namespace": "com.example.stylebook",


    "version": "1.0"


  }


}
```

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を指定することで、カスタムStyleBookをダウンロードできます。

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

```
GET



https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>/actions/download
```

IPアドレス、名前、バージョン、および名前空間の各フィールドに変更を加えた後、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。

```
GET



https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/
com.example.ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
```

.yaml形式のStyleBookがダウンロードされます。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/mas-api-download-custom-stylebook.png)

APIを使用してカスタムStyleBookを削除する

以下のStyleBooks REST APIを提供することで、カスタムStyleBookを削除できます。

```
DELETE



https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>?dependencies=true
```

URL内のdependenciesクエリパラメータが指定されていないか、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（およびその依存関係）がNetScaler® ADMから正常に削除されたことを意味します。

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

注

MAサービス内に、そのStyleBookに依存する他のStyleBookがある場合、そのカスタムStyleBookを削除することはできません。

たとえば、NetScaler ADMで「lb-virtual-ssl-extended」という名前のStyleBookを作成したとします。その後、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、および名前空間の各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、任意のツールでAPIを実行できます。

DELETE `<https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false>`

- [ ] StyleBookはNetScaler ADMから削除されます。

- [ ]

StyleBooksの文法

独自のStyleBooksを設計し、NetScaler® Application Delivery Management (ADM)にインポートして、NetScaler ADM 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
パラメーター	パラメーター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

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

条件構成要素	繰り返しコンストラクト(/ja-jp/netscaler-application-delivery-management-software/13-1/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/13-1/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	出力(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/outputs.html)
ネストされた繰り返し(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/nested-repeats.html)	親参照(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/parent-reference.html)
パラメータ参照(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/parameter-reference.html)	置換参照(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/substitutions-reference.html)
コンポーネント参照(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/components-reference.html)	操作(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/operations.html)
変数参照(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/variable-reference.html)	アラーム(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/alarms.html)
分析(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/analytics.html)	組み込み関数(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/built-in-functions.html)
式(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/expressions.html)	依存関係の検出(/ja-jp/netscaler-application-delivery-management-software/13-1/stylebooks/stylebooks-grammar/dependency-detection.html)
「インプレース補間」(/ja-jp/netscaler-application-delivery-management-software/	

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

13-1/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>`

- スタイルブック、パラメータ、置換、コンポーネント、プロパティ、出力、親、自身、オペレーション、アナリティクス、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
- ロール、ロール、ターゲット、ターゲット
- コンテキスト、親コンテキスト、親コンテキスト

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行が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。この属性は必須です。
表示名	StyleBookの表示名。この名前はNetScaler ADM 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。この説明はADM 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

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

属性	説明
	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を作成した作成者（個人または組織）。これはオプションの属性です。
名前空間	名前空間は、名前の衝突を避けるために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、またはユニットの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。
バージョン	StyleBookのバージョン番号です。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	StyleBookスキーマのバージョンです。NetScaler ADM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 ADM 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。そのデフォルト値はfalseです。

例:

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

```
    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"
```

システム内でStyleBookを一意に識別するのは、名前、名前空間、およびバージョンの組み合わせです。NetScaler® ADMでは、名前、名前空間、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、名前とバージョンが同じで名前空間が異なる2つのStyleBook、または名前空間とバージョンが同じで名前が異なる2つの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あり、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。これは必須のセクションです。

現在のStyleBookで参照したいStyleBookの**namespace**と**version**番号を宣言する必要があります。いずれかのNITRO構成オブジェクトを直接使用する場合、すべてのStyleBookは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、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するためにStyleBookを使用できることを意味します。

import-stylebooksセクションで使用される**prefix**属性は、namespaceとversionの組み合わせを参照するための短縮形です。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

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

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"
  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を参照するたびに、表記**\<namespace-shorthand\>::\<type-name\>**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で定義されているタイプlbvserver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、表記**stlb::\<stylebook-name\>**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。

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

パラメータ

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、NetScalerインスタンスで構成を作成するためにStyleBookを使用するユーザー向け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® ADMにインポートして構成を作成すると、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」

定義するパラメータの名前。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る必要があり、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、表記 $parameters.\<name> を使用して他のセクションでパラメータを参照できます。

必須ですか？はい

「ラベル」

ADM GUIでこのパラメータの名前として表示される文字列。

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。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、ADM GUIにこのテキストが表示されます。

必須ですか？いいえ

'型'

これらのパラメータが取りうる値の型。パラメータは、以下のいずれかの 組み込み型にすることができます。

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

- 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、文字列型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、この型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0〜128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 ADM 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”: {
```

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

```
        “namespace”: “com.example.stylebook”,

        “version”:“1.0”,

        “name”: “ipnetwork-example”,

        ..

        },

        “parameters”: {

           “name: “test-app”,

            “virtual-ip”: “212.100.30.0/255.255.255.0”,

        },

        “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。ADM GUI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`: 証明書ファイルを表します。この値を使用すると、ADM GUIを使用してStyleBook構成を作成するときに、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、ADM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、ADM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、ADM GUIを使用してStyleBook構成を作成するときに、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

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

す。アップロードされた証明書ファイルは、ADM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、ADM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ーを親要素の下にグループ化する場合に使用します。親パラメーターのタイプを「object」として指定します。「object」タイプのパラメーターには、含まれるパラメーター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ーを使用する場合、このパラメーターは、そのタイプを示すStyleBookで定義されたパラメーターの形式で値を持つことを想定しています。

パラメーターには、タイプのリストである `type` を含めることもできます。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、このパラメーターは文字列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ときに、このパラメーターに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、ADM 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、ADM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。

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

「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、ADM 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` のいずれかを取ることができます。`type: ipaddress` の場合、ADM にある ADM 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。構成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、ADM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。

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 ADM にある ADM 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。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。

「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では、「キー」パラメータとして定義できるパラメータは1つだけです。

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ADCインスタンス上）、各構成にはこの パラメータに対して異なる/一意の値が設定されます。

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

「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、構成を作成する際にユーザーは このパラメータの値を指定する必要があります。

ADM GUIは、このパラメータ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。

必須ですか？ いいえ

'許可される値'

タイプが「string」に設定されている場合、この属性を使用して、パラメータの有効な値のリストを定義します。

ADM 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：

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

```
-

      name: TCP Port

      type: tcp-port

      allowed-values:

            -  80

            -  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すると、デフォルト値が使用されます。

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

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提供しません。

例 1:

```
-

      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
```

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

```
      default: 20
```

例 4:

```
-

      name: tcpport

      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、パラメータの型が「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
```

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

```
      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`は正の値でなければなりません。

必須ですか？ いいえ

'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
```

必須ですか？ 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。

値として定義されている文字の最小長が0以上であることを確認してください。

例:

```
-

      name: appname

      type: string
```

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

```
      min-length: 3
```

必須ですか？ 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` で定義されている文字の長さ以上であることを確認します。

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。

最小項目数がゼロ以上であることを確認します。

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。

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

定義されている場合、最大項目数が最小項目数より大きいことを確認します。

例:

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2

      max-items: 250
```

必須? いいえ

'グラフィカルユーザーインターフェース'

この属性を使用して、ADM GUI で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

'列'

この属性は、`gui` 属性のサブ属性です。この属性を使用して、ADM 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、構成の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タイプにのみ設定します。

値が `false` に設定されている場合、構成を更新するときに、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。

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

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:

```
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
```

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

```
      required: true


  -


      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\[\]
```

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

```
    required: true


    parameters:


      -


            name: svc-ip


            label: Server IP


            description: The IP address of the server


            type: ipaddress


            required: true


      -


            name: svc-port


            label: Server Port
```

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

```
            description: The TCP port of the server

            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
```

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

```
            max-items: 3


            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、ADM 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:

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

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two

        - Three
```

「One」、「Two」、「Three」の値がADM 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。

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この属性を指定します。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外観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。

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

例:

```
-

   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、ユーザーは次のいずれかのオプションを選択できます。

- HTTP
- TCP
- UDP

パラメータデフォルトソース構成要素

この構成要素を使用して、他のStyleBookからパラメータ定義を再利用できます。

複数のStyleBookでパラメータまたはパラメータのグループが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** 構成要素を使用することで、その定義をこれらのパラメータを必要とするStyleBookにインポートできます。

例えば、多くのStyleBookで仮想IPを構成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、それに関連するすべてのパラメータをそこで定義できます。

```
-

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。以下に、そのようなStyleBookの例を示します。

```
     -

     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-**

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

sources 構成要素が追加され、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。

インポートされたStyleBookと現在のStyleBookの両方でパラメータが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することに注意してください。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し、残りのインポートされたパラメータはそのまま使用することで、これを効果的に使用できます。

parameters-default-sources構成要素は、示されているように、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同様です。

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

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内で同じ式や値が繰り返し使用される場合（例えば定数値など）にも役立ちます。パラメータに置換名を使用すると、StyleBook内のパラメータ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。

次の例では、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、そのポート番号が使用される回数に関係なく、StyleBookの1か所で定義できます。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場所で変更が有効になります。

次の例は、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"

          servicetype: HTTP

          ipv46: $parameters.ip
```

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

```
          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。次の例は、2つの置換が式をどのように使用するかを示しています。

```
substitutions:

  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS

  app-name: str("acme-") + $parameters.name + str("-app")
```

置換式は、次の例に示すように、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、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

        false: HTTP
```

次の例は、マップ secure-port と secure-protocol の使用方法を示しています。

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

```
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パラメータにブール値「true」を指定するか、NetScaler ADM GUIでこのパラメータ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` プロパティには**SSL**が割り当てられ、`port` プロパティには**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に「false」を指定するか、NetScaler ADM 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、その他の型などの単純な型にすることができます。

置換:

form-lb-name(名前): $名前 + "-lb"

この例では、「form-lb-name」という置換関数が定義されており、これは「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」を接尾辞として追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")`

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

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(優先度): 10100 - 100 &ast; $優先度
```

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。

次は、値がリストである `slist` という置換の例です。

```
substitutions:

  slist:

    - a

    - b
```

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

```
    - 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
```

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、その値自体は別のリストです。

```
  sdictoflist:
    a:
      - 1
```

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

```
    - 2
  b:
    - 3
    - 4
```

コンポーネントでは、これらの置換はcondition、properties、repeat、およびrepeat-conditionの各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内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に、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ーとして受け取り、キーと値のペアを値として生成する関数です。`cs-pools`コンポーネントでは、この置換の値を各プールに対して`lb-pool`パラメーターに割り当てることができます。

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

```
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:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
```

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

```
    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
```

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。

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

```
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。パラメーター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`という置換リストを反復処理して、`lbvserver`コンポーネントのセットと、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

      vport: 80

      protocol: HTTP
```

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

```
      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:
  -
    name: lbvserver-comp
```

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

```
    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"]
            repeat-item: server
            properties:
```

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

```
              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のコンポーネント構成は、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。この構成を使用して、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。

コンポーネント構成は、パラメータ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にはコンポーネント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（-）、またはアンダースコア（_）を含めることができます。

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

属性	説明
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の属性がある場合、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 ADMで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の属性がある場合、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、各StyleBookが最終構成の一部を作成する複数のStyleBookを組み合わせることができます。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に対応します。

例:

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

```
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 (組み込みタイプ) タイプです。「ns」は、import-stylebooks セクションで指定したネームスペース netscaler.nitro.config 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 の各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 のインポートが失敗します。

© 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、それ自体では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と、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インスタンス上でモニター付きロードバランシングサーバー (lb-mon-comp) 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
```

パラメータセクションでは、アプリケーション名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パラメータは、各項目に2つのサブパラメータ（ipとport）を持つオブジェクトのリストを期待します。

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

しかしながら、このStyleBookのパラメータセクションは、$parameters.ipsを介してサーバーIPのみを受け入れます。StyleBookは、すべてのサーバーがポート80で実行されていると仮定します。lb-mon StyleBookを使用してロードバランシング構成を作成するには、$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とポート（静的な80に設定されている）で構成されるオブジェクトを構築します。このように、help-compはIPアドレスのリストをオブジェクトのリストに変換し、これは後で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が式から値を取得することがあります。この式は、パラメーター参照のような単純な式の場合もあれば、より複雑な式の場合もあります。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、そうでない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。

たとえば、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。lbmethodプロパティの値は、以下に示すように、ユーザーが提供するパラメーター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、パラメーター **lb-advanced.algorithm** がオプションのパラメーターであるとします。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ーに値を指定しない場合、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、プロパティ名を「?」で終わらせることで、次のようにプロパティをオプションとして注釈付けできます。

```
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、そ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」で定義されている場合、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-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StyleBook内で既存のパラメータ（他のStyleBookからのもの）の再利用を可能にするのに対し、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の様々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、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来る場合があります。このような場合、StyleBookの他のセクションに存在するプロパティを、コンポーネントの定義内で再定義する必要があります。これは明らかに冗長であり、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、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特定するリストです。

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$parameters.lbオブジェクトから取得されていることに注目してください。これらは単一のソースから取得されているにもかかわらず、プロパティはStyleBookで再度定義されています。さらに、$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が追加された場合、新しいサブパラメータ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、変更が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特定します。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セクション内）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があるべきであることに注意することが重要です。両方を持つこともできます。

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

ネストされたコンポーネント

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することで、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オブジェクトごとに1つ以上のオブジェクトを作成できます。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、コンポーネントが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

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

ビ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 repeat コンストラクトを使用して、パラメーター svc-servers に指定されたサービスリストを反復処理することで実現されます。repeat コンストラクトの詳細については、「Repeat Construct」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、「StyleBook to Create a Basic Load Balancing Configuration」を参照してください。

条件構成要素

条件構成要素を使用すると、コンポーネントを条件付きにすることができます。条件構成要素の値は、trueまたはfalseに評価されるブール式です。条件がtrueの場合、コンポーネントはその構成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、コンポーネントはスキップされ、それを通じて構成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の値を指定した場合、コンポーネントである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しない場合、このパラメータにはnull値が割り当てられ、falseと評価されるため、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（たとえば、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）に基づくことができることに注意してください。

次の例では、条件がtrueと評価された場合、NITROタイプns::systemfileの構成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、この構成オブジェクトをStyleBookによって作成したいと考えています。これにより、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.

Repeat構文

コンポーネントの**repeat**構文を使用して、同じタイプの複数の構成オブジェクトを構築できます。

次の例では、**members-svcg-comp**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サービスグループにサービスリストをバインドするために使用されます。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、パラメータ**svc-servers**に指定されたサービスリストを反復処理するために、**repeat**構文を使用します。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**構文では**srv**として参照されます）に対して、タイプ**servicegroup_servicegroupmember_binding**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

                  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: $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。

- 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。

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

- 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ています。

```
           name: services

           type: ns::service

           repeat:

              repeat-list: $parameters.app-services

              repeat-item: srv

           properties:

               ip: $parameters.app-ip
```

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

```
                port: $parameters.base-port + repeat-index

                servicegroupname: $parent.properties.name
```

repeat-item構文と同様に、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
```

繰り返し条件構成要素

繰り返し条件構成要素は、繰り返し構成要素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、繰り返し条件構成要素の使用法を示しています。

例:

```
components

   -
```

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

```
      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、繰り返し条件式が評価され、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コンストラクトを使用すると、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コンストラクトを含めることができます。2レベルのネストされた繰り返しを考えてみましょう。外側のリスト（最初の繰り返しリスト）の各要素に対して、内側のリスト（2番目の繰り返しリスト）のすべての要素に対して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属性が関連付けられています。repeat-item属性とrepeat-index属性はどちらもオプションです。さらに、各繰り返しはrepeat-conditionも指定できます。

例：

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

```
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: $parameters.vip-ports
              repeat-item: port
      properties:
         name: str("lb-") + str($ip) + '-' + str($port)
         servicetype: HTTP
         ipv46: $ip
```

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

```
        port: $port
```

上記の例では、$parameters.vips の各項目に対して、$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に対して lbvserver 設定オブジェクトを作成します。プロパティセクションでは、IPアドレスとポートの組み合わせに「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。したがって、各反復において、$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。

次の例では、ネストされた繰り返しオブジェクトにおいて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ます。

例：

```
components:
-
     name: lbvservers-comp
     type: ns::lbvserver
     repeat:
         repeat-list: $parameters.vips
         repeat:
            repeat-list: $parameters.vip-ports
     properties:
        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)
```

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

```
        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 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、それをインポートする StyleBook により多くの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	公開する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:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
```

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

```
  -

    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。

パラメータ参照

コンポーネントコンストラクトでは、パラメータセクションで定義されたパラメータを `$parameters.<parametername>` 表記を使用して参照します。 `<parametername>` 自体がパラメータを含む場合（型がオブジェクトの場合）は、 `$parameters.<parametername>.<sub-parametername>` のような表記を使用する必要があります。

例:

```
parameters:

  -

    name: name

    label: Name

    type: string

    required: true

     -

      name: vip

      label: Virtual IP and Port

      type: object
```

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

```
      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:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
```

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

```
      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。例えば、$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:

       -

         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: $parameters.svc-servers
                    repeat-item: srv
                    properties:
                      ip: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
```

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最上位コンポーネントまで上位に移動することもできます。例えば、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。

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

コンポーネントリファレンス

コンポーネント構成では、StyleBook のトップレベルコンポーネントを **$components.\<componentname\>** 表記を使用して参照します。トップレベルコンポーネント内にネストされたコンポーネントがある場合、それらを参照するために **$components.\<componentname\>.components.\<component-name\>** 表記が使用され、以降も同様です。

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

     properties:

          name: $parameters.name + "-svcgrp"

          servicetype: HTTP

  -
```

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

```
    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv

    properties:

       ip: $srv

         port: str($parameters.svc-port)

         servicegroupname: $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、コンポーネント **my-svcg-comp** と **my-lbvserver-comp** は、最後のコンポーネント **lbvserver-svg-binding-comp** を構築する前に構築する必要があります。なぜなら、この最後のコンポーネントにはこれらのコンポーネントへの参照があるからです。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することで提供されます。

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**。

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

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

複数の構成オブジェクトを構築するためにコンポーネントでrepeatおよびrepeat-itemコンストラクトを使用する場合、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、`$\<varname\>` の表記を使用して参照できます。コンポーネントでrepeatコンストラクトがrepeat-itemコンストラクトなしで使用される場合、$repeat-itemというデフォルト変数が反復項目にアクセスするために使用できることに注意してください。

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:

      -

         name: service-members-comp

         type: ns::service
```

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

```
        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、変数名 server-name 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。

オペレーション

オペレーションは、StyleBook のオプションセクションです。このセクションでは、NetScaler Application Delivery Management (ADM) 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は、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 ADM を設定することもできます。

StyleBook を介して NetScaler® ADM を設定し、以下に示すさまざまな NetScaler ADM 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。

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には、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、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。

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

StyleBook を介して NetScaler インスタンスで有効になっている NetScaler ADM 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、クライアント側測定が負荷分散およびコンテンツスイッチング仮想サーバーで有効になります。クライアント側測定が有効になっていると、ADM 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 でオペレーション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

components:

    -

        name: vpnvserver-comp

        type: ns::vpnvserver
```

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

```
        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:

  -

    name: myvpns

    value: $components.vpnvserver-comp
```

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

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 でオペレーション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

        properties:

            name: str("lb-") + str($current-target.ip)

            servicetype: HTTP

            ipv46: 1.1.21.37
```

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

```
            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
```

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つ以上の仮想サーバーに対してNetScaler® ADM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。

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

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	アナリティクスの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つです。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、その仮想サーバーに対してアナリティクスが収集されます。	はい
フィルター	リスト内のプロパティの1つです。この属性の値は、アナリティクスが収集される仮想サーバー上の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、アナリティクスデータは仮想サーバーを通過するす	いいえ

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

属性	説明	必須
	べてのトラフィックで収集されます。	
インサイト	リスト内のプロパティの1つです。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。	いいえ

例1: 単一の仮想サーバーのアナリティクスを構成する

```
operations:


  analytics:
    -
    name: lbvserver-ops-comp
    properties:
        target: $components-basic-lb-comp.outputs.lbvserver-name
        filter: HTTP.REQ.URL.CONTAINS("catalog")
        insights:
          -
            type: webinsight
          -
            type: securityinsight
```

例2: VPN仮想サーバーのリストのアナリティクスを構成する

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

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        insights:

          -

            type: hdxinsight

          -

            type: gatewayinsight
```

アナリティクス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、対応する許可されたインサイトタイプは次のとおりです。

ターゲット仮想サーバー	インサイトタイプ
エルビーブイサーバー	ウェブインサイト、セキュリティインサイト
シーエスブイサーバー	ウェブインサイト、セキュリティインサイト

© 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
ブイピーエヌサーバー	エイチディーエックスインサイト、ゲートウェイインサイト

注記

IPFIXは、StyleBookで仮想サーバーのアナリティクス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

operationsセクションのalarmsサブセクションは、analytics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properties属性です。properties属性以外のすべての属性のリストについては、Analytics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以下のとおりです。

属性	説明	必須
ターゲット	NetScalerで構成された仮想サーバーの名前を評価する式で、その仮想サーバーに対してアラームが構成されます。	はい
メールプロファイル	NetScaler ADM 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 ADM 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電話番号のリストを含むSMS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）
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	はい

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

属性	説明	必須
	ムをトリガーする条件を定義するルールのリスト。	
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、期間単位で（たとえば、1日に1回）アラームが送信されることを意味します。	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ています。

カウンター|説明|詳細な説明|NetScaler ADMの計算

VPN仮想サーバーの場合：			

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	新しいアプリケーションが起動される

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

		サーバー上のユニークなVPNアプリケーションの合計数。	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（ミリ秒単位）	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全体で計算された平均値
その他の仮想サーバー（CS、LB、Auth、GSLB）			
total_requests	リクエスト数	この仮想サーバーに対するクライアントリクエストの数。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 ADM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記録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。	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新しい方）に、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。

StyleBookにおけるアラームセクションの例:

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

```
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。StyleBookの式は、さまざまなシナリオで動的な値を計算するために使用できます。次の例は、パラメーター値をリテラル文字列と連結する式です。

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。

次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つの数値の加算: $parameters.a + $parameters.b
- 2つの数値の乗算: $parameters.a * 10
- ある数値を別の数値で除算した後の剰余の検索:

`15%10` の結果は `5` です。

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 + $parameters.internal-servers
- `$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、それ以外の場合は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番目のオペランドより大きい場合はtrueを返し、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上である場合はtrueを返し、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**: 論理積演算子です。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**: 論理和演算子です。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**: 単項演算子です。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`を数値にキャストしたり、IPアドレスを文字列にキャストしたりできます。

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をリテラル形式で扱う必要がある場合に、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る場合があります。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。

StyleBook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。

逐語文字列を作成するには、次のように特殊文字で文字列を囲みます。

```
~{string}~
```

逐語文字列はStyleBookのどこでも使用できます。

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

注

入力文字列で文字シーケンス`}~`を使用しないでください。このシーケンスは逐語文字列の終わりを示すためです。

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の定義では、現在のターゲットADC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ADC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ADCインスタンスのIPアドレスで構築されます。

式の型検証

StyleBookエンジンは、コンパイル時のより厳密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、設定パックの作成中ではなく、StyleBook自体のインポート中に検証されます。

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

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、それら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 Application Delivery Management (ADM)では、型の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:

以前のリリースでは、プロパティ名に無効な式が割り当てられても、コンパイラは無効な式を検出せず、StyleBookがNetScaler® ADMにインポートされることを許可していました。現在、このStyleBookがNetScaler ADM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 ADMへのインポートに失敗します。

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

この例では、`lb-sg-binding-comp`コンポーネントの名前プロパティに割り当てられた式は`$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 ADM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を使用して構成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、この種のエラーはインポート中に識別され、StyleBookはNetScaler ADMにインポートされません。そ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

      servicetype: HTTP

  -

    name: lb-sg-binding-comp
```

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

```
    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、直接インデックス付けすることでアクセスできるようになりました。

式	説明
`$components.test-lbs[0]`	test-lbsコンポーネント内の最初の項目を参照します
`$components.test-lbs[0].properties.p1`	test-lbsコンポーネント内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`	`servicegroups`コンポーネント内の2番目の項目のプロパティ`servicegroupname`を参照します。これは、`lbcomps`コンポーネントの最初の項目からの出力です

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できるようになりました。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。

```
"...%{...}%..."
```

ここで、「%{」と「}%」で囲まれた文字が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。

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

たとえば、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。すると、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で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、たとえば「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したい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は、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。これを行うには、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いものに見えます。

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、および 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。

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。シーケンシャル補間では、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、$parameters.appnameが「app1」で$parameters.vipが「1.1.1.1」の場合、文字列lb-%{$parameters.appname}%-%{$parameters.vip}%は「lb-app1-1.1.1.1」を返します。

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

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中にネストして、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。ここでは、この式が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
lb-%{$parameters.appname}%-def	lb-lb1-def

自動型変換

式	結果
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{真}%	lb-真

シーケンシャル補間

式	結果
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

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

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(あいうえお)}%")str("%{quotewrap(`https://)}%+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	"あいうえお"<`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($parameters.n1) + }\%}%")	1}%
	lb-%{str($parameters.n1) + }\%}%	lb-1}%
	"%{str($parameters.n1) + \"\}\%\"}%"	1}%

組み込み関数

StyleBook の式では、組み込み関数を使用できます。

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

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)
```

StyleBook の式でサポートされている組み込み関数と、その使用例を次に示します。

str() 関数

`str()` 関数は、入力引数を文字列値に変換します。

許可される引数の型:

- `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。

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。

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

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、文字列内の文字数またはリスト内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 ADM")` 関数は `10` を返します。

例 3:

`$parameters.vips` に `['1.1.1.1', '1.1.1.2', '1.1.1.3']` の値がある場合、 `len($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。

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

- `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:

- `$parameters.ports` のサポートは `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。
- 「`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。

  「`max($parameters.ports)`」関数は「`8080`」を返します。

bin() 関数

「`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：

「`bin(100)`」関数は「`0b1100100`」を返します。

oct() 関数

「`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。

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

式の例：

「`oct(100)`」関数は「`0144`」を返します。

hex() 関数

「`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：

The `hex(100)` 関数は `0x64` を返します。

小文字()

The `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:

The `lower("ADM")` 関数は `adm` を返します。

大文字()

The `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:

The `upper("NetScaler ADM")` 関数は `NetScaler ADM` を返します。

合計()

The `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。

例 1:

置換を次のように定義した場合: substitutions:

```
list-of-numbers = [11, 22, 55]
```

The `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。

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

べき乗()

`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番目の引数で累乗した結果の数値を返します。

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アドレスが返されます。

    `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。
  - 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。

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

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。

exists() 関数

`exists()` 関数は任意の型の引数を受け取り、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。

`$parameters.monitor` はオプションのパラメーターであるとします。設定パックを作成する際にこのパラメーターに値を指定すると、`($parameters.monitor)` 関数は `True` を返します。

それ以外の場合、`False` を返します。

フィルター()

`filter()` 関数は2つの引数を受け取ります。

引数1：1つの引数を受け取り、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：

置換関数を次のように定義したとします。

置換：

```
x(a): $a != 81
```

この関数は、入力値が `81` と等しくない場合は True を返し、それ以外の場合は `False` を返します。

`$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` のすべての出現箇所を削除して `[80, 89]` を返します。

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

イフ-ゼン-エルス()

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:

`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)

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

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によって区切られます。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。

  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。

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

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]` であると仮定します。

- 組み込み関数 str を使用してマップする

  `map(str, $parameters.nums)` 関数は `["81", "82", "83"]` を返します

  map関数の結果は、入力リスト ($parameters.nums) の対応する要素に str 関数を適用して各要素が計算される文字列のリストです。

- 置換関数を使用してマップする
  - 置換:

    `add-10(port): $port + 10`

  - 式:

    `map($substitutions.add-10, $parameters.nums)` 関数は数値のリスト `[ 91, 92, 93 ]` を返します

このmap関数の結果は、入力リスト `($parameters.nums)` の対応する要素に置換関数 `$substitutions.add-10` を適用して各要素が計算される数値のリストです。

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後に文字列を返します。

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。

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

引数1: 文字列

引数2: 文字列またはリスト

引数3: 文字列 (オプション)

この関数は、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（つまり、空の文字列に置き換えられます）。

サブ文字列を別のサブ文字列に置き換える:

- `replace('abcdef', 'def', 'xyz')` 関数は `abcxyz` を返します。

  `def` のすべての出現箇所は `xyz` に置き換えられます。
- `replace('abcdefabc', 'def')` は `abcabc` を返します。

  3番目の引数がないため、 `def` は結果の文字列から削除されます。

文字列内で置き換えたい文字リストを指定します。

```
$parameters.spl_chars = ['@', '#', '!', '%']
```

このリストには、入力文字列内で置き換える必要がある値が含まれています。

`replace('An#example@to%replace!characters', $parameters.spl_chars, '_')` 関数は `An_example_to_replace_characters` を返します。

出力文字列には、 `$parameters.spl_chars` リストで指定された文字の代わりにアンダースコア (`_`) が含まれています。

トリム()

`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。

トランケート()

`truncate()` 関数は2つの引数を取ります。

引数1: 文字列

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

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 ADM', 6)` は `Citrix` を返します。

ディスティンクト()

`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:

`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

`is-ipv4()` 関数は、引数としてIPアドレスを受け取り、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。

`is-ipv4(10.10.10.10)` 関数は `True` を返します

is-ipv6() 関数

`is-ipv6()` 関数は、引数としてIPアドレスを受け取り、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。

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

`is-ipv6(2001:DB8::)` 関数は `True` を返します

スターツウィズ()

`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。この関数は、2つの必須文字列引数を必要とします。

```
startswith(str, sub_str)
```

この関数は、文字列 (`str`) がサブストリング (`sub_str`) で始まる場合に `True` を返します。

例:

- `startswith('Citrix', 'Ci')` 関数は `True` を返します。
- `startswith('Citrix', 'iC')` 関数は `False` を返します
- `startswith('Citrix', 'Ab')` 関数は `False` を返します

エンズウィズ()

`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。この関数は、2つの必須文字列引数を必要とします。

```
endswith(str, sub_str)
```

この関数は、文字列 (`str`) がサブストリング (`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:

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

- `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)`

この関数には、2つの必須引数と1つのオプションの整数引数が必要です。

- `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`) からサブストリングを返します。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サブストリングを抽出します。

注

`end_index` を指定すると、サブストリングは `end_index` の位置にある文字を除外します。

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、関数はインデックス位置2と4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文字を含むサブストリングを抽出します。

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

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:

      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

-
```

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

```
    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: HTTP
```

上記の例では、**lbvserver-comp**、**lb-sg-binding-comp**、**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の依存関係がコンポーネントの作成時までに解決されるようにコン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:
```

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

```
-
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $components.lb-sg-binding-comp.properties.name
    ipv46: 10.102.190.15
    port: 80
    servicetype: HTTP
-
  name: lb-sg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  condition: $parameters.create-binding
  properties:
   name: mylb
    servicegroupname: $components.sg-comp.properties.servicegroupname
-
  name: sg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: mysg
    servicetype: $components.lbvserver-comp.properties.servicetype
```

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

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® ADM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セキュリティ分析は、アプリケーションに対する脅威を監視、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
- Splunkとの統合
- New Relicとの統合

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、検出済み/ライセンス済み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、検出済み/ライセンス済み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. **セキュリティ** > **セキュリティダッシュボード** に移動します。
2. インスタンスリストからインスタンスの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大度を示す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大であるほど、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。値の範囲は1から7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。違反情報または攻撃が発生した場合にのみ、違反情報がNetScaler® ADM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。

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

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。値の範囲は1から7です。

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の構成とNetScalerシステムセキュリティの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るにもかかわらず、`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アドレスが表示されます。

2 - 脅威インデックススコア、発生した違反の合計、ブロックされた違反の合計などの詳細が表示されます。

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 - 違反をマップビューと表形式ビューで表示します。

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、違反の種類、攻撃時刻、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、攻撃時刻、攻撃カテゴリ、重大度、URLなどの違反の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。

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

安全指数詳細

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い場合があります。この情報は、アプリケーションの安全指数サマリーをドリルダウンすることで取得できます。

安全指数サマリーは、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およびセキュリティエンティティの数を示します。
- **NetScaler ADM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。

安全指数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、**安全指数**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の構成に関する詳細情報が表示されます。

2 - システムセキュリティに関する詳細情報が表示されます。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が表示されます。

仮想サーバーの**WAFセキュリティ違反**を有効にし、**セキュリティ** > **セキュリティ違反**に移動することで、脅威環境の概要も表示できます。

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、攻撃に対して大幅に脆弱になっています。NetScaler® ADMは、攻撃からアプリケーションを保護するために、実用的な違反の詳細を視覚化できるようにします。次の単一ペインソリューションについては、**Security** > **Security Violations** 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
- **Network**、**Bot**、**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

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

- 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

Security Violations ページには、次のオプションがあります。

- **Application Overview** – 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、「アプリケーションの概要」を参照してください。
- **All Violations** – 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

Metrics Collector が有効になっていることを確認します。デフォルトでは、NetScalerインスタンスで **Metrics Collector** が有効になっています。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。

Splunkとの統合

NetScaler® ADM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
- Bot違反
- SSL証明書のインサイト

Splunkアドオンを使用すると、次のことができます。

- 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 ADMは、Bot、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。

- NetScaler ADMからデータを受信するようにSplunkを構成する
- SplunkにデータをエクスポートするようにNetScaler ADMを構成する
- Splunkでダッシュボードを表示する

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

NetScaler ADMからデータを受信するようにSplunkを構成する

Splunkでは、次のこと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設定し、トークンを生成する(#setup-the-splunk-http-event-collector-endpoint-and-generate-a-token)
2. Splunk Common Information Model (CIM) アドオンをインストールする(#install-the-splunk-common-information-model)
3. Splunkでサンプルダッシュボードを準備する(#prepare-a-sample-dashboard-in-splunk)

Splunk HTTPイベントコレクターエンドポイントを設定し、トークンを生成する

まず、SplunkでHTTPイベントコレクターを設定する必要があります。この設定により、ADMとSplunk間のデータ送信統合が可能になります。次に、Splunkでトークンを生成する必要があります。

- ADMとSplunk間の認証を有効にする。
- 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する。

1. Splunkにログオンします。
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 が選択されています。

    e. **インデクサーの確認を有効にする**: デフォルトでは、このオプションは選択されていません。

    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. 必要に応じて、**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。

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

トークンが生成されます。NetScaler ADMで詳細を追加する際には、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 Common Information Model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 ADM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。

1. Splunkにログオンします。
2. **アプリ > その他のアプリを検索**に移動します。

   Splunkで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、**インストール**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)

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Bot、およびSSL証明書インサイト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) を使用してそのコンテンツをコピーし、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。

注記:

サンプルダッシュボードを作成するための以下の手順は、WAFとBot、およびSSL証明書インサイトの両方に適用できます。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、Observability Integration の下にあ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ーを使用して `json` ファイルを開き、ファイルからデータをコピーします。

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

注記:

解凍すると、2つの `json` ファイルが得られます。WAFおよびBotのサンプルダッシュボードを作成するには `adm_splunk_security_violations.json` を使用し、SSL証明書インサイトのサンプルダッシュボードを作成するには `adm_splunk_ssl_certificate.json` を使用します。

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** - オプションで、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。

      「**作成**」をクリックした後、レイアウトから「**ソース**」アイコンを選択します。

      ソースレイアウト(/en-us/netscaler-application-delivery-management-software/media/splunk-source-icon.png)

5. 既存のデータを削除し、手順2でコピーしたデータを貼り付けて、「**戻る**」をクリックします。

6. 「**保存**」をクリックします。

   Splunkで次のサンプルダッシュボードを表示できます。

   サンプルダッシュボード(/en-us/netscaler-application-delivery-management-software/media/splunk-sample-dashboard.png)

NetScaler ADM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 ADMを構成することです。

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

次の手順を完了すると、NetScaler ADM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。

1. NetScaler ADMにログオンします。
2. **設定 > エコシステム統合**に移動します。
3. 「**サブスクリプション**」ページで、「**追加**」をクリックします。
4. 「**サブスクライブする機能を選択**」タブで、エクスポートする機能を選択し、「**次へ**」をクリックします。
   - **リアルタイムエクスポート** - 選択した違反はすぐにSplunkにエクスポートされます。
   - **定期エクスポート** - 選択した違反は、選択した期間に基づいてSplunkにエクスポートされます。

   「機能を選択」(/en-us/netscaler-application-delivery-management-software/media/splunk-select-features.png)
5. 「**エクスポート構成の指定**」タブで、次のように設定します。
   a. **エンドポイントタイプ** – リストから「**Splunk**」を選択します。
   b. **エンドポイント** – 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。

   c. **認証トークン** – Splunkページから認証トークンをコピーして貼り付けます。
   d. 「**次へ**」をクリックします。

   「サブスクリプションの作成」(/en-us/netscaler-application-delivery-management-software/media/splunk-create-subscription.png)
6. 「**サブスクライブ**」ページで、次のように設定します。

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

a. **エクスポート頻度** – リストから「日次」または「時間単位」を選択します。選択に基づいて、NetScaler ADMは詳細をSplunkにエクスポートします。

> **注:**
>
> 「**定期エクスポート**」で違反を選択した場合にのみ適用されます。

b. **サブスクリプション名** – 任意の名前を指定します。

c. **通知を有効にする**チェックボックスをオンにします。

d. **送信**をクリックします。

購読(/en-us/netscaler-application-delivery-management-software/media/splunk-subscribe.png)

> **注**
>
> - **定期エクスポート**オプションを初めて設定すると、選択した機能データはすぐにSplunkにプッシュされます。次回のエクスポート頻度は、選択内容（毎日または毎時）に基づいて行われます。
> - **リアルタイムエクスポート**オプションを初めて設定すると、NetScaler ADMで違反が検出されたときに、選択した機能データがすぐにSplunkにプッシュされます。

Splunkでダッシュボードを表示する

NetScaler ADMでの設定が完了すると、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。

更新されたダッシュボード(/en-us/netscaler-application-delivery-management-software/media/splunk-updated-dashboard.png)

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。

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

SSL証明書(/en-us/netscaler-application-delivery-management-software/media/splunk-ssl-dashboard.png)

New Relicとの統合

NetScaler® ADMをNew Relicと統合して、New RelicダッシュボードでWAFおよびBot違反のアナリティクスを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。
- 一元化された場所でアナリティクスの可視性を確保します。

NetScaler ADM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
  ```

  イベントエンドポイントの設定の詳細については、New Relic documentation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 documentation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 documentationを参照してください。
- NetScaler ADMにキーの詳細を追加します

NetScaler ADM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 ADMに詳細を追加する必要があります。

1. NetScaler ADMにログオンします。
2. **Settings > Ecosystem Integration**に移動します。
3. **Subscriptions**ページで、**Add**をクリックします。
4. **Select features to subscribe**タブで、エクスポートする機能を選択し、**Next**をクリックします。

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

- **Realtime Export** - 選択した違反はすぐにNew Relicにエクスポートされます。
- **Periodic Export** - 選択した違反は、選択した期間に基づいてNew Relicにエクスポートされます。

5. 「**エクスポート設定の指定**」タブで:
   a. **End Point Type** – リストから**New Relic**を選択します。
   b. **End Point** – New Relicの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。

   c. **Authentication token** – New Relicページから認証トークンをコピーして貼り付けます。
   d. **Next**をクリックします。

6. 「**サブスクライブ**」ページで:
   a. **エクスポート頻度** – リストから「毎日」または「毎時」を選択します。選択内容に基づいて、NetScaler ADM は詳細を New Relic にエクスポートします。

      注

      定期エクスポートで違反を選択した場合にのみ適用されます。

   b. **サブスクリプション名** – 任意の名前を指定します。
   c. **通知を有効にする**チェックボックスをオンにします。
   d. **送信**をクリックします。

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

注

- **定期エクスポート**オプションで初めて設定する場合、選択された機能データはすぐに New Relic にプッシュされます。次回のエクスポート頻度は、選択内容（毎日または毎時）に基づいて行われます。
- **リアルタイムエクスポート**オプションで初めて設定する場合、NetScaler ADM で違反が検出されるとすぐに、選択された機能データが New Relic にプッシュされます。

設定は完了です。「**サブスクリプション**」ページで詳細を表示できます。

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、**メトリクスとイベント**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。

JSONデータがNew Relicダッシュボードに取り込まれたら、管理者として、NRQL (New Relic Query Language) を使用して、取り込まれたデータに基づいてクエリを構築し、選択した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。

このダッシュボードを作成するには、次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数

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

```
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
```

© 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

ゲートウェイインサイト

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、アクセス障害の問題をトラブルシューティングするために不可欠です。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。いつでも、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、すべてのユーザーが使用したバイト数とライセンス数を表示できます。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数、合計およびアクティブセッション数、合計バイト数、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。

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® ADM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。

留意事項

- Gateway Insightは、以下の展開でサポートされています。
  - アクセスゲートウェイ
  - 統合ゲートウェイ
- NetScaler ADM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、第2DMZの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、以下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が使用されている場合、Gateway Insightでいくつかの不一致が見られ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 ADM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 ADM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でAppFlowを有効にする必要があります。NetScaler ADM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 ADM 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 ADM が **13.0 Build 36.27** の場合に適用されます。

1. **Infrastructure > Instances** 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 の有効化**をクリックします。
5. **AppFlow の有効化**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 と **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 ADM バージョン 13.0 Build 41.x 以降の場合

1. **Infrastructure > Instances** に移動し、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. 「**詳細オプション**」で:
   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記録を有効にする

1. **構成 > システム > AppFlow > 設定** に移動し、「**AppFlow設定の変更**」をクリックします。
2. 「**AppFlow設定の構成**」画面で、「**AAAユーザー名**」を選択し、「**OK**」をクリックします。

Gateway Insightレポートの表示

NetScaler ADM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したり、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したりできます。「**概要**」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時間ごとに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は、グループにロールを割り当てたり、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たり、グループにユーザーを割り当てたりできます。NetScaler ADM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。

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 ADM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、障害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 ADM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 ADMで、**Gateway > Gateway Insight > Users** に移動します。
2. ユーザー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。

© 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、およびライセンスを表示できます。

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。

「**Users**」または「**Active Users**」タブでユーザーをクリックすると、次のユーザー詳細が表示されます。

- **ユーザーの詳細** - ADC 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して、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を表示します。
- **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して、選択したゲートウェイに関連付けられている上位10個のアプリケーションと上位10人のユーザーを表示します。
- **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してゲートウェイの詳細を表示します。
- ユーザーの**アクティブセッション**と**終了セッション**。
- **アクティブセッション**での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 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

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

- 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 ADMで、**Gateway > Gateway Insight > Applications**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。

これで、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、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)

その他のアプリケーションタブで、**名前**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。

ゲートウェイのGateway Insightレポートの表示

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ログオンアクティビティも表示できます。

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

ゲートウェイの詳細を表示するには

1. **NetScaler ADM**で、**Gateway > Gateway Insight > Gateways**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できます。**Go**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)

ゲートウェイドメイン名列のゲートウェイをクリックすると、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

Gateway Insightレポートは、GUIに表示されるすべての詳細を含め、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。

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 ADM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. **Dashboard**タブの右ペインで、**export**ボタンをクリックします。
2. **Export Now**で、必要な形式を選択し、**Export**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:

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

1. **Dashboard**タブの右ペインで、**export**ボタンをクリックします。
2. **Schedule Export**で、詳細を指定し、**Schedule**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. **Configuration**タブで、**Settings > Notifications > Email**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**Email Server**を選択するか、メール配布リストを作成するには**Email Distribution list**を選択します。
3. 詳細を指定し、**Create**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**」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

以下のユースケースは、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 ADM 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。

NetScaler ADM では、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 ADM 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 ADM で、**Gateway > Gateway Insight** に移動し、「**ユーザーを検索**」テキストボックスで検索したいユーザーを指定します。

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

認証の失敗

誤った資格情報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 ADM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。

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表示できます。

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

重要：

- クラシック式が構成されている場合にのみ、EPA障害が報告されます。
- 事前認証ポリシーまたは事後認証ポリシーで高度な式が構成されている場合、EPA障害は報告されません。
- nFactor認証フローの要因の1つとしてEPAが構成されている場合、EPA障害は報告されません。

EPA障害の詳細を表示するには：

1. NetScaler ADMで、 **>** の順に移動します。
2. セクションで、EPAエラー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。 をクリックします。

3. タブをクリックします。 グラフで、任意の時点でのEPA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、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するには、下にスクロールします。テーブルの 列にはEPA障害の理由が表示され、 列には障害の原因となったポリシーが表示されます。

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、テーブルをカスタマイズして列を追加または削除できます。

注

NetScaler Gatewayは、「clientSecurity」式がVPNセッションポリシールールとして構成されている場合、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：

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

1. NetScaler ADM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。

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。

下にスクロールすると、同じタブのテーブルから、**ユーザー名、NetScaler IPアドレス、エラー時刻、エラーの説明、リソース名**など、各SSOエラーの詳細が表示されます。

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、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。

NetScaler Gatewayへのログオンに成功した後、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、その理由を可視化できます。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：

1. NetScaler ADM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。

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。

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。

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

「**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 ADM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 ADM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。

- 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。
- 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。
-

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 ADMで、**Gateway > Gateway Insight > Applications** に移動します。
2. 表示された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。

   ユーザーアクセス詳細(/en-us/netscaler-application-delivery-management-software/media/use-cases-resource-access.png)
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。

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

異なるユーザーが異なるNetScaler Gateway展開を使用しているか、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時間ごとにログオンした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か従来のNetScaler Gateway展開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、およびログオンしたユーザー数の概要を表示するには：

1. NetScaler ADMで、**Gateway > Gateway Insight** に移動します。
2. **Overview** セクションで下にスクロールすると、**Session Mode**、**Operating Systems**、**Browsers**、および **User Logon Activity** の各チャートに、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時間ごとにログオンしたユーザー数が表示されます。

   Gateway Insightの概要(/en-us/netscaler-application-delivery-management-software/media/use-cases-deployment-types-access-modes-summary.png)

   Gateway Insightの概要グラフ(/en-us/netscaler-application-delivery-management-software/media/use-cases-deployment-types-access-modes-user-log-activity.png)

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 ADM 間の接続の問題。
- NetScaler でのレコード生成。
- NetScaler® ADM 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。

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

- 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 の展開では、Gateway Insight AppFlow ポリシーが VPN 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。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` パラメータを確認します。詳細については、「仮想サーバーの AppFlow の有効化」を参照してください。

NetScaler と NetScaler ADM 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。
- 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 **> >** 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検証します。

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 で統計情報の増分を確認します。
- `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。

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

注:

`nstrace logs` は IPFIX にのみ必要です。Logstream の場合、nstrace ログでは ADC 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 ADM 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 ADM 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 ADM 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 ADM でライセンスされていることを確認します。

NetScaler ADM での Logstream ログの検証

NetScaler ADMが受信したLogstreamデータの検証は、以下の方法で行うことができます。

- **NetScaler ADM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。

  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

以下の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

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

- 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、NetScalerログをチェックしてAppFlowレコードがエクスポートされているか確認できます。`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
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
```

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

```
Web BackendServername= SSOurl= email="

SSO logs:
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=1 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=3 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=2 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:443 SessSeq=c
Sessid=<sessid> Gwip=<ip>:443 StatusCode=155 CSappid=0 CSAppname=(null)
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。

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

- NetScalerおよびNetScaler ADMのバージョン。
- NetScalerおよびNetScaler ADM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、ADCリリースノートを参照してください。

HDX™ インサイト

HDX Insightは、NetScalerを通過するCitrix Virtual Apps and DesktopへのHDXトラフィックに対して、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表示し、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。リアルタイムおよび履歴の可視性データの両方が利用可能であるため、NetScaler Application Delivery Management (ADM) 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
- 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セッションを表示できます。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。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。

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

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 ADM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、承認されたアプリケーション（仮想サーバー）のみのすべてのInsight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 Insight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Admin Partitionをサポートしています。

次のシンクライアントはHDX Insight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。

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、またはクライアントネットワーク上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

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

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. グラフには、指定された期間のユーザーのICA RTTとDC遅延値が表示されます。

4. **Current Sessions**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. **Current Sessions**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

Citrix Virtual AppまたはDesktopでアプリケーションを起動中にユーザーに遅延が発生している

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。

- 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。

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

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。

   現在のセッション(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-7.png)

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遅延が低いにもかかわらずRTTが高い場合、ホストサーバーでアプリケーションエラーが発生していることを示します。

注 NetScaler ADMソフトウェア11.1ビルド51.21以降を使用している場合、HDX Insightは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。

ユーザー(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-8.png)

HDX Insightのジオマップ

NetScaler® ADM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地図上に表示します。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。

特定の地理的場所またはLANのジオマップを表示するようにNetScaler ADMを構成するには、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：

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

組織ABCに2つの支社があり、1つはサンタクララに、もう1つはインドにあるというシナリオを考えてみましょう。

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

サンタクララのユーザーはSClara.x.comの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の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、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している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、ユーザーがVPNにアクセスするための2つのローカルNetScaler Gatewayアプライアンスを持つように、別のNetScaler Gatewayをインストールすることを決定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、分析データが1時間しか収集されないため、NetScaler ADMでHDX Insight用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 Application Delivery Management (ADM) 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。

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 および 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

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

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 および Desktop アプリケーションに直接接続できるようにするために、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ト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。

ADC を LAN ユーザーモードで展開(/en-us/netscaler-application-delivery-management-software/media/lan.png)

注

NetScaler ADM 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、その後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 ADM 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

- ADC インスタンスで、**設定 > AppFlow > コレクター** に移動して、コレクター (つまり NetScaler ADM) 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 ADM に送信します。しかし、インスタンスは SNIP を使用して NetScaler ADM との接続性を検証します。したがって、SNIP がインスタンスで構成されていることを確認してください。
- NetScaler ADM 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、次の操作を行います。

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

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 )]



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 ADM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、コレクターをアクションに関連付けます。

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

```
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。入力: `save ns config`

© 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 Application Delivery Management (ADM) インベントリに追加し、ADMでAppFlowを有効にする必要があります。

NetScaler® ADMからAppFlow機能を有効にするには:

1. Webブラウザーで、NetScaler ADM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。
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>
```

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

```
-  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 ADM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 ADMに表示されます。

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

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遅延に対してどのように機能するかを分析したい場合は、NetScaler ADM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。

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 ADM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、最初のDMZにあるNetScaler ADMと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 ADM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 ADM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 ADM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 ADM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。

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

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 ADMインベントリに追加し、NetScaler ADMでAppFlowを有効にしてから、NetScaler ADM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を設定する手順:

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、**分析の設定**を選択します。
3. 認証用に設定された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。
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. もう一方のVPN仮想サーバーで手順3から6を繰り返します。

NetScaler ADMでデータ収集を有効にする

NetScaler ADMで両方のアプライアンスからICAの詳細の収集を開始するように設定すると、収集される詳細が冗長になります。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。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 ADMからAppFlow機能を有効にするには:

1. Webブラウザで、NetScaler ADM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。
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、**分析の設定**を選択します。
5. VPN仮想サーバーを選択し、**Enable Analytics**をクリックします。
6. **HDX Insight**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**ICA**または**TCP**を選択します。

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

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「有効」と表示されていても、NetScaler ADMダッシュボードにはレコードが表示されません。

7. **OK**をクリックします。

データをエクスポートするためのNetScaler Gatewayアプライアンスの構成

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 ADMにエクスポートするために、NetScaler Gatewayアプライアンスで以下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を、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。
- NetScaler Gatewayアプライアンスのいずれかを ICAレコードをエクスポートするように有効にします
- もう一方のNetScaler Gatewayアプライアンスを TCPレコードをエクスポートするように有効にします：
- 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
```

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

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。

```
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レコードをエクスポートできるようにします。

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
OTHERTCP_REQUEST
```

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

6. 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。

```
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。
   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。
   c. **Next Hop Server**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. **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. 「詳細」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。

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

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. NetScaler Gatewayアプライアンスのいずれかを有効にしてTCPレコードをエクスポートします。
   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「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**」を選択し、「**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アプライアンスを有効にしてICAレコードをエクスポートします。
   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、「**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」を選択し、「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ーンを有効にします。
   a. **Configuration**タブで、**System** > **Appflow**に移動します。
   b. 右ペインで、**Settings**グループの「**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。

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

7. 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。

   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、「**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. 「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**」の選択を解除します。

10. NetScaler Gatewayアプライアンスのいずれかを有効にして、TCPレコードをエクスポートします。

    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「**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」を選択し、「**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。

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

11. もう一方のNetScaler Gatewayアプライアンスを有効にして、ICAレコードをエクスポートします。

    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「**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」を選択し、「**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。

12. NetScaler Gatewayアプライアンスの両方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 Desktop環境でNetScalerアプライアンス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 ADM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NetScaler ADMを追加し、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。

注

- NetScaler ADM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。

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

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 ADM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。

```
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、コレクターをアクションに関連付けます。

```
add appflow action <name> -collectors <string> ...
```

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

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。

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`

© 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 Application Delivery Management (ADM) インベントリに追加し、ADM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)

ADMからAppFlow®機能を有効にするには：

1. **インフラストラクチャ** \> **インスタンス** に移動し、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の有効化** をクリックします。
4. **AppFlowの有効化** フィールドで、**true** と入力し、**ICA®** を選択します。
5. **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、次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`

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

- `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® ADM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 ADMに引き続き表示されます。

透過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が透過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が透過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 ADM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 ADM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。

注

- NetScaler ADM構成ユーティリティを使用して、透過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が透過モードで展開されている場合のNetScaler ADM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：

© 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. 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AppFlowコレクターとしてNetScaler Insight Centerを追加します。

```
add appflow collector <name> -IPAddress <ip_addr>
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

注: NetScalerインスタンスに構成されている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。

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

```
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
```

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、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遅延に対してどのように機能するかを分析したい場合は、NetScaler ADMをインス

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

トールして、NetScaler Gatewayアプライアンスがこれらの重要な統計を報告するように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® ADM

ダブルホップモード(/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。

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により、ICAトラフィックは2番目のDMZを通過し、サーバーファームへのユーザー接続を完了できます。

NetScaler ADM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 ADM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 ADM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 ADM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 ADM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 ADM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 ADMインベントリに追加し、NetScaler ADMでAppFlowを有効にしてから、NetScaler ADMダッシュボードでレポートを表示する必要があります。

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

NetScaler ADMでデータ収集を有効にする

NetScaler ADM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。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 ADM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. 「**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の有効化**」をクリックします。
4. 「**AppFlowの有効化**」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 ADM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。

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 ADM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

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

- 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。

   add vpn nextHopServer \<名前\> \<次ホップIP\> \<次ホップポート\> \[**-secure**(ON|OFF)\] \[**-imgGifToPng**\] など.

   ```
   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\> \[**- doubleHop** (有効 |無効)\] \[**- appflowLog** (有効 |無効)\]

   ```
   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。

   set vpn vserver\<name\> \[**-authentication** (ON|OFF)\]

   ```
   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\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \[**-type**\<type\>\]

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

```
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イニングを有効にします。

   set appFlow param \[**-接続チェイニング** (ENABLED|DISABLED)\]

   ```
   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。

   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。

   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。

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

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**」をクリアします。

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、詳細設定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**ドロップダウンリストから**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。

5. 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. 右ペインで仮想サーバーをダブルクリックし、**詳細設定**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**ドロップダウンリストから**AppFlow**を選択し、種類の選択ドロップダウンリストから**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。

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. **構成**タブで、**設定 > Appflow**に移動します。
b. 右ペインの**設定**グループで、**Appflow設定の変更**をクリックします。
c. **接続チェーン**を選択し、**OK**をクリックします。

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

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、透過モードの展開では、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、管理者が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。

図4. LANユーザーモードで展開されたNetScaler® ADM

LANユーザーモード(/en-us/netscaler-application-delivery-management-software/media/lan.png)

注 NetScaler ADM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 ADM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 ADM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、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。

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

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\> \[-HDX ( ON | OFF )\]



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NetScaler ADM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、コレクターをアクションに関連付けます。

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

```
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
```

8. 構成を保存します。

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

```
save ns config
```

HDX™ Insight のしきい値を作成し、アラートを設定する

NetScaler Application Delivery Management (ADM) 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 ADM 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ーにしきい値を設定できます。また、NetScaler ADM 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、ユーザーなどのさまざまなエンティティに関連付けられています。すべてのエンティティには、それら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 レイテンシー、DC レイテンシー、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® ADM 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 ADM では、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にのみアラートが生成されます。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を1つのしきい値グループとしてアプリケーションを監視できます。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。

いくつかの例を以下に示します。

- 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 レイテンシー (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、ルールを作成する際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、エンティティごとに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。

カウンターの値がしきい値を超えると、NetScaler ADM はしきい値侵害を示すイベントを生成し、すべての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 ADM にアラートを表示したり、電子メールまたはモバイルデバイスへの SMS としてアラートを受信したりできます。最後の2つのアクションについては、NetScaler ADM 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カ国以上にオフィスを持つグローバル企業です。同社は、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おり、1つはシンガポールに、もう1つはカリフォルニアにあります。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、世界中でCitrix Virtual Apps and Desktopsにアクセスしています。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クセスできるようにアプリとデスクトップの配信を最適化するため、すべてのオフィスで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、逸脱があればプロアクティブに通知したいと考えています。

ABC Inc.のユーザーは分散しています。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、リモートの場所では約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を使用すると、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、容量の問題があれば根本原因を特定することができます。Ericは、Citrix Virtual Apps and Desktopsのすべての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 ADM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 ADMで、 **> >** の順に移動します。開いた ページで、 をクリックします。
2. ページで、次の詳細を指定します。

    a. **名前**。NetScaler ADM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**。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、参照キーが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。エンティティは、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-citrix.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、 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 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-citrix.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、個別のルールとしてではなく、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-citrix.png)

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

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

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-citrix.png)

5. **しきい値を有効にする**をクリックして、NetScaler ADM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レポートとメトリックの表示

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ックを完全に可視化します。

選択したエンティティのHDXメトリックを表示できます。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。
- **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。

ユーザー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 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。

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

- 概要ビュー
- 「ユーザーごとの表示」(#per-user-view)
- 「ユーザーセッションごとの表示」(#per-user-session-view)

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ック/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 GatewayとVDIまたはCVADまたはStoreFrontサーバー間の遅延です。
帯域幅	選択され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。

© 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。
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。

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

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

メトリック	説明
	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。
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。
合計アプリ起動回数	選択した期間中にユーザーによって起動された合計アプリ。

© 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によって消費された合計バイト数。
アクティブなデスクトップ	指定された時間間隔中のアクティブなCitrix Virtual Desktopsの合計数。

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た全体の帯域幅または合計バイト数をドーナツグラフの形式で表します。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、各ワークスペースクライアントによって消費された全体の帯域幅/合計バイト数をドーナツグラフの形式で表します。グラフ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、選択した期間における違反したしきい値の数を表します。

世界地図

HDX Insight の世界地図ビューを使用すると、管理者は地理的な観点から過去および現在の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、さらに都市や州別に情

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

報を表示するためにドリルダウンできます。NetScaler ADM 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、以下の詳細が表示され、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

「世界地図」(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

ユーザーごとのビュー

「ユーザーごとのビュー」は、選択され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を提供します。

特定のユーザーのメトリクスに移動するには：

1. サポートされているWebブラウザを使用して、NetScaler® ADMにログオンします。
2. **Gateway > HDX Insight > Users** に移動します。
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

折れ線グラフは、選択された期間における、選択された特定のユーザーのすべてのメトリクスの概要を表示します。
現在/終了したセッションレポート
このレポートは、選択されたユーザーの現在/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。これらのメトリクスは、開始時刻、セッション再接続、ACRカウントでソートできます。

メトリクス	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。

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

メトリクス	説明
ホスト遅延	サーバーネットワークによって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。
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	バックエンド側/Citrix Virtual Appサーバー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。
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。たとえば、NetScaler Gatewayユーザー/透過モードなどです。
国	セッションが確立された国。

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

メトリクス	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: 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

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

メトリクス	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ています。
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 Application Delivery Management (ADM) 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、ADM は現在、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、ユーザーが使用するプロトコルの種類に基づいた総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。

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

注

HDX InsightにおけるEDTは、NetScaler ADM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 ADM 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る平均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間で観測される平均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インサイトを提供します。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。

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

メトリック	説明
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。
DC遅延	NetScaler GatewayとVDIまたはCVADまたはStoreFrontサーバー間の、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。
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 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と対話しているときにユーザーが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、および起動期間でソートされたアプリケーションを表す棒グラフ。

- 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。

- 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/総バイト数をドーナツチャート形式で表します。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(/en-us/netscaler-application-delivery-management-software/media/hdx-user-agents.png)

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

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. **ユーザーサマリーレポート**セクションから特定のユーザーを選択します。
3. **現在のセッション**または**終了したセッション**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セッションの数を表します。
ACRカウント	この数値は、アクティブなCitrix Virtual App セッションの数を表します。
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。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

© 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信タイムアウトが発生した回数。
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。

- 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。

- 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。

-

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。

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

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
# 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。

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。
セッション起動の合計数	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。
アプリ起動の合計数	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

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

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	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。

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。

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/非アクティブなセッションの場合は緑/赤。
ホスト遅延	NetScalerを通過するICAトラフィックの、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。
間隔あたりの帯域幅	セッションが特定の時間間隔で消費した帯域幅。

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

メトリック	説明
セッション帯域幅	時間間隔に関係なくセッションが消費した帯域幅。
間隔あたりのバイト数	セッションが特定の時間間隔で消費したバイト数。
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	バックエンド側/Citrix Virtual AppサーバーIPアドレス。
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。
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。

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

メトリック	説明
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。

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

メトリック	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。
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	セッションの状態：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る平均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間で観測される平均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。

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

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 ADM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した合計回数。
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。
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への遅延です。
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。
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。

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。

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. サポートされているWebブラウザを使用してNetScaler ADM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

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Citrix Virtual Desktopsのレポートが表示されます。

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

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。

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

メトリック	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。

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、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。
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要した1秒あたりの合計バイト数。
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。

© 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デスクトップが選択されている場合に、しきい値が侵害された回数を表します。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では、選択したCitrix Virtual Desktop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。

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 ADM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。

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通信に要した1秒あたりの合計バイト数。

© 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。
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。

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

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

メトリック	説明
	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)

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。

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。

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

メトリック	説明
アップタイム	セッション期間。
クライアントIPアドレス	エンドユーザーの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。
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インスタンスの数です。
クライアントホスト名	クライアントのホスト名です。
HAフェイルオーバー回数	HAフェイルオーバーが発生した回数です。

© 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。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です。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です。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	ユーザーが選択した期間中に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ています。
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。

© 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。
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表示

デスクトップセッションごとの表示では、特定の選択されたCitrix Virtual Desktopセッションに関するレポートが提供されます。

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 ADMにログオンします。
2. **Analytics \> HDX Insight \> Desktop**に移動します。
3. **Desktop Summary Report**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. サポートされているWebブラウザを使用してNetScaler ADM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. 「**現在のセッション**」または「**終了したセッション**」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。

© 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 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。
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

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。
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る帯域幅。
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	エンドユーザーの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。

© 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。
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。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。

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

メトリック	説明
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。
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。
合計バイト数	選択された期間中にユーザーによって消費された合計バイト数。
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タイムアウトが発生した回数。

© 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

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ブラウザを使用してNetScaler ADMにログオンします。
2. **Analytics \> HDX Insight \> Instances** に移動します。

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。

- インスタンスサマリービュー
- インスタンスごとのビュー

インスタンスサマリービュー

このビューは、NetScaler ADM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、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 | 合計アプリを表示します。

インスタンス棒グラフ(/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。
合計セッション起動数	指定された時間間隔で作成された一意のユーザーセッションの総数。
合計アプリ	特定の時間間隔で起動された一意のアプリケーションの総数。
種類	N/A

© 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*がインスタンスとして選択されている場合に、侵害され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。そのため、これらのセッションは監視からスキップされます。

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持ち、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 ADM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

世界ビュー(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

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、選択された特定の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。

インスタンスビューに移動するには：

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

1. サポートされているWebブラウザを使用してNetScaler ADM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。
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。
アプリケーションの合計	指定された時間間隔に起動されたユニークな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ケーション、セッション起動総数、アプリケーション起動総数、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の遅延です。
ICA RTT	ICA RTTは、ユーザーがそれぞれ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と対話する際に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の世界地図ビューでは、管理者は過去および現在のアクティブユーザーの詳細を地理的な観点から表示できます。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、都市および州ごとの情報を表示するためにさらにドリルダウンできます。NetScaler ADM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の世界地図では次の詳細を表示でき、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

世界地図ビュー(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

ライセンスビューの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 ADM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セッ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。

しきい値レポート

しきい値レポートは、選択した期間においてエンティティがライセンスとして選択されている場合に、侵害され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クス

このビューのレポートとメトリクスは、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。

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

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アプリケーションのレポートが表示されます。

以下に示すすべてのメトリクス/レポートは、明示的に記載されていない限り、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

メトリクス	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	アプリケーションを起動するのにかかる平均時間。

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 を起動するのにかかった平均時間。

アプリケーション概要レポート(/en-us/netscaler-application-delivery-management-software/media/hdx-application-summary-report.png)

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。

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

メトリック	説明
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	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	このアプリケーションのアクティブなセッション数。

しきい値レポート

しきい値レポートは、選択した期間にアプリケーションとしてエンティティが選択された、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。
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/非アクティブな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。

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

メトリック	説明
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 アップサーバー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。
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。

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

メトリック	説明
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: 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 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。
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。
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ます。

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

メトリック	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。
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。
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。

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

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。
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した合計回数。
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。
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。
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。

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. **Gateway > HDX™ Insight > Desktop** に移動します。

概要ビュー

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、すべてのメトリクス/レポートは、選択された期間に対応する値を持っています。

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

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。
# アクティブアプリ	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。

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

メトリクス	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、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。
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。
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)

© 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。

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	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	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。

© 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。
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。

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
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。
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する際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)

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 ADC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	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。
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。

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

メトリック	説明
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。
市町村	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。

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

メトリック	説明
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 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。
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。

© 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。
VDIイメージ名	ユーザーが接続しているCitrix Virtual Desktopの名前
図	

非アクティブなレポート(/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。

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。

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 and 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。

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

メトリック	説明
ICA RTT	ICA RTTは、Citrix Virtual App and 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。
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.

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。
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。

© 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。
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: 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。
VDIイメージ名	ユーザーが接続しているCitrix Virtual Desktopの名前

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：

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

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：

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、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とそれぞれ対話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。
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。

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

メトリクス	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。
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)

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 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、ユーザーがそれぞれ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と対話しているときに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。
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。
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。
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。

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

メトリック	説明
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、ドーナツチャート形式で、各ICA®仮想チャネルによって消費された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する全体的な帯域幅/合計バイト数をドーナツグラフの形式で表します。帯域幅または合計バイト数でメトリックを並べ替えることもできます。

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。

ワールドマップ

HDX Insight のワールドマップビューでは、管理者が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 ADM 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
- 合計バイト数

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

ユーザー別ビュー

ユーザーごとのビューでは、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を表示します。

現在/終了済み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および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 ADC 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。

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

メトリック	説明
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 Apps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。
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。たとえば、NetScaler Gatewayのユーザー/透過モードなどです。
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。

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

メトリック	説明
HAフェールオーバー数	HAフェー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。

© 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。

HDX INSIGHTでのEDTのサポート

NetScaler Application Delivery Management (ADM) 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、ADM は現在、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での高精細なユーザーエクスペリエンスが保証されます。

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、「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。

NetScaler ADM 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遅延の最大値。
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。

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

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	Citrix Virtual 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、ユーザーが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中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ケーションを表す棒グラフ。

インスタンス

アクティブおよび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

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

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。

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。

ユーザーごとのセッションビュー

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クスを表示するには：

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

メトリクス	説明
セッション再接続	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、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。

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

メトリクス	説明
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。
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。

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

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。

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 ADM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。

明示的に記載されていない限り、すべてのメトリック/レポートは、選択された期間に対応する値を持っています。

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。

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

メトリック	説明
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)

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。そのため、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を使用すると、管理者は過去およびアクティブなユーザーの詳細を地理的な観点から表示できます。管理者は、領域をクリックすることで、システムのワールドビューを表示し、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、都市および州別に情報をさらにドリルダウンして表示できます。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

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

- DC遅延
- 帯域幅
- 合計バイト数

インスタンス別ビュー

インスタンス別ビューは、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を提供します。

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。
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、選択したインスタンスのNetScaler IPアドレスを表します。
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。
合計アプリ数	指定された時間間隔に起動されたユニークな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。

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

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

- 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。

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	選択され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。
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。

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、都市や州ごとの

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

情報を表示するためにドリルダウンできます。NetScaler ADM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

ライセンスビューの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。
総ライセンス数	顧客が利用できるNetScaler Gateway CCUライセンスの総数。

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。

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

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、各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 ADM 間の接続。
- NetScaler での HDX/ICA トラフィックのレコード生成。
- NetScaler® ADM でのレコードの投入。

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 HDX 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 HDX Insight の構成を確認します。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/ICA トラフィックが流れている VPN 仮想サーバーに HDX 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。
- 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仮想サーバーで `appflowlog` パラメータがAccess Gatewayまたはダブルホップ展開に対して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の信頼性」を参照してください。

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

NetScalerとNetScaler ADM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®ポリシーヒットを確認します。

  AppFlowポリシー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。

  GUIで**Settings > AppFlow > Policies**に移動して、AppFlowポリシーヒット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検証します。

NetScalerでの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: サポートされていないバージョンのCitrix Workspace

  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

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

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が見つかりません**

  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。サポートされているバージョンのCitrix Workspaceアプリを使用していることを確認してください。

- 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 エク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ためのバイトが不足しています

© 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
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チャネルで指定されたパラメーター数が無効です
108	NS_ICA_ERR_INVALID_TW_DECODER	Thinwireチャネルのデコーダが無効です
109	NS_ICA_ERR_REDUC_NO_DECODER	チャネルにデコーダ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

© 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
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XenDesktopバージョン5.0未満を示します
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が不足しています
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

© 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
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
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確認されています。
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA署名またはマジック文字列が不正です。
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

© 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
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	クライアント再接続クッキーの解析状態を検出できません
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	展開エラー
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の解析に無効なイベントです
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRLチャネル解析用の無効なイベント

© 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
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
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化コマンド
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5暗号化/復号化におけるエラー
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5暗号化/復号化におけるエラー
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

© 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
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICAハンドシェイクにおける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
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	サービスノードでのサービス再接続チケットの取得エラー

© 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
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のエラー
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	非NSAP接続のHDX Insightを無効にしているときのエラー

ログの例:

```
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。以下の表に、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、`nsconmsg -g hdx -d statswt0`コマンドを実行します。

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	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）
	ICA接続が検出されるたびに増加します。	
hdx_tot_cgp_conn	NSによって検出されたCGP接続の総数（セッション信頼性ON）を示します。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署名のため、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を無効にしたために、AppFlowがセッションからデタッチされたインスタンスの総数。	統計/診断
hdx_dbg_transparent_user	透明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総数	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_dbg_lan_user	LANユーザーモードアクセスの総数	統計/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総数	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	`nsapimgr` ノブを使用してセッションの信頼性が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であることを示しており、HDX Insightはこの接続をスキップします。	エラー
hdx_err_skip_old_server	サポートされていない古いサーバーバージョン	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_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、HDX Insightはこの接続をスキップします	エラー
hdx_sm_ica_cam_channel_disabled	SmartAccessポリシーによって無効化された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化された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化された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化された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

© 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_sm_ica_cpm_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_CPM_CHANNELの総数	診断
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	USBエンドポイントのリセット総数	診断
hdx_dbg_usb_reset_device	USBデバイスのリセット総数	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

© 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_gone	消失したUSBデバイスの総数	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

CFLOWプロトコルをチェックして、NetScalerから出力されるすべてのAppFlowレコードを確認します。

NetScaler ADMチェックリスト内のレコードの入力

- コマンド`tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`を実行し、ログをチェックして、NetScaler ADM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 ADM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 ADMで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ます。
- 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ます。

Citrixテクニカルサポートに問い合わせる前に

迅速な解決のために、Citrixテクニカルサポートに問い合わせる前に、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 ADMのバージョン。
- Citrix Virtual Apps and Desktops サーバーバージョン。
- 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テクニカルサポートバンドル。
- NetScaler ADM用に取得したテクニカルサポートバンドル。

© 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、ADC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 ADMは、NetScalerインスタンスの検出、監視、管理を可能にする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
- アップグレードジョブ
- オーケストレーション
- ビデオインサイト

インフラストラクチャ分析

ネットワーク管理者の主要な目標は、NetScalerインスタンスを監視することです。ADCインスタンスは、それを介し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、ADCインスタンスを監視し、各ADC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、構成、セットアップ、接続、証明書など、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問題を修正できます。たとえば、アプリケーションの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、または構成変更に関する問題がないこと
- 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、それをインスタンスの健全性を定義する測定可能なスコアに定量化することで、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、および実行可能な修正策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 Application Delivery Management (ADM) 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**に定量化します。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、ADC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を意味します。インスタンススコアは、インスタンス上の潜在的な問題のさまざまなレベルを捉えます。これはインスタンスの健全性の定量的な測定値であり、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、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、事前に定義された「監視期間」に対して定期的にスコアが計算されます。現在、インフラストラクチャ分析は、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
- 構成偏差インジケータ

健全性インジケータ

- システムリソースインジケータ

  以下は、NetScalerインスタンスで発生し、NetScaler ADMによって監視される可能性のある重要なシステムリソースの問題です。

  - **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**。ADC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**。電源が故障したか、ADCインスタンスから切断されました。
- **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、「インスタンスダッシュボード」を参照してください。

- 重大イベントインジケータ

  以下の重大イベントは、ADMのイベント管理機能の下で、重大度「クリティカル」に設定されているイベントによって識別されます。

  - **HA同期失敗**。高可用性構成のADC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ADCインスタンスのペアの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ADCインスタンスのペアの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ADCインスタンスのペアにインストールされているADC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ADC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ADCインスタンスにインストールされているADC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、「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」を参照してください。

NetScaler ADMのイベントの詳細については、「イベント」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**。ADC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証明書の期限が近づいています**。ADCインスタンスにインストールされているSSL証明書は、今後1週間で期限切れになります。
  - **推奨されないアルゴリズム**。ADC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は、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。

構成の逸脱と、構成の逸脱を確認するための監査レポートの実行方法の詳細については、監査レポートの表示を参照してください。

ADC容量の問題を表示する

ADC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、ADC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ADC容量の問題を理解することで、ADC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。

ADC容量の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. 容量の問題を表示したいインスタンスを展開します。

ADMは、ADCインスタンスからこれらのイベントを5分ごとにポーリングし、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。

ADM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、ADC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、`ADCCapacityBreach` 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。

健全性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。

同じインジケーターグループ内の健全性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、メモリ使用量が高い場合、ディスク使用量が高い場合、CPU使用量が高い場合、NIC破棄よりも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、次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。

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

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もクリアされ、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、しきい値レベルが侵害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. **低しきい値と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せられます。
    - 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せられます。
    - 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せられません。

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。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。

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接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

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

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、Circle Pack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。

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。

グループ化されたインスタンスの円

Circle Packは当初、以下の基準に基づいて、グループ化、ネスト化、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。

- それらが展開されているサイト
- 展開されているインスタンスのタイプ - VPX、MPX、SDX、およびCPX
- ADC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ADCイメージバージョン

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-citrix.png)

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

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 ADM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ーを表しています。

クラスター化されたインスタンスの円

NetScaler ADM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は別のグループ化の中にネストできます。

たとえば、BLRデータセンターには、VPXとMPXの2種類のADCインスタンスがデプロイされています。まずADC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何種類のインスタンスがデプロイされているか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-citrix.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いくつか示します。

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)

Circle Pack の使用方法

色付きの各円をクリックして、そのインスタンスを強調表示します。

Circle Pack の使用方法の図(/en-us/netscaler-application-delivery-management-software/media/circle-pack-how-to.png)

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

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。

Circle Pack の図(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-10.png)

健全性インジケーターをクリックすると、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サマリーレポートを表示します。

Circle Pack の図(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-11.png)

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
- リスク指標の総数
- 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

危険な状態にあるインスタンスがテーブルの最上位に表示され、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(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-12.png)

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.

レポートに関連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。

表形式ビュー(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-20.png)

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。

表形式ビュー(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-13.png)

展開されたテーブル行には、すべてのカテゴリでインスタンスに発生した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。しかし、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。

サマリーパネルの使用方法

サマリーパネルは、レビューが必要なインスタンスや危険な状態にある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
- メモリ使用率
- 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

以下の例は、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:

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

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。

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、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ると、グラフの下部にある凡例にその使用範囲と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は、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:

ディスク容量を0%から10%の間で消費している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。

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: 有効期限切れのSSL証明書のインスタンスを表示する:

1 - **フィルター**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、「**期限切れ**」チェックボックスを選択してインスタンスを表示します。

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

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。

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、**サークルパック**または表形式を選択します。選択した形式は、NetScaler ADMでページにアクセスするたびに表示されます。
- **サークルパック - インスタンスサイズ**。インスタンスサークルのサイズを、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。
- **サークルパック - クラスター化の基準**。インスタンスサークルの2レベルクラスタリングを決定します。インスタンス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サークル」を参照してください。

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

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。

注

これらの変更を適用するには、**設定の適用**をクリックするか、すべての変更を削除するには、**リセット**をクリックします。

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す。データ視覚化をさらに詳しく理解するために、ExampleCompanyのネットワーク管理者であるクリスの場合を考えてみましょう。

Chrisは組織内で多くの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、Chrisはそれらを綿密に監視する必要があります。Chrisは、いくつかの高トラフィックインスタンスが、それらを通過するトラフィック全体を処理しなくなっていることに気づきました。この減少を分析するために、以前はChrisはさまざまなソースから来る複数のデータレポートを読み込む必要がありました。Chris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。

Chrisは、すべてのインスタンスの健全性を視覚的に確認するために、Infrastructure Analytics機能を使用します。

以下の2つの例は、Infrastructure AnalyticsがChrisのメンテナンス活動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:

Chris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、そのインスタンスが「Critical」状態にあることに気づきました。Chris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、インスタンスが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。Chrisはその情報を抽出し、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:

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

Chrisはまた、別のインスタンスが「Review」状態にあり、最近設定の逸脱があったことにも気づきました。Chris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、TLS 1.1に関連する設定変更が行われており、これはセキュリティ上の懸念によるものである可能性があることに気づきました。Chrisはまた、このインスタンスのSSLトランザ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。Chrisはこのレポートをエクスポートし、さらに調査するために管理者に送信します。

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

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。

   また、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** – ADC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** – ADCインスタンスのIPアドレスを示します
- **スコア** – ADC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** – **稼働中**、**停止中**、または**サービス停止中**など、ADCインスタンスのステータスを示します。
- **最大寄与度** – ADC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における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** – ADC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ADCインスタンスタイプを示します
- **展開** – ADC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** – ADCインスタンスのモデル番号を示します

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

- **バージョン** – ADC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** – ADC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
- **HTTPSリクエスト/秒** – ADC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** – 確立されている現在のTCP接続を示します
- **SSLトランザクション** – ADC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** – ADC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 – 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。

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

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および無効になっているネットワークインターフェー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ース名やステータス（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 – ADC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。

- **主要メトリクス**

  各タブをクリックして詳細を表示します。各メトリクスでは、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、最初の値は**139**で、最後の値は**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クス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の両方で表示されます）。
  - **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リクエスト/秒** – 選択した期間におけるインスタンスが受信した平均HTTPSリクエスト数。
  - **TCP接続** – 選択した期間における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** – 選択した期間における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。	- CPU使用率が高い
		- メモリ使用率が高い
		- ディスク使用率が高い
		- SSLカードの障害
		- 電源障害
		- ディスクエラー
		- フラッシュエラー
		- NIC破棄
SSL構成	NetScalerインスタンス上のSSL構成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セカンダリ状態不良
		- 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、インスタンスに選択した期間の次のエラーがあるとします。

- **現在の**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。
- **すべての**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。

ADCインスタンスのキャパシティ問題を表示する

ADC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、ADC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ADCのキャパシティ問題を理解することで、ADC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、ADC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。

ADCのキャパシティ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。

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

2. サークルパックビューを選択します。

注

Infrastructure Analytics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する(/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。

容量の問題を解決するための推奨アクションを表示する

ADMは、容量の問題を解決できるアクションを推奨します。推奨されるアクションを表示するには、次の手順を実行します。

1. **インフラストラクチャ > インフラストラクチャ分析**で、表形式ビューを選択します。
2. 容量の問題があるインスタンスを選択し、**詳細**をクリックします。

   インスタンスの詳細(/en-us/netscaler-application-delivery-management-software/media/instance-details-citrix.png)
3. インスタンスページで、**問題**セクションまでスクロールします。
4. 各問題を選択し、容量の問題を解決するための推奨アクションを表示します。

   容量の問題を解決するための推奨アクション(/en-us/netscaler-application-delivery-management-software/media/adc-capacity-issues-drill-down.gif)

ADMは、ADC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.

ADM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つの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個の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、ADC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されたり、レート制限カウンターが増加したりすると、`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、**アカウント > システムイベント**に移動します。

新しいインジケーターによるインフラストラクチャ分析の強化

NetScaler® ADM 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 ADM 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 が新しいサーバー接続と通信するために SNIP を使用し、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
デフォルトルート設定なし	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。ADC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数が課されたときに検出します。
GSLBサイト名の不一致	サイト名の不一致によりGSLB設定の同期失敗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キータイプが使用されているために、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。

をクリックすると、詳細が表示されます。

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

インスタンスは、NetScaler Application Delivery Management (ADM) を使用して管理、監視、トラブルシューティングできるCitrix Application Delivery Controller™ (ADC) アプライアンスです。インスタンスを監視するには、NetScaler ADM に追加する必要があります。インスタンスは、NetScaler ADM のセットアップ時または後で追加できます。NetScaler ADM にインスタンスを追加すると、問題の解決やレポートデータとして後で使用できる情報を収集するために、継続的にポーリングされます。

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

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。

インスタンスの追加

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

NetScaler ADM 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 ADM 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、**インフラストラクチャ > インスタンス** に移動し、**すべてのインスタンス** をクリックして削除できます。インスタンスページで、削除するインスタンスを選択し、**削除** 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® ADM 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およびグラフィカル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1分ごとにデータ収集のために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、メモリ使用量、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、これらすべての収集されたデータを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に即座に行動を起こすことができます。

特定のインスタンスのダッシュボードを表示するには、**インフラストラクチャ > インスタンス** 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 **ダッシュボード** 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。

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

- **概要**。概要タブには、選択したインスタンスのCPUとメモリの使用状況が表示されます。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、連絡先などのイ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** グラフには、保存済み構成と未保存構成における構成変更に関する大まかな詳細が表示されます。
- **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して、選択したNetScalerインスタンスに設定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、画面の右下隅にある「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® Application Delivery Management (ADM) のジオマップは、サイトのグラフィカルな表現を提供し、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。

次のセクションでは、NetScaler ADM でデータセンターを監視する方法について説明します。

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

NetScaler ADM サイトは、特定の地理的場所にあるCitrix Application Delivery Controller (ADC) 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敷地内にホストされます。NetScaler ADMは、すべてのサイトに接続されているすべてのNetScalerインスタンスを管理および監視します。NetScaler ADM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 ADM のジオマップは、サイトのグラフィカルな表現を提供します。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現については、**インフラストラクチャ > インスタンス** ページに移動してください。

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、タブをクリックしてください。

- **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
  - 発生した重大イベントの数
  - 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リスト
  - 有効期限ステータス

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

- 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。

  エージェントの表示(/en-us/netscaler-application-delivery-management-software/media/nmaservice-global-datacenters-3.png)

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 ADM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、その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 ADM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 ADM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。

「**Infrastucture > Instances > Sites**」に移動し、「**Add**」をクリックします。

1. 「**Create Site**」ページで、次の情報を指定します。

   a. **Site Type**: 「**Data Center**」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. **Type**: 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**
   >
   > それに応じて「**Use existing VPC as a site**」チェックボックスをオンにします。

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

c. **Site Name**: サイトの名前を入力します。
d. **City**: 都市を入力します。
e. **Zip Code**: 郵便番号を入力します。
f. **Region**: 地域を入力します。
g. **Country**: 国を入力します。
h. **Latitude**: 位置の緯度を入力します。
i. **Longitude**: 位置の経度を入力します。

2. 「**作成**」をクリックします。

ジオマップを作成(/en-us/netscaler-application-delivery-management-software/media/createsite.png)

インスタンスを追加してサイトを選択するには:

サイトを作成した後、NetScaler ADM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。

サイトを作成した後、NetScaler ADM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 ADMで、 **>** に移動します。
2. 作成するインスタンスの種類を選択し、 をクリックします。
3. 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。 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。

エージェントを選択(/en-us/netscaler-application-delivery-management-software/media/nmaservice-global-datacenters-5.png)

6. エージェントを選択した後、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、 をクリックします。

サイトをアタッチ(/en-us/netscaler-application-delivery-management-software/media/nmaservice-global-datacenters-6.png)

リストからサイトを選択し、 をクリックします。

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

をクリックします。

「**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 ADM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、「**Save**」をクリックします。

NetScaler ADM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 Application Delivery Management (ADM) では、Citrix Application Delivery Controller™ (ADC) 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、これらの特定のキーワードに基づいてインスタンスを分類し、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、クライアント要求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. であるあなたが所有する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。

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

NetScaler VPXインスタンスにタグを割り当てるには:

1. NetScaler ADMで、**Infrastructure > Instances > NetScaler** の順に移動します。
2. **NetScaler VPX** タブを選択します。
3. 必要なNetScaler VPXを選択します。
4. **タグ** 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 **タグ** 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、次の図は、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。

複数のタグを追加(/en-us/netscaler-application-delivery-management-software/media/instance-tags-example2.png)

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。

たとえば、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® ADM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。

複数の値を追加(/en-us/netscaler-application-delivery-management-software/media/instance-tags-example3.png)

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。

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

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 Application Delivery Management (ADM) 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 ADM は現在、検索フィールドで定義する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。

- **タグ**。タグとは、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。これで、NetScaler インスタンスにタグを関連付けることができます。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 ADM 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状態の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、自分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 ADM 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、あるいはその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® ADM 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。

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

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とします。そのような場合、値を「\|」式で区切って入力できます。

   正規のインスタンスを使用してインスタンスを検索(/en-us/netscaler-application-delivery-management-software/media/instance-search-tags-properties-3-citrix.png)

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。

   ワイルドカードを使用してインスタンスを検索(/en-us/netscaler-application-delivery-management-software/media/instance-search-tags-properties-4-citrix.png)

   注意

   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インスタンスの管理パーティションを管理する

Citrix Application Delivery Controller (ADC) インスタンスで管理パーティションを構成すると、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® Application Delivery Management (ADM) は、単一のコンソールから管理者が所有するすべてのパーティションをシームレスに管理する方法を提供します。他のパーティション構成を中断することなく、これらのパーティションを管理できます。

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 ADMの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インスタンスで構成された管理パーティションは、自動的にシステムに追加されます。

各インスタンスに2つのパーティションが構成された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（次の画像に示すとおり）。

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

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、分割された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、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、分割されたNetScalerインスタンスをクリックします。

2. **Action** メニューから、**Revision History Diff** をクリックします。

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。

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

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の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。また、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。

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。

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差異を表示します。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。
   - **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。

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

グループの作成(/en-us/netscaler-application-delivery-management-software/media/create-system-group.png)

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の資格情報でログオンします。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 ADMを使用してADC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® ADMでADC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**に移動します。
2. HAペアを作成するADC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が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。

   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ADCインスタンスを選択します。

   c. オプションで、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。

   ▢
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。

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

- **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、このタスクを実行したい**実行日**と**開始時刻**を選択します。

> **注**
>
> 実行時刻は、NetScaler ADMで設定されているタイムゾーンで表示されます。

ADC HAペアタスクまたはジョブを実行(/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、以下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-citrix.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。

  Slackプロファイル(/en-us/netscaler-application-delivery-management-software/media/upgrade-slack-citrix.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状態に復元できます。

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。また、NetScaler ADM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 ADM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 ADM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

詳細については、「ADC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。

注

- NetScaler® ADMプロファイルに、ADC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 ADMからは、NetScalerクラスターで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、圧縮されたTARファイルとして次のディレクトリに保存されます。

```
/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ADC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 ADM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。

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

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 ADMで構成できます。

1. NetScaler ADM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 ADM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 ADM 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 ADMで保持するバックアップファイルの数を指定します。ADC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。

  注

  各バックアップファイルには、ある程度のストレージ要件があります。Citrixは、要件に応じて最適な数のNetScalerバックアップファイルをNetScaler ADMに保存することを推奨します。

  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/configuring-instance-backup-settings-1.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。

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

a. デフォルトのバックアップスケジューリングオプションは「間隔ベース」です。指定された間隔が経過すると、NetScaler ADM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 ADM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 ADM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。ただし、NetScalerインスタンスがNetScaler ADM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。
- **地理データベースファイル**：（オプション）デフォルトでは、NetScaler ADMは地理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を有効にすることもできます。

  NetScaler設定の指定(/en-us/netscaler-application-delivery-management-software/media/configuring-instance-backup-settings-3.jpg)
- **外部転送**：（オプション）NetScaler ADM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 ADM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)

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

注

NetScaler ADM 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 ADM 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 ADM で、**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** 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、**アクションの選択** リストから **バックアップ/復元** を選択します。
   - SDX インスタンスの場合は、**バックアップ/復元** をクリックします。
3. **バックアップファイル** ページで、**バックアップ** 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、インスタンスバックアップ設定 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. **続行** をクリックします。

NetScaler ADM 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 ADC 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 ADC 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

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

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. **Infrastructure > Instances** に移動し、復元するインスタンスを選択して、**View Backup** をクリックします。
2. **Backup Files** ページで、復元したい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表示(/en-us/netscaler-application-delivery-management-software/media/configuring-instance-backup-settings-5.jpg)

NetScaler ADM を使用して NetScaler SDX アプライアンスを復元する

NetScaler ADM 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）
- 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、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が付与されており、バックアップファイルの最小

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

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は復元できません。

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 ADM GUIで、**Infrastructure > Instances > NetScaler** に移動します。
2. **Backup/Restore** をクリックします。
3. 復元したい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スペース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アプライアンスの正常な復元を保証します。
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。

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

You might want to force a failover if, for example, you need to replace or upgrade the primary Citrix Application Delivery Controller™ (ADC) instance. You can force failover from either the primary instance or the secondary instance. When you force a failover on the primary instance, the primary

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

becomes the secondary and the secondary becomes the primary. Forced failover is only possible when the primary instance can determine that the secondary instance is UP.

強制フェイルオーバーは伝播または同期されません。強制フェイ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。

強制フェイルオーバーは、以下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イ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、フェイ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。

NetScalerインスタンスは、強制フェイ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、警告メッセージを表示します。メッセージには、警告をトリガーした情報が含まれ、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イルオーバーを強制できます。

NetScaler ADM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には：

1. In NetScaler Application Delivery Management (ADM), navigate to **Infrastructure > Instances > NetScaler > VPX** tab, and then select an instance .
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、強制フェイルオーバーアクションを確認します。

   強制フェイルオーバーを作成する (/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。

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

例えば、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を検出した場合でも、セカンダリノードのままであってほしいのです。

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ペア内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、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 ADM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 Application Delivery Management (ADM)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セットアップ内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。
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。

インスタンスグループの作成

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 ADM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アップグレード、バックアップ、または復元を一度に実行できます。

NetScaler® ADMを使用してインスタンスグループを作成するには

1. NetScaler ADMで、**Infrastructure > 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。

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

3. **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、選択し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する場合は、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。

4. **Create**をクリックします。

インスタンスグループの作成(/en-us/netscaler-application-delivery-management-software/media/024_instancegroups.png)

ADM を使用して SDX 上に NetScaler VPX インスタンスをプロビジョニングする

NetScaler ADM を使用して、SDX アプライアンス上に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、ADM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ADM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

ADM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** - ADC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、ADM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

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

る）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ついて、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ADMサーバーに割り当てます。

- **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。XVAファイルを選択するには、次のいずれかのオプションを使用します。
  - **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** - ADM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、ADM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)

© 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、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。

リソースの割り当て(/en-us/netscaler-application-delivery-management-software/media/resource-allocation.png)

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可能なコア数を示します。

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

© 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 8900	8	7	7
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、および11.0と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

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

注

SDX 26xxxプラットフォームでは、VPXインスタンスに最大26個のCPUコアを割り当てることができます。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。

たとえば、インスタンスに24000個の暗号ユニットを割り当てる場合、24個のCPUコアと最大2つのデータインターフェイスを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イスと暗号ユニットをPCIデバイスと見なします。26000個の暗号ユニットの場合、データインターフェイ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、**Instance Administration**セクションで**Add Instance Administration**を選択します。

次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とインターフェイスを構成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。
- **Shell/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。

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。

- **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。

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

> **注**
>
> インスタンスのL2モードを無効にする場合は、インスタンスにログオンして、そのインスタンスから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、管理インターフェイスのVLAN IDを指定します。
- **0/2** - **VLANタグ**で、管理インターフェイスのVLAN IDを指定します。

デフォルトでは、インターフェイス**0/1**と**0/2**が選択されています。

ネットワーク設定(/en-us/netscaler-application-delivery-management-software/media/network-settings.png)

データインターフェイスで、**追加**をクリックしてデータインターフェイスを追加し、以下を指定します。

- **インターフェイス** - リストからインターフェイスを選択します。

  > **注**
  >
  > インスタンスに追加するインターフェイスのインターフェイスIDは、必ずしもSDXアプライアンスの物理インターフェイス番号に対応するとは限りません。

  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イスがSDXインターフェイス1/4の場合、そのインスタンスでインターフェイス設定を表示すると、インターフェイス1/1として表示されます。このインターフェイスは、インスタンス-1に関連付けられた最初のインターフェイ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** - 生成されたMACアドレスを上書きするMACアドレスを指定するには、このモードを選択します。
  - **生成済み** - 以前に設定したベース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)**

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

- **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、「インターフェイスでの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、「インターフェイスでのVMACの構成」を参照してください。

☐ **追加**をクリックします。

手順6 - 管理VLAN設定を指定する

管理サービスとVPXインスタンスの管理アドレス (NSIP) が同じサブネットワークにある場合、通信は管理インターフェイ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なときにネットワーク経由で到達可能になります。

VPXインスタンスのプロビジョニング中に、NSIPが選択したインターフェイスを介してのみアクセス可能である必要がある展開の場合は、**NSVLAN**を選択します。これにより、NSIPは他のインターフェイスを介して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イ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。
- VPXインスタンスの`clear config full`コマンドは、**NSVLAN**が選択されていない場合、VLAN設定を削除します。

☐ 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。

プロビジョニングされたVPXインスタンスを表示する

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IPを指定します。

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

VMware ESX で NetScaler VPX インスタンスをプロビジョニングする

ADM を使用して、VMware ESX で NetScaler VPX インスタンスの展開と管理を自動化できます。NetScaler ADM を使用して VMware ESX 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 ADM GUI で管理できるようになります。

NetScaler® ADM は、すでに展開されているインスタンスの ADC 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 サーバーの詳細はサイトに保存されます。また、サーバーへのアクセスには Cloud Access Profile を使用します。

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、6.7) をインストールします。
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 をインストールします。
3. NetScaler VPX セットアップファイルをダウンロードする。
4. NetScaler VPX ファイルを ESX のテンプレートに変換する。
5. ADM でサイトを作成する。

NetScaler VPX ファイルをテンプレートに変換する

NetScaler ADM は、NetScaler VPX ファイルによって変換された ESX 内の ADC 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. ADC セットアップファイルを使用して、VMware に NetScaler VPX インスタンスを展開します。

   初回は、ADC 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 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。
2. 展開された VM を右クリックし、**Template** を選択します。
3. 「**テンプレートに変換**」をクリックします。

ADMでサイトを作成

NetScaler ADMでサイトを作成し、VMware ESXの詳細を追加します。

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

1. NetScaler ADMで、**Infrastructure > Instances > Sites**に移動します。
2. 「**追加**」をクリックします。
3. 「**クラウドの選択**」ペインで、,
   a. **サイト**タイプとして**データセンター**を選択します。
   b. **タイプ**リストから**VMware vCenter**を選択します。
   c. 「**次へ**」をクリックします。
4. 「**リージョンの選択**」ペインで、,
   a. 「**クラウドアクセスプロファイル**」ペインで、VMware ESX用に作成され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、「**追加**」をクリックし、以下を指定します。
      - **名前** – NetScaler ADM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。

      クラウドアクセスプロファイルの作成(/en-us/netscaler-application-delivery-management-software/media/cap-vmware-citrix.png)
   c. **ネットワーク (データセンター)**で、ADC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特定するために、**地域**、**緯度**、**経度**を指定します。
   f. **完了**をクリックします。

VMwareでインスタンスプロビジョニング用のサイトを作成する(/en-us/netscaler-application-delivery-management-software/media/create-site-citrix.png)

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

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 ADMはスタンドアロンADC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 ADM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、**プロビジョニング**をクリックします。

   このオプションにより、**クラウドでのNetScaler VPXのプロビジョニング**ページが表示されます。
3. 「**VMware vCenter**」を選択し、「**Next**」をクリックします。

   VMware vCenterの選択(/en-us/netscaler-application-delivery-management-software/media/select-vmware-citrix.png)
4. 「**基本パラメータ**」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ADC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-citrix.png)
5. 「**Next**」をクリックします。
6. 「**プロビジョニングパラメータ**」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。

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

- 「**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. **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 Application Delivery Management (ADM) のセットアップで、複数のNetScaler VPXインスタンスを再検出できます。また、こ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 ADMサーバーは、すべてのNetScaler VPXインスタンスを再検出し、Citrix Application Delivery Controller (ADC) インスタンスに到達可能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：

1. Webブラウザで、NetScaler ADM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**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。デフォルトの管理者資格情報は`nsroot`と`nsroot`です。
3. **インフラストラクチャ > インスタンス > 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® Application Delivery Management (ADM) 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。

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て「**Select Action**」リストから「**Unmanage**」を選択します。

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

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)

インスタンスはNetScaler ADMによって管理されなくなり、NetScaler ADMとのデータ交換も行われなくなります。

インスタンスへの経路をトレースする

NetScaler® Application Delivery Management (ADM) からインスタンスへのパケットの経路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。Traceroute は、送信元から宛先へのパケットのパスをトレースします。経路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。

インスタンスの経路をトレースするには:

1. NetScaler ADM 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、インスタンスへの経路と、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インスタンス間で構成をレプリケートする

NetScaler® ADMの「構成のレプリケート」機能を使用すると、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。

あるインスタンスから他のNetScalerインスタンスへ構成をレプリケートするには

1. **Infrastructure > Instances > 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、**Select Action**リストから**Replicate Configuration**をクリックします。
2. **Replicate Configuration**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。

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

3. **Create**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は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、**Infrastructure > Network Functions**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処理を必要とする組織または個人のウェブサイトには、SSL証明書が必要です。ウェブサーバー上のSSL証明書は、接続するクライアントに対してウェブサーバーの信頼性を保証するのに役立ちます。これは、ウェブサイトのIDを認証するだけでなく、セッションキーの生成にも役立ち、このセッションキーは後でセッション全体の暗号化に使用されます。

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。この証明書には公開鍵コンポーネントがあり、サーバーとの安全なトランザクションを開始したいすべてのクライアントに表示されます。Citrix Application Delivery Controller™ (ADC) 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。

NetScaler® Application Delivery Management (ADM) 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、ウェブ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 ADM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、アルゴリズムを確保するための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

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

- 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、そのようなすべての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 ADM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。

非準拠 (推奨されません) 証明書の概要は、SSLダッシュボードで確認できます。

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 ADM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。

- **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、使用済みおよび未使用のSSL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されずに見落とさ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。

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

- **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ダッシュボード(/en-us/netscaler-application-delivery-management-software/media/ssl-dashboard-page.png)

SSL証明書管理のユースケース

以下のユースケースでは、複数のNetScalerインスタンス間でSSL証明書を管理および監視するためにSSL証明書をどのように使用できるかを説明します。

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 ADMは、複数のNetScalerインスタンスにSSL証明書を一度に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つ以上の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つ以上のNetScalerインスタンスにわたってSSL証明書の一括インストールを実行できます。

SSL証明書の概要を取得するには、**NetScaler ADM**にログオンし、**Infrastructure > SSL Dashboard**に移動します。

証明書有効期限の通知設定

このユースケースでは、複数のNetScalerインスタンスに多数の証明書がある場合があり、各証明書の有効期限を追跡するのは負担になります。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のは面倒な作業です。このようなシナリオを避けるために、NetScaler ADMを設定して、構成済みの電子メール、ポケットベル、Slack、または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、多数のアプリケーションがユーザーに影響を与える可能性があります。ADM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、概要を表示し、有効期限が近づいている証明書を追跡できます。

任意の期間で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。

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

有効期限切れSSL証明書(/en-us/netscaler-application-delivery-management-software/media/expiry-ssl-certificate.png)

証明書の更新

NetScaler ADM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。

既存の証明書の更新

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 ADM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 ADMからSSL証明書を更新できるようになりました。

いずれかの証明書を更新するには、NetScaler ADMにログオンし、**インフラストラクチャ > SSL ダッシュボード**に移動します。

更新する証明書を選択し、**更新**をクリックします。

NetScaler ADM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。

更新SSL証明書ページ(/en-us/netscaler-application-delivery-management-software/media/update-ssl-certificate-page.png)

証明書署名要求の作成

SSL証明書の1つが組織のポリシーに準拠していないユースケースを想像してみてください。認証局から新しい証明書を取得したいとします。NetScaler ADM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、**Create CSR** 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。キーをアップロードするには、**Choose File** をクリックしてリストから選択します。キーを作成するには、**I do not have a Key option** を選択し、関連するパラメータを指定します。

キーペアCSRを作成(/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、州、組織単位、メールIDなどの詳細情報を提供します。

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

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 ADM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 ADMを使用して特定のNetScalerアプライアンスに追加、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、特定の操作の開始時刻、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、**SSL Dashboard** で **Audit Log** 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)

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、関連する証明書のチェックボックスを選択します。**Device Log** をクリックします。

デバイスログ監査証跡(/en-us/netscaler-application-delivery-management-software/media/device-log-audit-trail.png)

コマンドの種類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。

コマンドログ監査証跡(/en-us/netscaler-application-delivery-management-software/media/command-log-audit-trail.png)

SSLダッシュボードを使用する

NetScaler® Application Delivery Management (ADM) のSSL証明書ダッシュボードを使用して、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。

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

- 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2048ビット以上の最小キー強度を持ち、信頼できるCA機関が承認する必要があるなど、特定のSSL証明書要件を定義している場合、NetScaler ADM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 ADM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。

NetScaler ADM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 ADMに即座に追加できます。これを行うには、,

1. 「**Infrasturcture > 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ADC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、ADC 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。

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

たとえば、ダッシュボードの「**Self signed vs CA signed**」の下にある数字をクリックすると、ADM 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。

ADC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 ADM 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。管理者として、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、「SSLポリシーの構成」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、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されると、ドーナツチャートが表示されます。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との安全な通信を可能にします。適切なチャートをクリックすると、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 ADMでSSL証明書のログ詳細を表示できるようになりました。ログ詳細には、NetScaler ADM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 ADM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 ADM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、すべての証明書がデフォルト証明書を含めてSSLダッシュボードに表示されます。

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

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 ADM 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を入力して、証明書の有効期限に関する通知を受け取ります。
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 ADMでSSLファイルを表示するには、**Infrastructure > SSL Dashboard > SSL Files on NetScaler ADM**に移動します。

このページでは、NetScaler ADMで次のファイルを表示、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ファイルにアクセスできるのは、NetScalerインスタンスが手動で、またはスケジュールされたバックアッププロセスを通じてバックアップされた後のみです。

重要:

ADC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、**インスタンスSSL証明書**機能を有効にします。詳細については、ADM機能の有効化または無効化を参照してください。

SSL証明書の有効期限切れに関する通知を設定する

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、およびどのCitrix Application Delivery Controller™ (ADC) 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通知する設定を行うことができます。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。

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

たとえば、証明書の有効期限が切れる30日前に、電子メール配布リストに電子メール通知を送信するように設定できます。

NetScaler® ADMから通知を設定するには：

1. NetScaler アプリケーション デリバリー マネジメント (ADM) で、**Infrastructure > SSL Dashboard** に移動します。
2. ページで、 をクリックします。
3. **SSL Settings** ページで、**Edit** アイコンをクリックします。
4. 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 ADM と統合されていることを確認します。詳細については、「NetScaler ADM と ServiceNow インスタンスを統合する」(/ja-jp/netscaler-application-delivery-management-software/13-1/configure/integrate-itsm-adapter-citrix-adm-servicenow.html) を参照してください。

     SSL証明書の有効期限切れの通知(/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 ADM は、SSL証明書の有効期限が近づくと、SSL証明書の有効期限切れトラップを外部トラップ宛先サーバーに送信するようになりました。NetScaler ADM 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。

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

- 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構成しました。
- トラップ宛先を追加しました。

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。

インストール済みの証明書を更新する

認証局 (CA) から更新された証明書を受け取った後、個々のCitrix Application Delivery Controller™ (ADC) インスタンスにログオンすることなく、NetScaler Application Delivery Management (ADM) から既存の証明書を更新できます。

NetScaler® ADMからSSL証明書、キー、またはその両方を更新するには：

1. NetScaler ADM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 Certificates** ページで、証明書を選択し、**Update** をクリックします。または、SSL証明書をクリックして詳細を表示し、**SSL Certificate** ページの右上隅にある **Update** をクリックします。
4. **Update SSL Certificate** ページで、証明書、キー、またはその両方に必要な変更を加え、**OK** 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

Citrix Application Delivery Controller™ (ADC) 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、証明書キーの鍵強度が2048ビット以上であり、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。

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：

選択したNetScalerインスタンスから証明書をインポートし、NetScaler Application Delivery Management (ADM) GUIから他のターゲットNetScalerインスタンスに適用することもできます。

1. **>** の順に移動します。
2. SSLダッシュボードの右上隅にある をクリックします。
3. ページで、次のパラメータを指定します。

    a. 証明書ソース オプションを選択します。

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

- 証明書をインポートする 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 を選択します。

b. 証明書の詳細

- 。証明書キーの名前を指定します。
- 。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. 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。
5. 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® ADMからSSL証明書をインストールするには：

1. NetScaler ADMで、**Infrastructure > SSL Dashboard** に移動します。
2. ダッシュボードの右上隅にある **Install** をクリックします。
3. **Install SSL Certificate on NetScaler Instance** ページで、**Upload Certificates File** を選択し、次のパラメーターを指定します。
   - **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 ADM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。
   - **キーファイル** - キーファイルをアップロードします。
   - **証明書名** – 証明書キーの名前を指定します。
   - **パスワード** - プライベート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、暗号化されたプライベートキーをアップロードできます。
   - **インスタンスの選択** - 証明書をインストールするNetScaler ADMインスタンスを選択します。
4. 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。
5. **OK** をクリックします。

ADM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)

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

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上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、コモンネーム (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® ADM を使用して CSR を作成するには:

1. NetScaler Application Delivery Management (ADM) の管理画面で、**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インストールされているSSL証明書のリストを表示し、次に、CSRを作成したい証明書を選択し、**Select Action** リストから **Create CSR** を選択します。
3. **Create Certificate Signing Request (CSR)** 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** - **I have a Key** 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、**Local** (ローカルマシン) または **Appliance** (キーファイルはNetScaler ADM仮想インスタンス上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** - I do not have a Key オプションを選択し、次のパラメーターを指定します。

暗号化アルゴリズム	キーの種類。例: RSA。
キーファイル名	RSAキーが保存されるファイルの名称。
キーサイズ	ビット単位のキーサイズ。
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**のいずれかを選択します。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で、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

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

	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、詳細を入力します。

   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あります。サブジェクトには、共通名、組織名、都道府県、国などの詳細が含まれています。

   サブジェクトの別名フィールドでは、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。サブジェクトの別名は、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。

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証明書のリンクとリンク解除

複数の証明書をまとめてリンクすることで、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にリンクする場合、証明書Aの「発行者」が証明書Bの「ドメイン」と一致している必要があります。

NetScaler® ADM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：

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

1. NetScaler Application Delivery Management (ADM)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. 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. リンクする証明書を選択し、**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、リンクする証明書を選択し、**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 ADMを使用してSSL証明書のリンクを解除するには：

1. NetScaler ADM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。

エンタープライズポリシーを構成する

NetScaler Application Delivery Management (ADM) 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、安全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 Application Delivery Controller™ (ADC) 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® ADMでエンタープライズポリシーを構成するには：

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

1. NetScaler ADMで、**Infrastructure** \> **SSL Dashboard** に移動し、**Settings** をクリックします。
2. SSL設定ページで、**Edit** アイコンをクリックして、すべての信頼できるCA、安全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。
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**Signature Algorithms** 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 Application Delivery Management (ADM)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 Application Delivery Controller (ADC)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® ADMで、**Infrastructure > SSL Dashboard**に移動します。
2. **SSL Dashboard**ページで、右上隅にある**Poll Now**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. **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かのオプションが表示されます。

   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、**All Instances**タブを選択し、**Start Polling**をクリックします。

      ポーリングを開始する(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now-1.png)

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

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。

   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)

イベント

Citrix Application Delivery Controller™ (ADC) インスタンスの IP アドレスが NetScaler Application Delivery Management (ADM) に追加されると、NetScaler ADM は NITRO コールを送信し、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て、トラップまたはイベントを受信します。

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 ADM サーバーに記録されます。NetScaler ADM 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® ADM は、インスタンスで生成されたイベントもチェックし、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、その中には即座の対応が必要なものもあります。たとえば、システム障害は「重大」なイベントの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。

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、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、Citrix Application Delivery Controller (ADC) インスタンスにおける構成変更、ログイン条件、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におけるイベントとその重大度を表示できます。NetScaler

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

Application Delivery Management (ADM) の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重大度詳細のレポートを表示できます。

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**) に移動して、次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

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® ADM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え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ADC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

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

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を受け取ります。

NetScaler ADMでイベント期間を設定するには:

1. NetScaler ADMで、**Infrastructure > Events > Rules** に移動し、**Add** をクリックします。
2. **ルールの作成**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(/en-us/netscaler-application-delivery-management-software/media/createer1.png)

   イベント期間を設定する際には、**カテゴリ**セクションで関連するすべてのトラップを設定し、**重大度**セクションでそれぞれの重大度も設定してください。前の例では、`entityup`、`entitydown`、および`entityofs`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® Application Delivery Management (ADM) サーバーから通知を送信したくない場合は、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メール通知を有効にしている場合、NetScaler ADMがこれらのトラップを受信すると、サーバーは多数のメール通知を送信します。サーバーがこれらの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 ADMを使用してフィルターをスケジュールするには：

1. NetScaler ADM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オンにします。

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

- **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。複数の日付をカ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。

フィルターをスケジュールする](/en-us/netscaler-application-delivery-management-software/media/nmas-schedule-rule.png)

イベントの繰り返しメール通知を設定する

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、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ことを選択できます。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ことを選択できます。

これらのメール通知は、受信者が通知を確認したことを認識するか、イベントルールがクリアされるまで、事前に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、Citrix Application Delivery Controller™ (ADC) 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。

- **インフラストラクチャ > イベント > イベント概要** に移動し、**カテゴリ** を選択して、そのカテゴリ内のイベントを選択し、**クリア** をクリックします。
- または、**インフラストラクチャ > イベント > イベントメッセージ** 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、**クリア** をクリックします。

NetScaler® ADM から繰り返しメール通知を設定するには:

1. NetScaler Application Delivery Management (ADM) 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. **ルールの作成** ページで、ルールパラメータを設定します。

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

3. **イベントルールアクション** で、**アクションの追加** をクリックします。次に、**アクションタイプ** ドロップダウンリストから **メール送信アクション** を選択し、**メール配信リスト** 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、添付ファイルをメールにアップロードすることもできます。
5. **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オンにします。

イベントを抑制する

抑制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、その場合は無限の時間となります。時間期間を指定しない場合、NetScaler® ADM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 ADMを使用してイベントを抑制するには:

1. NetScaler Application Delivery Management (ADM)で、**Infrastructure > Events > Rules**に移動します。**Add**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。

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。

© 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、イベントを抑制（ドロップ）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できます。

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NetScalerインスタンスの停止につながる可能性がある場合、そ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、午前11時から午後11時までなど、特定の時間にルールを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。

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

1. ルールの定義
2. ルールが検出するイベントの重大度を選択
3. イベントのカテゴリを指定
4. ルールを適用するNetScalerインスタンスを指定
5. 障害オブジェクトを選択
6. 詳細フィルターを指定
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

ステップ1 - イベントルールを定義する

インフラストラクチャ > イベント > ルール に移動し、**追加** をクリックします。ルールを有効にする場合は、**ルールを有効にする** チェックボックスをオンにします。

イベント期間 オプションを設定して、NetScaler® ADM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。

注記:

> 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「CPU使用率が高い」イベントが60秒以上発生するたびに、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「CPU使用率が高い」イベントが60秒以上発生するたびに、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。

NetScaler ADM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詳細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します

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: Critical、Major、Minor、Warning、Clear、Information。

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

注

一般的なイベントとAdvanced固有のイベントの両方で重大度を設定できます。NetScaler ADM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します

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NetScaler ADMにマッピングされ、イベントルールを定義するために使用できます。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インスタンスを指定する

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。

ステップ 5 - 障害オブジェクトを選択する

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のことです。

重要

正規表現を使用して障害オブジェクトをリストするには、ステップ 1で**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。

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

障害オブジェクトは、イベントが処理される方法に影響を与え、通知された正確な問題を反映していることを保証します。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、ユーザーにログインの問題がある場合、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 - 高度なフィルターを指定する

イベントルールをさらに次の条件で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および/または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、`[.]*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、`[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress : \^([.]*10.122.132.142[.]*)`と入力します。

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

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

- 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の設定

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 ADM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、設定された設定をテスト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、関連する配布リスト、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ことを選択できます。

メールイベントルールアクションを設定(/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。トラップ配布リスト（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。

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

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 ADM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、イベントが処理される方法に影響を与え、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す。これは、生のイベントを単に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は実際の値に置き換えられます。

たとえば、ロードバランシング仮想サーバーのステータスが**ダウン**したときに、コマンド実行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 ADM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。

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

以下はスクリプト (.sh) ファイルのサンプルです。

```
#!/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
```

- .sh ファイルをNetScalerエージェント上の永続的な場所に保存します。たとえば、`/var`。
- ルール条件が満たされたときに実行されるように、NetScaler ADM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：

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。

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

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NetScaler ADMサーバーのログファイルで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 ADM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**
>
> 「**出力の追加**」と「**エラーの追加**」オプションを有効にすると、コマンドスクリプトをNetScaler ADMサーバーのログファイルで実行したときに生成された出力とエラー（もしあれば）を保存できます。これらのオプションを有効にしない場合、NetScaler ADM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。

「`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インスタンスでジョブが組み込みジョブまたはカスタムジョブとして実行されます。

1. 「**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**」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. ジョブを作成する際に、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。

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

抑制アクションを設定するには

「**抑制アクション**」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 ADMからSlack通知を設定するには

NetScaler ADM 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。イベント通知はその後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 ADM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. 「**ルールの作成**」ページで、重大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も選択します。
3. 「**イベントルールアクション**」で、「**アクションの追加**」をクリックします。次に、「**アクションタイプ**」リストから「**Slack通知の送信**」を選択し、「**Slackプロファイルリスト**」を選択します。
4. 「**Slackプロファイルリスト**」フィールドの横にある「**追加**」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. **プロファイル名**。NetScaler ADMで構成するプロファイルリストの名前を入力します。
   b. **チャネル名**。イベント通知を送信する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. 「**作成**」をクリックし、「**イベントアクションの追加**」ウィンドウで「**OK**」をクリックします。

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

注：

「**システム**」 \> 「**通知**」 \> 「**Slackプロファイル**」に移動して、Slackプロファイルを追加することもできます。「**追加**」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 ADMからPagerDuty通知を設定するには

NetScaler ADMにPagerDutyプロファイルをオプションとして追加して、PagerDutyの設定に基づいてインシデント通知を監視できます。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、電話で通知を設定できます。

NetScaler ADM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。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。

ADM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 ADM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. 新しいプロファイルを作成するには、**追加**をクリックします。
4. ページで、次の操作を行います。
    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:

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

次のようなシナリオを考えてみましょう。

- PagerDutyプロファイルに通知を送信したい。
- PagerDutyで通知を受信するための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に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 ADMからServiceNowインシデントを自動生成するには

NetScaler ADM GUIでServiceNowプロファイルを選択することで、NetScaler ADM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 ADMでServiceNowプロファイルを選択する必要があります。

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 ADMをServiceNowインスタンスと統合してください。詳細については、「ServiceNow 用 ITSM アダプターの構成」を参照してください。

イベントルールを設定するには、**イベント** > **ルール**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**」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。

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

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る重大度を変更する

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し、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たり、イベントの重大度に基づいてレポートを表示したりできます。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したり、重大度設定を変更したりできます。汎用イベントと企業固有のイベントの両方について重大度を設定できます。

重大度レベルは、次のとおり定義できます: 重大、主要、軽微、警告、クリア。

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Citrix Application Delivery Controller™ (ADC) 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)

イベント概要の表示

NetScaler® Application Delivery Management (ADM) 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。 **>** 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 ADM 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（Critical、Major、Minor、Warning、Clear、Information）が異なる列に表示されます。たとえば、Citrix Application Delivery Controller™ (ADC) インスタンスがダウンし、NetScaler ADM サーバーへの情報送信を停止した場合に、Critical 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。

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

- **カテゴリごとに受信したトラップの数**。重大度別に分類された、受信したトラップの数。デフォルトでは、NetScaler インスタンスから NetScaler ADM 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 ADM 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、 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。

イベントの重大度とSNMPトラップの詳細を表示する

NetScaler Application Delivery Management (ADM) 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 ADMサーバーに追加されたすべてのCitrix Application Delivery Controller™ (ADC) 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、不要な値をマスクできるようになりました。これにより、NetScalerインスタンスの重大度別のイベント、健全性、稼働時間、モデル、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、**重大**な重大度レベルのイベントはめったに発生しない場合があります。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。重大度レベルで「重大」以外をすべて選択すると、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、**重大度別イベント**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、*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使用率などの詳細が表示されます。また、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® ADMで重大度別に特定のイベントを選択するには：

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

1. 管理者資格情報を使用してNetScaler ADMにログオンします。
2. **インフラストラクチャ > ダッシュボード**に移動します。

   または、,

   インフラストラクチャ > イベント > レポートに移動します。
3. ページの右上隅にあるメニューから、重大度別にイベントを表示する期間を選択します。

   重大度別のイベント(/en-us/netscaler-application-delivery-management-software/media/masvc-events-report-severity-mask.png)
4. **重大度別イベント**ドーナツチャートは、すべてのイベントを重大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種類の重大度のイベントの総数に対応します。
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**重大度別イベント**ページが表示され、選択した期間の選択した重大度について、次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 ADMでNetScaler SNMPトラップの詳細を表示するには：

NetScaler ADMサーバーの**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。

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

- **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

ADMソフトウェアから、Citrix Application Delivery Controller (ADC) 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インスタンスのsyslogサーバーとしてADMを設定する必要があります。ADMを設定すると、すべてのsyslogメッセージがADCインスタンスからADMにリダイレクトされます。

ADMをsyslogサーバーとして設定する

ADMをsyslogサーバーとして設定するには、次の手順に従います。

1. ADM GUIから、**Infrastructure > Instances** に移動します。
2. syslogメッセージを収集してNetScaler ADM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。

これらの手順により、NetScalerインスタンス内のすべてのsyslogコマンドが設定され、NetScaler ADM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** から利用できます。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レポートを作成できます。

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

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。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。

次に、検索語を追加します。一部のカテゴリでは、検索語の事前入力された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。

syslogメッセージのエクスポートとスケジュール設定

ADMにログインせずにsyslogメッセージを表示するには、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します。ADCインスタンスで生成されたsyslogメッセージをPDF、CSV、PNG、および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してスケジュールするには、右上隅の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 Application Delivery Management (ADM) は、構成済みのCitrix Application Delivery Controller™ (ADC) 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。これで、関心のない一部のsyslogメッセージを破棄できます。フィルタを設定することで、NetScaler ADMに入ってくる一部のsyslogメッセージを抑制できます。NetScaler ADMは、条件に

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

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 ADM GUIには表示されず、顧客のNetScaler ADMデータベースにも保存されません。

フィルタを設定することで、NetScaler ADMに入ってくる一部のログに記録されたsyslogメッセージを抑制できます。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 ADM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 ADMは、条件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 ADM GUIには表示されず、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容量を大幅に節約できます。

syslogメッセージを抑制する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。

フィルタを作成してsyslogメッセージを抑制する

1. NetScaler ADM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**に移動します。
2. **抑制フィルタの作成**ページで、次の情報を更新します。
   a. **名前** - フィルタの名前を入力します。

   > **注**
   >
   > 異なるユーザーが複数のNetScalerインスタンスに対して異なるアクセス権を持っている場合、ユーザーはすべてのインスタンスへのアクセス権を持つフィルタ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を作成する必要があります。

   b. **重大度** - 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、「情報」を選択してそれらのメッセージを抑制できます。
   c. **インスタンス** - 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。

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

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。

フィルターの無効化

NetScaler® ADM 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。

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プルーニング設定を構成する

NetScaler Application Delivery Management (ADM)サーバーによって管理されるCitrix Application Delivery Controller (ADC)インスタンスは、イベントメッセージデータを継続的に送信し、NetScaler ADMに保存されます。NetScaler ADM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）にプルーニングされます。

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プルーニング設定を構成するには：

1. **System** \> **System Administration** に移動します。
2. **Prune Settings** の下で、**Instance Events Prune Settings** をクリックします。
3. NetScaler® ADMサーバーにデータを保持する期間を日数で入力し、**OK** をクリックします。

ネットワーク機能

ネットワーク機能を使用すると、管理対象のCitrix Application Delivery Controller™ (ADC) 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。ロードバランシング仮想サーバーの

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

トランザクション詳細、接続詳細、スループットなどの統計情報を表示できます。また、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
- 最大スループット（MB/秒）の仮想サーバー上位5件
- 最小スループット（MB/秒）の仮想サーバー下位5件
- 仮想サーバー数が最も多いインスタンス上位5件
- 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 Application Delivery Management (ADM) を使用すると、Citrix Application Delivery Controller (ADC) 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 ADM \> Network Functions 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、統合レポートまたは要約レポートをダウンロードして表示できます。

このレポートを使用すると、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。

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

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

- **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。
- 空の列は、それぞれのエンティティがそのNetScalerインスタンス用に構成されていないことを示します。

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のみ、ロードバランシングサービスのみ、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 ADM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、1週間に1回、または1ヶ月に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 ADMで、**インフラストラクチャ > ネットワーク機能 > ロードバランシング**に移動します。
2. **ロードバランシング**ページで、(/en-us/netscaler-application-delivery-management-software/media/exportbutton.png)をクリックします。
3. 開いた**エクスポート**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. **今すぐエクスポート**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. **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. **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** - 時:分 の形式で24時間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。

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

注

毎週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曜日を選択してください。

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-citrix.png)

注

月次の繰り返しを選択した場合、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 ADM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。

   個別の負荷分散エンティティレポートを生成する(/en-us/netscaler-application-delivery-management-software/media/services-export.png)

   a. レポートをすぐに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、**エクスポートをスケジュール**を選択します。

注

レポートはダウンロードするか、メール添付としてエクスポートすることのみ可能です。NetScaler ADM GUIでレポートを表示することはできません。

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

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 Application Delivery Management (ADM) では、負荷分散、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負荷分散 (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
- 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、すべてのLBサーバー、つまりデフォルトサーバーとポリシーベースサーバーの両方が表示されます。

- 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設定できます。

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

注記

- 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 ADM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. **Network Functions**ページで、右側のペインのページ右上にある**Generate Report**をクリックします。

3. **Generate Report**ページには、次の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。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. レポートを定期的に生成およびエクスポートするようにスケジュールするには、**レポートのスケジュール**タブを選択します。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. **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** - 時:分 の形式で24時間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。

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

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、**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 ADM) 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。複数の場所に多数のアプリケーションが展開された分散展開を行っている場合があります。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 ADM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
- グローバルサービス負荷分散 (GSLB)
- 認証
- ネットスケーラー ゲートウェイ

NetScaler® ADM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

次の図は、ダッシュボードのさまざまな機能を示しています。

- 左側のパネルには、NetScaler ADM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

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

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。

- 各ダッシュボードを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、それは関連する複数の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バイトの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、タイムラインスライダーオプションを使用して、NetScaler ADMで生成されるレポートの期間をカスタマイズ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 ADM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、「保存」をクリックします。

以下のセクションでは、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 ADM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。

2. 既存のダッシュボードを表示するには、**ダッシュボードの表示**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、**新しいダッシュボード**をクリックします。ダッシュボードの作成ページが開きます。

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。

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

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**。ダッシュボードに意味のある説明を入力します。

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-citrix.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-citrix.png)
3. **作成**をクリックします。

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。

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

注

読み取り専用権限がある場合、NetScaler ADMでレポートをエクスポートすることはできません。NetScaler ADMでファイルを作成し、そのファイルを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、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。

   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、レポートはタイムスタンプと日付スタンプを上書きします。

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。

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

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可能です。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**オプションを表示するには、期間を1日以降に選択します。

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。

追加できる集計は次のとおりです。

- カウント
- 最大
- 最小
- 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

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

- 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 ADM 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。

NetScaler ADM 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 ADM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ついて生成したいレポートを選択することもできます。

カウンターの値が（ルールで指定されたとおりに）しきい値を超過または下回った場合、パフォーマンス関連の問題を示すために、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す値に戻ると、イベントはクリアされます。これらのイベントは、**Infrastructure > 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、**重大度別のイベント**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メッセージの送信などのアクションをしきい値に関連付けることもできます。

しきい値を作成するには：

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

1. NetScaler ADMで、**Infrastructure > 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、またはしきい値以下であるかをチェック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、現在のクライアント接続の監視対象値が80パーセントに達した場合に、重大なイベント重大度を持つ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。**インフラストラクチャ > イベント > レポート**に移動して、「重大な重大度」のイベントを表示できます。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**。しきい値はすべてのインスタンスに設定されます。
   - **特定のインスタンス**。しきい値は特定のインスタンスに設定されます。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**リスト内のインスタンスに設定されます。
   - **特定のエンティティ**。しきい値は特定のエンティティに設定されます。

     エンティティを選択するには、**追加**をクリックします。

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

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。

エンティティの追加(/en-us/netscaler-application-delivery-management-software/media/choose-lb-servers-entities-citrix.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は**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 ADMは、監視対象値としきい値をこのメッセージに追加します。
6. しきい値でアラームを生成できるようにするには、**有効にする**を選択します。
7. オプションで、電子メールまたはSlack通知、あるいはその両方などの**アクション**を設定できます。
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。ADMは、カウンター情報などのインスタンス統計を取得し、分単位、時間単位、日単位、または週単位で集計します。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、**ポーリング間隔の設定**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を構成する

NetScaler ADM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 ADM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に対して24時間ごと（01:00）にプルーニングが行われます。

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

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 ADM) の構成管理プロセスは、ネットワーク内の複数のCitrix Application Delivery Controller™ (ADC) インスタンス全体で、構成変更、システムアップグレード、その他のメンテナンス活動の適切なレプリケーションを保証します。

NetScaler® ADM を使用すると、これらのすべてのアクティビティを複数のデバイスで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、最も反復的な管理タスクをNetScaler ADM 上の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または別の機器からファイルをコピーすることができます。例えば、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。

NetScaler ADM で以下の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することはできます。

以下のテンプレートのいずれかを使用できます。

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て、ジョブの構成に使用できます。

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

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つまたは複数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。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 ADM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の変更が記録され、NetScaler ADMにコピーされます。

関連記事

- 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

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

- 監査テンプレートを作成するための構成テンプレートの使用方法
- 構成ジョブを作成するための記録と再生の使用方法
- NetScaler ADM でマスター構成テンプレートを使用する方法

構成ジョブを作成する

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構成コマンドのセットです。インスタンス全体で構成変更を行うため、ネットワーク上の複数のインスタンスで構成を複製するため、およびNetScaler Application Delivery Management (ADM) GUIを使用して構成タスクを記録および再生する、それをCLIコマンドに変換するためにジョブを作成できます。

NetScaler® ADMの構成ジョブ機能を使用すると、構成ジョブを作成し、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 ADMで構成ジョブを作成するには：

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、**Select Configuration**タブの下で、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**
>
> 初めて`Deploy Master Configuration Job`テンプレートを追加し、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。

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

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、コマンドをある行から別の行に移動できます。テキストボックスで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。構成ジョブの作成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中に定義した変数を、統合された単一ビューでプレビューできます。

設定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。カスタマイズされ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にローカルな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、プライマリノードでのみジョブが実行されます。
      - **セカンダリノードで実行** - このオプションを選択すると、セカンダリノードでのみジョブが実行されます。

      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、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、そのファイルをNetScaler ADM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

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

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**、および**トークン**を指定します。

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、メールおよび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オンにし、実行レポートを送信するSlackチャネルを選択します。

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

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。
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

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

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、それを複数の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 ADM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、それを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-citrix.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。

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

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。

タスクを構成(/en-us/netscaler-application-delivery-management-software/media/record-and-play.png)

その後、構成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。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並べ替えることもできます。

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、単一の統合ビューでレビューできます。
6. すべての変数を単一の統合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/record-and-play-preview-citrix.png)
8. 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、**完了**ボタンをクリックします。

   パラメータの編集(/en-us/netscaler-application-delivery-management-software/media/record-and-play-preview-1-citrix.png)
9. **インスタンスの追加**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**次へ**をクリックします。

   インスタンスの追加(/en-us/netscaler-application-delivery-management-software/media/mas-record-play-create-jobs-3-citrix.png)

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

10. コマンドに変数を指定した場合は、**変数の値を指定**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。

    - **変数値の入力ファイルをアップロード: 入力キーのダウンロード**ファイルをクリックして、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、ファイルをNetScaler® ADM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**: 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）永続化されます。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、**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、**変数の値を指定**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、編集してファイルをアップロードします（同じファイル名を保持します）。

    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、**変数の値を指定**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、編集してファイルをアップロードします（同じファイル名を保持します）。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. **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。
12. **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 ADMが実行するアクションを選択することもできます。

    また、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したり、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したりすることもできます。

13. 「**ジョブ**」ページで、すべてのインスタンスにおける設定タスクの実行の進行状況を確認できます。

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

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 ADM の構成ジョブ機能を使用して、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 インスタンスでロードバランシング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、今度は 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. **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タイプを指定します。
3. **構成ソース**として**インスタンス**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。「時間期間による構成」を選択した場合は、この構成を実行した期間を設定し、**抽出**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。

4. コマンドを右ペインの**コマンド**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、ロードバランシング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、**次へ**をクリックします。

5. **インスタンスの追加**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。**OK** をクリックし、**次へ**をクリックします。
6. コマンドで変数を指定した場合は、「Specify Variable Values」タブで「**Download Input Key File**」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、そのファイルを NetScaler® ADMにアップロードします。
7. 「**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。

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

8. 「**Execute**」タブで「**Finish**」をクリックし、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つまたは複数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® ADM で変数を定義して構成ジョブを作成するには:

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、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選択するためにダブルクリックし、**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、次の図に示すように **Convert to Variable** をクリックします。

   変数に変換 (/en-us/netscaler-application-delivery-management-software/media/configjob_convvar.png)

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

5. ドル記号が変数の値を囲んでいることを確認したら、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. 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、統合された単一ビューで確認できます。
7. 統合された単一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。

8. 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、構成エディターでコマンドを適切に再配置および並べ替えることができます。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。
11. 構成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、サービス名を指定する必要があります。ファ

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

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できます。**Upload** をクリックして、入力キーファイルをNetScaler ADMにアップロードします。**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 ADMは、インスタンスレベルの値を最優先します。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 ADM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 ADM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提供した場合、NetScaler ADM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. **Upload** をクリックして、入力キーファイルをNetScaler ADMにアップロードします。**Next** をクリックします。

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指定し、**Upload** をクリックして入力キーファイルをNetScaler ADMにアップロードすることもできます。

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

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）永続化されます。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、**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. **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。
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 ADM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。

「ジョブのスケジュール」(/en-us/netscaler-application-delivery-management-software/media/executetabconfigjob-citrix.png)

ジョブを設定して実行した後、「**インフラストラクチャ > 設定ジョブ**」に移動し、設定したばかりのジョブを選択することで、ジョブの詳細を確認できます。「**詳細**」をクリックし、次に「**変数詳細**」をクリックすると、ジョブに追加された変数の一覧が表示されます。

「変数の一覧」(/en-us/netscaler-application-delivery-management-software/media/var6.png)

「

注

」

ステップ5で変数に指定した値は、ジョブを保存して終了した場合、または後で実行するようにジョブをスケジュールした場合に、NetScaler ADMによって保持されます。

© 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

NetScaler Application Delivery Management (ADM) の監査テンプレート機能を使用すると、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て構成変更を監査する一般的なワークフローは、次の手順で構成されます。

1. インスタンス構成を監査するための、有効な/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に差異がないかを確認するために、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 ADM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は、NetScaler ADMの修正コマンド機能を使用して、特定のNetScalerインスタンスの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差異がある場合、**監査レポート**ページに**差異あり**のステータス メッセージが表示されます。**差異あり**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。

NetScaler® ADM 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。

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

3. 構成コマンドを修正したいインスタンスの**差異あり**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。**構成差分**ページが表示され、そのインスタンスの保存済み構成、実行中の構成、および修正構成の間の差異が一覧表示されます。

   構成の差分(/en-us/netscaler-application-delivery-management-software/media/auditreports-citrix.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 ADM で構成ジョブを作成する方法」を参照してください。

   ジョブを作成する(/en-us/netscaler-application-delivery-management-software/media/correctivecommands2-citrix.png)

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 ADM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 ADM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® ADM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. **構成ソース**として**インスタンス**を選択し、他のインスタンスに複製したい構成を持つ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。

   - 実行中の構成
   - 保存済みの構成
   - 期間による構成

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

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-citrix.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。たとえば、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です。これには、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場合があります。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。したがって、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. コマンドで変数を指定した場合は、「**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の値を指定し、そのファイルをNetScaler ADM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。また、コマンドが失敗した場合にNetScaler ADMが実行すべきアクションや、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。

実行済み構成ジョブの再利用

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、保存された同じ構成ジョブのセットを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。

NetScaler® Application Delivery Management (ADM) は、完了したジョブを再度実行する機能を提供します。この機能を使用すると、完全に実行されたジョブをジョブ名を変更せずに再度実行できます。

注

実行モードが「今すぐ」の場合に実行されたジョブのみを再実行できます。

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

完了したジョブを編集するには:

1. NetScaler ADM 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、実行概要が「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** ページでは、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。構成ソースの変更、インスタンスの追加、変数値の編集、実行設定の設定など、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。

   完了したジョブを編集 (/en-us/netscaler-application-delivery-management-software/media/editcompletedjob.png)

注

ジョブを選択し、**実行** を再度クリックして、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し、ジョブを再度実行する必要がある場合があります。

ジョブを実行 (/en-us/netscaler-application-delivery-management-software/media/executecompletedjob-citrix.png)

構成ジョブでSCP (put) コマンドを使用する

NetScaler® ADMの構成ジョブ機能を使用して、構成ジョブの作成、電子メール通知の送信、および作成されたジョブの実行ログの確認を行うことができます。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 ADM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、構成ジョブを構成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して、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 ADM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 ADMにアップロードされ、その後選択した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 ADMに保存され、ジョブが削除されたとき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。

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。また、ジョブ内の複数の場所でファイルを使用し、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。

   ```
   put ssl-file /nsconfig/ssl-file
   ```

   この例では、,

   - `ssl-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/ssl-file` - これは、タスクの実行後に`ssl-file`が配置されるインスタンス上の宛先フォルダーです。

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

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。

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します）を確認し、変数をクリックします。
6. 変数名、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 ADMにファイルをアップロードできます。

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 ADMにファイルをアップロードし、**Next**をクリックします。

10. **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。
11. **Execute**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 ADMが実行する必要がある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。**Finish**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と、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**をクリックすると、ジョブに追加された変数が一覧表示されます。

    変数の一覧(/en-us/netscaler-application-delivery-management-software/media/configjobs-put-command4.jpg)

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
- 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

© 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
- 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
- 構成ジョブで構成監査テンプレートを再利用する
- 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

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、構成変更を行い、ライセンス、証明書、その他のファイルをADCインスタンスに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。

ADC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行います。

- 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、追加の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ADC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ADCインスタンスにアップロードし、それらにも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した構成ジョブは、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ADCインスタンスでは実行できません。

NetScaler® ADM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：

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

1. NetScaler ADM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ために、***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。

4. 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、単一の統合ビューで確認できます。
5. すべての変数を単一の統合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、構成ジョブの作成中または編集中に定義した変数を単一の統合ビューでプレビューできます。

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。

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。

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

- **構成テンプレートファイル (.conf)** - ADC 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。

使用例としてサンプル XML ファイルをここに示します。XML ファイルには、使用している ADC 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。

```
<?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.
```

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

```
-  name. This attribute represents the name of the instance group.



-  device. This tag contains all the instance specific parameters and
value.



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>
```

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

```
<device name="10.106.101.209">

<param name="IP" value="10.106.101.209"/>

</device>



<!-- HA PAIR-->

<!--<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. をクリックします。

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された構成ジョブを表示するには、 **\>** に移動し、 をクリックします。 ページで、 タブで、 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既に実行された構成ジョブを表示するには、 **\>** に移動し、ジョブ名を選択して をクリックします。 ページで、 タブで、 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）。

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

1. 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、 をクリックします。

2. 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 ADM が実行する必要があ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できます。

ジョブを実行した後、 **>** に移動して、構成したジョブを選択すると、ジョブの詳細を表示できます。 をクリックし、次に をクリックしてジョブの詳細を表示します。インスタンスをクリックして を表示し、ジョブで実行されたコマンドを確認します。

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選択できます。

NetScaler® Application Delivery Management (ADM) 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 ADMで、**Infrastructure > Configuration Jobs** に移動し、**Create Job** をクリックします。
2. **Create Job** ページで、**Select Configuration** タブの **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-citrix.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。

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

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。

   - **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 ADM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メール通知を、その他の詳細とともに送信することもできます。

10. **完了**をクリックします。

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 ADM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。

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

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**ジョブの作成**ページに保存すると、**テンプレートの作成**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® ADMで構成テンプレートを保存するには:

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. **ジョブの作成**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**構成テンプレート**を選択し、**コマンド**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. **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。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。

   設定テンプレート(/en-us/netscaler-application-delivery-management-software/media/audittemplates1-citrix.png)

NetScaler ADM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：

1. **Infrastructure > Configuration Audit > Audit Templates** に移動し、「**Add**」をクリックします。
2. 「**Create Template**」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. 「**Configuration Source**」リストから「**Configuration Template**」を選択し、テンプレートを右ペインの「Commands」フィールドにドラッグします。設定を編集して、別の名前でテンプレートを保存することもできます。「**Next**」をクリックします。

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

4. 「**Select Instances**」タブで、「**Add Instances**」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. 「**Finish**」をクリックします。

監査テンプレート(/en-us/netscaler-application-delivery-management-software/media/audittemplates2-citrix.png)

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設定されたジョブを再スケジュールする

NetScaler® Application Delivery Management (ADM) 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 ADM が実行す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 ADM の組み込みテンプレートを使用して設定されたジョブを再スケジュールするには

1. NetScaler ADM で、**Infrastructure > Configuration Jobs** に移動します。
2. 編集するジョブを選択し、インスタンスの追加または削除、変数値の指定を行い、実行アクションと設定を変更します。
3. ジョブを再スケジュールするには、**Finish** をクリックします。

注

ジョブを選択して **Execute Again** 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便利です。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。

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、テンプレートを構成ジョブとして実行できるように、構成ジョブで利用できます。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。

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

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おいて作業の重複が発生していました。

NetScaler® Application Delivery Management (ADM) を使用すると、このテンプレートをシステムに保存できるため、監査テンプレートが構成ジョブでも利用できるようになります。これにより、監査テンプレートを使用して構成ジョブを作成できます。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。この構成では、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
```

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 ADMで、**Infrasturcture > 構成監査 > 監査テンプレート**に移動し、**追加**をクリックします。

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

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、このテンプレートに「LBVariablesTemplate」という名前を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。

   「テンプレート1を作成」(/en-us/netscaler-application-delivery-management-software/media/nmas-configaudit-template-reuse--1-citrix.jpg)

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。

   「テンプレートを作成」(/en-us/netscaler-application-delivery-management-software/media/nmas-configaudit-template-reuse-2-citrix.jpg)

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、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。

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た場合は、**変数値を指定**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。

© 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、そのファイルをNetScaler ADM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たことがわかります。

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® Application Delivery Management (ADM) 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 ADM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 ADM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 ADM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。
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。

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

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。

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、ローカルシステムに **.json** 形式で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、その **.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強くお勧めします。
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. 「**構成エディター**」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、構成テンプレートの.**json**ファイルをアップロードします。

   テンプレートをアップロード(/en-us/netscaler-application-delivery-management-software/media/import-export-5-citrix.png)

   「

   注

   」

   - インポートされた新しいテンプレートはすべて、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、構成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**ファイル以外の構成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が失敗します。

構成監査

このドキュメントには以下が含まれます。

- 監査テンプレートの作成(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/configuration-audit/audit-templates.html)

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

- 監査レポートの表示(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/configuration-audit/audit-reports.html)
- インスタンス間の構成変更の監査(/ja-jp/netscaler-application-delivery-management-software/13-1/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の取得(/ja-jp/netscaler-application-delivery-management-software/13-1/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方法(/ja-jp/netscaler-application-delivery-management-software/13-1/networks/configuration-audit/how-to-poll-configuration-audit-of-netscaler-instances.html)

監査テンプレートを作成する

ネットワークの最適なパフォーマンスのために、特定のインスタンスで特定の構成が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Citrix Application Delivery Controller™ (ADC) 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とします。特定のインスタンスで監査したい特定の構成を持つ監査テンプレートを作成できます。NetScaler Application Delivery Management (NetScaler ADM) 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は報告します。構成の不一致があるたびに、NetScaler ADM は構成差分レポートを生成し、不要な構成変更のトラブルシューティングと修正を可能にします。

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時間をスケジュールする
- NetScaler® ADM がテンプレートを実行する頻度を設定します。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。

また、NetScaler ADM 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。このオプションにより、ユーザーはレポートをメール添付ファイルとして受け取ることができ、手動でレポートをエクスポートするために NetScaler ADM にログインする必要がありません。

注 名前の変更オプションは、デフォルトの構成テンプレートで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。

監査テンプレートを作成するには：

1. **インフラストラクチャ > 構成監査 > 監査テンプレート** に移動し、**追加** をクリックします。

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

2. **テンプレートの作成** ページで、**監査コマンド** タブで、テンプレート名とその説明を指定します。
3. **構成エディター** 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。左ペインから既存のテンプレートを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、**変数に変換** 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、**変数に変換** をクリックします。変数は、下の画像に示すように「$」で囲まれます。

   変数の定義 ウィンドウで、この変数のプロパティ（名前、表示名、変数の種類）を設定します。変数のデフォルト値をさらに指定したい場合は、**詳細設定** オプションをクリックします。

   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。

5. **保存**をクリックし、次に**次へ**をクリックします。
6. **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、**次へ**をクリックします。

7. **変数値を指定**タブには、次の2つのオプションがあります。

   a. コマンドで定義した変数の値を入力するために入力ファイルをダウンロードし、そのファイルをNetScaler ADM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。
8. **次へ**をクリックします。

9. **テンプレートプレビュー**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。**次へ**をクリックします。

10. **テンプレートのスケジュール**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。

    - **グローバルポーリング間隔を使用**。このオプションを選択すると、NetScaler ADM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。

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

> **注**
>
> NetScaler ADM でグローバルポーリング間隔を構成するには、**インフラストラクチャ > 構成監査 > 監査テンプレート**に移動し、**グローバルポーリング間隔**をクリックします。**ポーリング間隔**フィールドに、NetScaler ADM がインスタンスをグローバルにポーリングする必要がある分数を入力します。

- **テンプレートスケジュールをカスタマイズ**します。このオプションを使用して、テンプレートを実行する必要がある時間と頻度を構成します。
- **メールでレポートを送信**します。このオプションを使用して、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。

11. **完了**をクリックします。

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、スケジュールされた時間に実行されます。

監査レポートを表示

NetScaler® Application Delivery Management (NetScaler ADM) を使用すると、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、すべてのインスタンスおよびインスタンスごとのサマリーレポートをエクスポートできるほか、インスタンスとテンプレートのペアごとに詳細な差分レポートをエクスポートすることもできます。

監査テンプレートリストに表示される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刻に実行されます。**構成監査**ダッシュボードの**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高レベルの詳細が表示されます。**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、「差分あり」と「差分なし」の両方を示すインスタンスのリストが表示されます。NetScaler ADM が表示する差分レポートをダウンロードできます。

NetScaler ADM 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スケジュールを設定するオプションも提供します。レポートのエクスポートをスケジュールする方法の詳細については、「監査テンプレートの作成」を参照してください。

構成監査レポートをエクスポートするには:

1. NetScaler ADM で、**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、**NetScaler Config Drift**チャート内をクリックします。

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

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。

この画像では、一部のインスタンスでは**保存済みと実行中の差分**にのみ差分が存在し、一部のインスタンスでは**テンプレートと実行中の差分**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、**保存済みと実行中の差分**と**テンプレートと実行中の差分**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、その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。たとえば、**保存済みと実行中の差分**の下にあるインスタンスの**差分あり**をクリックします。

ここでは、そのインスタンスの保存済み構成と実行中の構成の差分レポートを確認できます。

「**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。「是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、構成ジョブから関連するNetScaler ADMインスタンスでコマンドを実行し、そのインスタンスの構成を修正できます。

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。たとえば、**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。

これで、2つのテンプレートに差分が表示され、NetScaler ADMインスタンスの構成がテンプレートが求めているものと異なることがわかります。

もう一度**差分が存在**をクリックします。次の図は、テンプレートが求めている構成と、そのようなコマンドが構成されていないか削除されているため空白になっている実行中の構成を示しています。また、修正構成または構成を修正するために実行するコマンドも確認できます。

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。

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

- 監査テンプレート構成をインスタンス上の実行中の構成と比較します。
- インスタンス上の実行中の構成を監査テンプレートと比較します。

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、ADM GUIから**構成監査**ページの**設定**を選択します。

「**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。「**是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、そのインスタンスの構成を修正できます。

次の図は、システムにダウンロードされる.csv差分ファイルの例を示しています。

ファイルステータス監査レポートの表示

NetScaler File Statusチャートを使用すると、`nsconfig`フォルダー内でファイルが追加、変更、または削除されたかどうかを監視できます。たとえば、ADCインスタンスでライセンス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、適切に対応できます。

NetScalerインスタンスのファイルステータス監査レポートをエクスポートするには：

1. NetScaler ADMで、**Infrastructure > Configuration Audit**に移動します。
2. **Configuration Audit**ページで、**NetScaler File Status**チャート内をクリックします。

   Audit Reportsページには、差分ステータスを持つインスタンスが一覧表示されます。

   Diff Statusは、**Previous Polled Time**から**Latest Polled Time**までの間隔で計算されます。**Diff Status**は次のいずれかになります。

   - **Diff exists** - このステータスは、**Previous Polled Time**以降にインスタンスの`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 Exists**をクリックします。

   - **No Diff** - 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間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 ADM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。

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

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。

インスタンス全体での構成変更の監査

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Citrix Application Delivery Controller™ (ADC) インスタンス全体で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とします。特定のインスタンスで実行したい特定の構成を含む監査テンプレートを作成できます。NetScaler Application Delivery Management (NetScaler ADM) 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。これにより、エラーをトラブルシューティングして修正できます。

テンプレートを実行する時間をスケジュールすることで、監査テンプレートの実行を自動化できます。また、NetScaler® ADM がテンプレートを実行する頻度を設定することもできます。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付に実行できます。NetScaler ADM 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。このオプションにより、ユーザーはレポートをメールの添付ファイルとして受け取ることができ、手動でレポートを確認するためにNetScaler ADMにログインする必要がありません。

監査テンプレートを作成するには:

1. **Infrasturcture > 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**」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。エディターの左ペインから既存のテンプレートを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。例えば、ロードバランシングサーバーのIPアドレス `ipaddress` を選択し、下の画像に示すように **Convert to Variable** をクリックします。

   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します。

   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。

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、構成監査を実行したいインスタンスを選択します。
7. 「**Specify Variable Values**」タブには、2つのオプションがあります。

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

a. コマンドで定義した変数の値を入力するために入力ファイルをダウンロードし、そのファイルをNetScaler ADM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。

8. **次へ**をクリックします。

   テンプレート変数を指定します(/en-us/netscaler-application-delivery-management-software/media/nmas-audit-confg-changes-instances-3.png)

9. **テンプレートプレビュー**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。**次へ**をクリックします。

10. **テンプレートのスケジュール**タブには、テンプレートの実行を自動化し、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3つのオプションがあります。

    - **グローバルポーリング間隔を使用**。このオプションを選択すると、NetScaler ADM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。
    - **テンプレートのスケジュールをカスタマイズ**。このオプションを使用して、テンプレートを実行する必要がある時間と頻度を設定します。
    - **メールでレポートを送信**。このオプションを使用して、差分レポートをメール添付として送信するメールプロファイルを構成します。

11. **完了**をクリックします。

    テンプレートのスケジュール(/en-us/netscaler-application-delivery-management-software/media/nmas-audit-confg-changes-instances-4.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スケジュールされた時間に実行されます。

構成変更の詳細を表示する

構成監査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。

- 構成変更による上位10インスタンス
- 保存済みおよび未保存の構成の数
- `nsconfig`フォルダで追加、削除、または変更されたファイル

構成監査(/en-us/netscaler-application-delivery-management-software/media/config-audit-dashboard.png)

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

NetScaler ADMでは、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 ADMに即座に追加することもできます。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。ポップアップページ**今すぐポーリング**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。

インスタンスに対して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**今すぐポーリング**を選択します。

今すぐ監査イベントをポーリング(/en-us/netscaler-application-delivery-management-software/media/configuration-audit-poll-now.png)

NetScaler構成ファイルステータスグラフには、`nsconfig`フォルダにあるNetScalerファイルの状態が表示されます。NetScaler ADMは、`nsconfig`フォルダ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。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. **通知設定**ページで、**編集**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、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できるように、Citrix Application Delivery Controller™ (ADC) 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。

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 Application Delivery Management (NetScaler ADM) 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。推奨される構成は NetScaler ADM から適用できます。

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

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 > 構成監査 > 構成アドバイス** の順に移動します。
2. 次のいずれかを実行します。

   「**構成ファイルのアップロード**」をクリックして、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® ADM 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。

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、次の図に示すように **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。読み取りおよび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る場合があります。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、**Actions** ドロップダウンリストから **Events** をクリックします。

アクションの選択(/en-us/netscaler-application-delivery-management-software/media/config-advice4.png)

Events ページで、構成変更の詳細を表示できます。

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

構成変更の表示(/en-us/netscaler-application-delivery-management-software/media/config-advice5.png)

NetScalerインスタンスの構成監査をポーリングする

NetScaler Application Delivery Management (NetScaler ADM) は、Citrix Application Delivery Controller (ADC) インスタンスで発生する構成変更を検出するために、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インスタンス全体の構成監査をポーリングする代わりに、選択したインスタンス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. NetScaler® ADMで、**Infrastructure > Configuration Audit** に移動します。
2. **Configuration Audit** ページの右上隅にある **Poll Now** をクリックします。

   今すぐポーリング(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now.png)
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かの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。

      ポーリングを開始(/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、**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。

      特定のインスタンスをポーリング(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now-2.png)

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Citrix Application Delivery Controller™ (ADC) インスタンスで構成変更が発生すると、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 Application Delivery Management (NetScaler ADM) に送信します。インスタンスがConfigChange

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

SNMPトラップを送信したときに、NetScaler ADMでそのインスタンスの構成監査を実行できるように設定できます。

監査テンプレート構成と実行中の構成の間に差分がある場合、「監査レポート」ページに「差分が存在する」ステータスメッセージが表示されます。「差分が存在する」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。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 ADM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® ADMでは、NetScaler ADM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 ADMで、**Infrastructure > Configuration Audit** に移動します。
2. **Configuration Audit** ページで、**Settings** をクリックします。
3. **Configuration Change Audit Settings** セクションで、編集アイコンをクリックします。
4. **netScalerConfigChangeイベントが受信されたときに構成監査を実行する** チェックボックスをオンにします。

注

これはすべてのインスタンスに対するグローバル設定です。NetScaler ADM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までの時間遅延** (分) フィールドに、分数を入力します。NetScaler ADMは、そのインスタンスによってConfigChange SNMPトラップが受信された後、この時間遅延の後にNetScalerインスタンスで構成監査テンプレートを実行します。

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

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、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: 9月上旬からLASをサポートします。

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、責任を負うことなくCitrixメンテナンス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。
NetScaler ADMを使用して、次のメンテナンスジョブを作成できます。その後、特定の期日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インスタンスのアップグレード
- Autoscaleグループ内のNetScalerインスタンスのアップグレード

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

- 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

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。

   メンテナンスジョブの作成 (/en-us/netscaler-application-delivery-management-software/media/upgrade-1-m.png)

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。

   アップグレードメンテナンスジョブの選択 (/en-us/netscaler-application-delivery-management-software/media/upgrade-2-m.png)

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. **インスタンスの追加** をクリックして、アップグレードするADCインスタンスを追加します。

   - HAペアをアップグレードするには、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。

     アップグレードメンテナンスジョブにインスタンスを追加 (/en-us/netscaler-application-delivery-management-software/media/upgrade-3-m.png)

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 ADM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 ADM 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、ADC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、このオプションを選択します。

© 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する** - インスタンスのアップグレード後、ADC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。

6. 選択したインスタンスでアップグレード前検証を開始するには、「**次へ**」をクリックします。

   「**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 ADM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。
   - 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。

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

ADC 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。

      - **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ADCインスタンスをバックアップします。** - 選択したADC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ADC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。
      - **ADC 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、ADC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維持する移行機能を提供します。これにより、ダウンタイムなしでADC 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。

   - **NetScaler ADM 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 ADM Service Connectは自動的に有効になります。詳細については、「NetScaler ADM 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。メール配信リストを追加するには、「メール配信リストを作成する」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。

   アップグレードジョブを作成し、ADCにイメージをアップロードします。(/en-us/netscaler-application-delivery-management-software/media/config-jobs-upgrade-m.png)

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。

   NetScaler SDXのアップグレード(/en-us/netscaler-application-delivery-management-software/media/upgrade-sdx2.png)
3. 「**NetScaler SDXのアップグレード**」ページの「**インスタンスの選択**」タブで、:

   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 ADM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。

      アップグレードの進行状況バー(/en-us/netscaler-application-delivery-management-software/media/upgrade-validate.png)

   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。

      SDXのアップグレード(/en-us/netscaler-application-delivery-management-software/media/upgrade-sdx4.png)
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. 後でNetScaler SDXインスタンスを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間を選択し、「**完了**」をクリックします。

6. アップグレード中のNetScaler SDXインスタンスの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、「**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。(#schedule-upgrading-of-pagecitrix-adc-generic-instances)

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

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. **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 BLXのアップグレード**」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. 「**インスタンスの追加**」をクリックして、アップグレードするBLXインスタンスを追加します。

   - 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. 「**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 ADM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 ADM 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既に利用可能な場合は、ADC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インスタンスに既に存在する場合に、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** - インスタンスアップグレード後にADC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。

6. **次へ** をクリックして、選択したインスタンスのアップグレード前検証を開始します。

   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。

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

重要

クラスターIPアドレスを指定した場合、NetScaler ADM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、インスタンスアップグレードの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、インスタンスアップグレードの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。
   - インターフェース、高可用性ノード、仮想サーバー、およびサービスのアップグレード前後のステータス。
   - 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。

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

- **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ADCインスタンスをバックアップ** - 選択したADC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ADC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。
- **ADC 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、ADC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ADC 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。

- **NetScaler ADM 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 ADM Service Connect は自動的に有効になります。詳細については、「NetScaler ADM 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。電子メール配布リストを追加するには、「電子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 グループの一部であ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. **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. **Autoscale グループのアップグレード**を選択し、**続行**をクリックします。
3. **アップグレード設定**タブで、次の操作を行います。
   a. アップグレードする**Autoscale グループ**を選択します。
   b. **イメージ**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。

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

c. **NetScaler イメージ**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。

グレースフルアップグレードをオンにすると、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. **次へ**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する場合。
- **Later:** NetScalerインスタンスのアップグレードを後で開始する場合。

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通知を有効にすることもできます。「**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て、通知を有効にします。

5. 「**Finish**」をクリックします。

NetScalerインスタンスのHAペア構成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. 「**Configure HA Pair of NetScaler Instances**」を選択し、「**Proceed**」をクリックします。

HAペアを構成する(/en-us/netscaler-application-delivery-management-software/media/ha-upgrade-2.png)

3. 「**NetScaler HA Pair**」ページの「**Instance Selection**」タブで：

a. 「**Task Name**」を追加します。

b. Primary IP Addressを入力します。

c. Secondary IP Addressを入力します。

d. 「**次へ**」をクリックします。

e. 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。

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

ADC HAペアの選択(/en-us/netscaler-application-delivery-management-software/media/upgrade-ha-pair.png)

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 HAペア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間を選択し、「**完了**」をクリックします。

   ADC HAペアのスケジュール(/en-us/netscaler-application-delivery-management-software/media/ha-upgrade-6.png)
6. ADC 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の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。

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。

   HAペアインスタンスの変換(/en-us/netscaler-application-delivery-management-software/media/ha-cluster2.png)
3. 「**NetScaler HAをクラスターに移行**」ページで、「**インスタンスの選択**」タブに「**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。

   ADC HAをクラスターに移行(/en-us/netscaler-application-delivery-management-software/media/ha-cluster3.png)
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。

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

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。

インスタンスアドバイザリ

インスタンスアドバイザリは、NetScalerインスタンスを安全かつ最新の状態に保つのに役立つ推奨事項を提供します。以下のトピックは、これらのアドバイザリを確認し、対応するのに役立ちます。

- アップグレードアドバイザリ
- 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 (プレビュー)

ネットワーク管理者として、NetScaler ADMで異なるADCビルドを実行している多数のADCインスタンスを管理している場合があります。各ADC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ADCインスタンスを特定する必要があります。その後、それらのアップグレードを計画します。

NetScaler ADMオンプレミス版のアップグレードアドバイザリは、ADCのバージョンをスキャンし、お使いのADCインスタンス全体のEOM/EOLビルドのビューを提供します。

重要

詳細なインサイトとADCインスタンスをアップグレードするワークフローについては、**NetScaler® ADM Serviceをお試しください。**

アップグレードアドバイザリの表示

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に移動し、次の情報を表示します。

- ADCインスタンスの総数。
- ライフサイクル終了に近づいているインスタンス。
- メンテナンス終了に近づいているインスタンス。

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

アップグレードアドバイザリページでは、ADCインスタンスをリリース別にグループ化します。

NetScaler ADMオンプレミス版のアップグレードアドバイザリでは、ADCインスタンスのいずれかを選択し、そのADCインスタンスをADM Serviceにオンボードすることもできます。**ADM Serviceを試す**をクリックして、ADCインスタンスをADM Serviceにオンボードします。ADM Serviceのアップグレードアドバイザリは、選択したADCインスタンスをアップグレードするワークフローを提供します。

ADM Serviceのアップグレードアドバイザリの詳細については、**アップグレードアドバイザリ**ページでGIFアニメーションをご覧ください。

セキュリティアドバイザリ (プレビュー)

注:

13.1-53.22ビルド以降、セキュリティアドバイザリは自動的に有効になります。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。

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軽減策と修復策を理解し、計画する必要があります。

NetScaler® ADMオンプレミスセキュリティアドバイザリは、NetScaler CVEとリスクのあるADCインスタンスのみを強調表示します。

重要

CVEの影響に関する詳細な分析、カスタムスキャン/システムスキャンに関する決定的な情報、修復および軽減のワークフローについては、**NetScaler ADM Serviceをお試しください**。

セキュリティアドバイザリの表示

セキュリティアドバイザリにアクセスするには、**Infrastructure > Instance Advisory > Security Advisory**に移動します。NetScaler ADMを通じて管理しているすべてのADCインスタンスの脆弱性ステータスを確認できます。

© 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(/en-us/netscaler-application-delivery-management-software/media/security-advisory-adm.png)

NetScaler ADMオンプレミスセキュリティアドバイザリは、CVEをチェックするためにADCバージョンのみをスキャンし、以下の情報が表示されます。

- **CVE ID**: インスタンスに影響を与えるCVEのID。
- **脆弱性の種類**: このCVEの脆弱性の種類。
- **影響を受けるADC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。

NetScaler ADMオンプレミスセキュリティアドバイザリでは、ADCインスタンスのいずれかを選択し、そのADCインスタンスをADM Serviceにオンボードすることもできます。**ADM Serviceを試す**をクリックして、ADCインスタンスをADM Serviceにオンボードします。ADM Serviceセキュリティアドバイザリを使用すると、特定のCVEの脆弱性の種類を確認し、脆弱性を解決するための軽減策と修復策に関する情報を取得できます。

ADMサービスセキュリティアドバイザリの詳細については、「**セキュリティアドバイザリ**」ページでGIFアニメーションをご覧ください。

セキュリティアドバイザリでサポートされているCVE

NetScaler Consoleオンプレミスでは、自動有効化チャネルを通じ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完全版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。

最新のサポート対象CVE

次の表は、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対象CVEの詳細を示しています。

リリース日	CVE ID	識別	修復	リソースリンク
11 Nov 2025	CVE-2025-12101	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.

注：

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でサポートされてい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、**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できます。

サポートされているCVE

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は次のとおりです。

リリース日	CVE ID	リソースリンク
Nov 11, 2025	CVE-2025-12101	セキュリティ速報
Aug 26, 2025	CVE-2025-8424	セキュリティ速報
Aug 26, 2025	CVE-2025-7776	セキュリティ速報
Aug 26, 2025	CVE-2025-7775	セキュリティ速報
Jun 25, 2025	CVE-2025-6543	セキュリティ速報
Jun 17, 2025	CVE-2025-5349	セキュリティ速報
Jun 17, 2025	CVE-2025-5777	セキュリティ速報
Nov 12, 2024	CVE-2024-8534	セキュリティ速報
Nov 12, 2024	CVE-2024-8535	セキュリティ速報
Jul 09, 2024	CVE-2024-5491	セキュリティ速報
Jul 09, 2024	CVE-2024-5492	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
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
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	セキュリティ情報
May 09, 2023	CVE-2023-24488	セキュリティ情報
May 09, 2023	CVE-2023-24487	セキュリティ情報
Dec 13, 2022	CVE-2022-27518	セキュリティ情報
Nov 08, 2022	CVE-2022-27516	セキュリティ情報
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	セキュリティ情報
Nov 09, 2021	CVE-2021-22955	セキュリティ情報
Jul 19, 2021	CVE-2021-22927	セキュリティ情報
Jul 19, 2021	CVE-2021-22920	セキュリティ情報
Jul 19, 2021	CVE-2021-22919	セキュリティ情報

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

リリース日	CVE ID	リソースリンク
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
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

オーケストレーション

ソフトウェア定義ネットワーキング (SDN) 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ー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集中管理ツールを使用してネットワークサービ

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

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を作成する機能、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。

- 集中型ネットワークプロビジョニング
- きめ細か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

NetScaler® Application Delivery Management (ADM) 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により、エンタープライズネットワークでSDNをサポートします。NetScaler ADMは、VMware NSX ManagerとCisco Application Policy Infrastructure Controller (APIC) の両方をサポートします。

ヴイエムウェア NSX マネージャー

NetScaler ADM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抽象化され、vSphere/vCenter管理者が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キングを可能にします。また、外部ネットワーキングおよびセキュリティサービスもサポートしています。

NetScaler ADM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、事前プロビジョニングされたVPXをオンデマンドで特定のEdgeゲートウェイに割り当てる機能。
- 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。

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

- 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部として、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部としての、新しいADC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ADC機能の簡素化された構成
- クラウド管理者に単一の制御ポイントを提供しながら、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
- 予期せぬ将来の用途をサポートするのに役立つNetScaler ADM APIとのより簡単な統合。

NetScaler ADMでVMware NSX Managerを構成する方法の詳細については、「NetScalerアプライアンスとVMware NSX Managerの統合」を参照してください。

Cisco ACIハイブリッドモード

Cisco ACIはバージョン1.3 (2f) でハイブリッドモードのサポートを導入しました。ハイブリッドモードでは、Application Policy Infrastructure Controller (APIC) を介してネットワーク自動化を実行し、L4-L7構成はAPICでデバイスマネージャーとして機能するNetScaler ADMに委任できます。

NetScalerハイブリッドモードソリューションは、ハイブリッドモードデバイスパッケージとNetScaler ADMによってサポートされています。ハイブリッドモードデバイスパッケージをAPICにアップロードする必要があります。詳細については、「Cisco ACIのハイブリッドモードでNetScaler ADMを使用するNetScaler自動化」を参照してください。

OpenStack: NetScalerインスタンスの統合

NetScaler Application Delivery Management (ADM) 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® ADM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。

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

OpenStack Neutron LBaaS用NetScalerドライバー

OpenStack Neutron LBaaSプラグインには、OpenStackがNetScaler ADM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 ADMに転送し、NetScaler ADM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 ADMを呼び出し、NetScalerからの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 ADM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 ADM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 ADMとOpenStackの相互登録

まず、NetScaler ADM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者ユーザーの資格情報、およびOpenStack NetScalerドライバーユーザーの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 ADMに接続できるようになります。

OpenStackとNetScaler ADM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 ADM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す。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 ADM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連するいくつかの点を以下に示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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用に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。

次のリストは、OpenStackのLBaaS V1とLBaaS V2の両方でサポートされる機能を示しています。

- 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を使用した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、次の情報を提供します:

- ユースケースシナリオ
- OpenStackワークフローとのNetScaler ADM統合
- 前提条件
- NetScaler ADMおよび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 ADMとOpenStack Heatサービスとの統合
- NetScaler ADMでのOpenStackアプリケーションの監視

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユースケースシナリオ

次のユースケースシナリオでは、NetScaler ADM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S2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負荷分散するための専用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 ADMの両方をインストールおよび構成し、互換性があるように準備する必要があります。SteveはOpenStackで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のリソースと構成を管理するために、Example-SportsOnline用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るようになります。

SteveはOpenStackの詳細をNetScaler ADM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 ADM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 ADM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 ADM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 ADM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 ADM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用に非共有インスタンスを選択します。次に、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 ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、サーバーを監視するためのヘルスモニターを作成し、常に稼働しており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もできます。

OpenStackで作成されたロードバランシング構成は、NetScalerインスタンスに実装されます。完全に構成されると、NetScaler VPXインスタンスがロードバランシング機能を引き継ぎ、アプリケーショントラフィックの受け入れを開始し、Tomによって作成されたサーバーS1とS2間のトラフィックをロードバランスします。

NetScaler ADMとOpenStackワークフローの統合

次のフローチャートは、LBaaS V1およびLBaaS V2を構成する際に従う必要があるワークフローを示しています。

LBaaS V1およびV2構成ワークフロー(/en-us/netscaler-application-delivery-management-software/media/openstack-orchestartion-workflow.png)

OpenStack: NetScalerインスタンスの統合

NetScaler Application Delivery Management (ADM) 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® ADM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 ADM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 ADMに転送し、NetScaler ADM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 ADMを呼び出し、NetScalerからの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 ADM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 ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADMとOpenStackの相互登録

まず、NetScaler ADM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者ユーザーの資格情報、およびOpenStack NetScalerドライバーユーザーの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 ADMに接続できるようになります。

OpenStackとNetScaler ADM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 ADM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す。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 ADM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連するいくつかの点を以下に示します。

- 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用に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。

次のリストは、OpenStackのLBaaS V1とLBaaS V2の両方でサポートされる機能を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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を使用した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、次の情報を提供します:

- ユースケースシナリオ
- OpenStackワークフローとのNetScaler ADM統合
- 前提条件
- NetScaler ADMおよび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 ADMとOpenStack Heatサービスとの統合
- NetScaler ADMでのOpenStackアプリケーションの監視

ユースケースシナリオ

次のユースケースシナリオでは、NetScaler ADM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S2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負荷分散するための専用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 ADMの両方をインストールおよび構成し、互換性があるように準備する必要があります。SteveはOpenStackで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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ます。また、SteveはExample-SportsOnlineのリソースと構成を管理するために、Example-SportsOnline用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るようになります。

SteveはOpenStackの詳細をNetScaler ADM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 ADM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 ADM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 ADM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 ADM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 ADM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用に非共有インスタンスを選択します。次に、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 ADM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、サーバーを監視するためのヘルスモニターを作成し、常に稼働しており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もできます。

OpenStackで作成されたロードバランシング構成は、NetScalerインスタンスに実装されます。完全に構成されると、NetScaler VPXインスタンスがロードバランシング機能を引き継ぎ、アプリケーショントラフィックの受け入れを開始し、Tomによって作成されたサーバーS1とS2間のトラフィックをロードバランスします。

NetScaler ADMとOpenStackワークフローの統合

次のフローチャートは、LBaaS V1およびLBaaS V2を構成する際に従う必要があるワークフローを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LBaaS V1およびV2構成ワークフロー(/en-us/netscaler-application-delivery-management-software/media/openstack-orchestartion-workflow.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® ADMおよびOpenStackのソフトウェア要件

- NetScaler ADM 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、実行されていること。
- NetScaler ADM 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**。

NetScaler ADM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、OpenStackプラットフォームにNetScaler ADMを展開するためのものです。OpenStackのハードウェア要件は、実行されている仮想マシンの数によって異なります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® ADM および OpenStack での事前構成タスク

このセクションでは、NetScaler Application Delivery Management (ADM) および 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 ADM 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 ADM をインストールします。NetScaler ADM 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 ADM 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 ADM の登録

NetScaler ADM のダウンロードページから、OpenStack 用の NetScaler バンドルをダウンロードします。

NetScaler ADM 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:

1. NetScaler ADM で、**ダウンロード**をクリックします。NetScaler ADM の**ダウンロード**ページには、**Newton**、**Ocata**、および **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提供されています。
2. 最新の NetScaler バンドルの 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 ドライバーの 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. 次のコマンドを実行してドライバーをインストールし、NetScaler ADM IPアドレス、OpenStackをNetScaler ADMに登録したときに構成したNetScalerドライバーパスワード、およびプロトコルを指定します。

   ```
   ./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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任意です。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。

NetScaler ADMがOpenStackに正常に登録された後、OpenStackユーザー資格情報を使用してNetScaler ADMにログオンすることもできます。
NetScaler ADMがOpenStackに正常に登録された後、OpenStack Neutronサービスを再起動します。

OpenStackをNetScaler ADMに登録する

NetScaler ADM GUIを使用してOpenStackをNetScaler ADMに登録するには:

1. NetScaler ADMで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** 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 ADM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、デフォルトとカスタマイズの2つのオプションがあります。

   OpenStackのNewtonおよび**Ocata**リリースでは、デフォルトまたはカスタマイズされたデプロイタイプを使用できます。しかし、Pikeリリースでは、NetScaler ADMにOpenStackを登録するためにカスタマイズされたデプロイタイプを使用する必要があります。

- **デフォルトのデプロイタイプ**

  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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. OpenStackコントローラー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デプロイタイプ**

  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、デプロイタイプとして**カスタマイズ済み**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は、ここで指定します。OpenStack Newton および**Ocata**リリースをNetScaler ADMに登録する方法は、OpenStack Pikeリリースを登録する方法とは異なります。

  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. 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は、以前**デフォルト**設定で指定したとおりに指定します。

  OpenStackのPikeリリース:

  OpenStackのPikeリリースを登録する場合は、次の図に示すようにOpenStackサービスの詳細を入力します。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も指定する必要があります。

  OpenStackの詳細(/en-us/netscaler-application-delivery-management-software/media/orchestration-openstack-pike-citrix.png)

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 ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADMで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **OpenStack Tenants**の順に移動し、**Add**をクリックします。
2. **Add OpenStack Tenants**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、事前にプロビジョニングされたインスタンスを使用しているか、インスタンスを自動プロビジョニングしているかに基づいて、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デバイスのプロビジョニング

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、以下の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デバイスの事前プロビジョニング

NetScalerデバイスをCitrix Hypervisor、KVM、ESXなどのハイパーバイザープラットフォームのいずれかにインストールし、インスタンスをNetScaler ADMに追加します。NetScaler ADM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 ADMに既存のNetScaler VPXインスタンスを追加するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler ADMで、**Infrastructure** \> **Instances** \> **NetScaler VPX** の順に移動し、**Add** をクリックします。
2. **Add NetScaler VPX** ページで、NetScaler VPXインスタンスのIPアドレスを指定し、**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。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

NetScalerダウンロードページから必要なNetScalerインスタンスイメージをダウンロードし、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：

1. NetScaler ADMで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** の順に移動します。
2. **Deployment Settings** をクリックします。
3. 次のパラメーターを設定します。

    a. 管理ネットワーク - 自動プロビジョニングされたNetScaler VPXが接続されている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 ADMは、このプロファイルに含まれるパスワードを使用して、新しい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 - 新しい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 ADMライセンスアクセスコードを提供します。NetScaler ADM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 - ライセンスのインストールに必要な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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **OK**をクリックします。

NetScaler ADMでサービスパッケージを作成する

NetScaler ADMでテナントのサービスパッケージを作成するには：

1. NetScaler ADMで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Service Packages**の順に移動し、**Add**をクリックします。
2. **Service Package**ページで、次のパラメータを指定します。
   a. 名前 - サービスパッケージの名前。例として、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たインスタンス割り当てのタイプで、それに基づいてNetScalerインスタンスリソースがテナントに割り当てられます。**Dedicated**を選択します。ポリシーの詳細については、サービスパッケージ分離ポリシーを参照してください。
   c. NetScalerインスタンスプロビジョニング - 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. **続行**をクリックして、テナントをサービスパッケージに関連付けます。

> **注**
>
> NetScalerインスタンスを高可用性モードで展開している場合は、**高可用性のためのNetScalerインスタンスペアのプロビジョニング**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**の下で、**追加**をクリックし、テナントを選択します。
6. **続行**をクリックし、**完了**をクリックします。

© 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 ADMはテナントに基づいてNetScalerインスタンスを割り当てます。テナントがどのサービスパッケージにも属していない場合、NetScaler ADMは「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。」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。ポリシーがテナント名またはIDだけでなく、他のカスタム属性にも基づいているような、柔軟な配置ポリシーを作成できます。

NetScaler ADMでテナントの配置ポリシーを作成するには:

1. NetScaler ADMで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Placement Policy**に移動し、**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、ブール式がこのフィールドに入力されます。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設定するには、次の設定を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「**Orchestration** > **Cloud Orchestration** > **OpenStack** > **Deployment Settings**」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 ADM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 ADMにNetScaler SDXプラットフォームを追加すると、NetScaler ADMは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します。

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 ADM 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. 「**管理ネットワーク**」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. 「**プロファイル名**」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 ADMは、このプロファイルに含まれるパスワードを使用して、新しい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、**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** \> **サービスパッケージ** に移動します。
   a. 「**追加**」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インスタンス割り当て**」フィールドで、「**専用**」を選択します。
   d. 「**NetScalerインスタンスプロビジョニング**」フィールドで「**オンデマンドでインスタンスを作成**」を選択し、「**自動プロビジョニングプラットフォーム**」フィールドで「**NetScaler SDX**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 「**続行**」をクリックします。

g. 「**自動プロビジョニング設定**」セクションで、「**リソース**」プロパティを設定します。

   i. 「**スループット**」フィールド。1000 Mbpsと入力します。

   ii. 「**NetScalerバージョン**」フィールド。リストから、NetScaler SDXプラットフォームに存在するNetScaler VPXイメージの適切なバージョンを選択します。

h. 「**NetScaler SDXプラットフォーム**」セクションで、「**追加**」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. 「**続行**」をクリックします。

j. 「**OpenStackテナントの構成**」セクションで、「**追加**」をクリックしてテナントを追加します。「**新規**」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。

k. 「**完了**」をクリックします。

5. 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。

Horizonを使用してLBaaS V1を設定する

TomはOpenStack Horizonポータルにログインして LBaaSプールを作成し、このプールのすべてのメンバーが配置されているサブネットを選択できるようになりました。Tomは仮想IP (VIP) アドレスを追加し、作成したプールにこのVIPを割り当てる必要があります。Tomはこれをコマンドラインまたは API経由で実行することもできます。Tomの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、NetScalerはすべてのリクエストを設定されたポートのプールメンバーに分散します。

LBaaSプールメンバーは、選択されたプールに追加されるロードバランシングされたサーバーです。Tomはこれらの各メンバーに重みとポートを割り当てることができます。

ヘルスモニターは、プールのすべてのメンバーの健全性と正常な機能を監視するために使用されます。Tomは、遅延、タイムアウト、再試行制限を指定することで、OpenStackでヘルス監視テンプレートを作成できます。また、メソッド、URLパス、成功時の期待されるHTTPコードも指定できます。モニターを作成した後、Tomは以前に作成したプールにそのモニターを関連付ける必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Documentationを参照してください。

重要

OpenStackのLibertyリリースでは、LBaaS V1はサポートされていません。詳細については、OpenStack Release Notes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**によって管理される証明書、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ています。LBaaS V2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ースのみをサポートしています。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. 次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. 次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>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例:

```
barbican secret store -- payload-content-type='text/plain' --
name='shp_server_key' --payload="hp-server/tmp/server_key"
```

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が表示されます。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. 次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、<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指定する必要があります。

4. OpenStack で環境変数を設定します。これらの変数により、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なります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例:

エクスポート OS_PASSWORD-hp

エクスポート OS_AUTH_URL=`http://10.106.43.15:35357/v2.0/`

OS_USERNAME=hp_user をエクスポートします。

OS_TENANT_NAME=hp をエクスポートします。

エクスポート OS_IDENTITY_API_VERSION=2.0

エクスポート BARBICAN_ENDPOINT="`http://10.106.43.15:9311/`"

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name
<listener-name> --protocol <protocol_type> --protocol-port
<port_number> --default-tls-container-id<container_url>
```

例:

```
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、コンテナへの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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例:

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --
protocol-port 80 hp-lb-test-pool
```

メンバーを作成(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-member-create.png)

NetScaler® ADM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 Application Delivery Management (ADM)にログオンし、任意のブラウザからOpenStackで作成されたVIPとプールを監視できます。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 ADMのIPアドレスです。

注

- OpenStack VIPは、NetScaler ADMの仮想サーバーに対応します。
- OpenStackプールは、NetScaler ADM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 ADM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を構成する

NetScaler Application Delivery Management (ADM) 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 ADM 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し、ロードバランスすることができます。

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、一方、`http://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、ルールの値パラメーターと比較されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- クッキー: キーパラメーターで指定されたクッキーは、ルールの値パラメーターと比較されます。クッキー要求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」という名前のクッキーで「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-。

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。

- regex: Perl 型の正規表現マッチング
- starts_with: 文字列が〜で始まる
- ends_with: 文字列が〜で終わる
- contains: 文字列が〜を含む
- equal_to: 文字列が〜と等しい

注記

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regex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」値を返します。

どのL7ポリシーにおいても、すべてのルールは論理的にAND演算子で結合されます。リクエストはすべてのルールに一致する必要があり、そうすることでポリシーは「true」値を返します。ロードバランサーによって実行されるアクションは、ポリシーによって返される値に基づいています。同じアクションを持つ2番目のポリシーを作成することで、ルール間の論理OR演算を実現できます。

例えば、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ている場合に、ロードバランサーが要求されたコンテンツを提供するために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するという適切なアクションを実行するポリシーを作成できます。同じアクションを実行する別のポリシーを作成することもできますが、そのポリシーは「example-sports」、「example-sports-football」、または「example-football」に一致します。ユーザーがこれら6つのキーワード

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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そのリクエストを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。例えば、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レスポンスを送信します。そのレスポンスのLocationヘッダーには新しい場所が含まれます。ブラウザはアドレスバーを新しい場所に更新し、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。例えば、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は実行しません。例えば、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レスポンス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際、ターゲットの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、リスナーに必ずしも関連付けられていなくても、ロードバランサーの直下に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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プールは複数のL7ポリシーによってサービスされることができますが、少なくとも1つのポリシーがアタッチされている場合は「active」状態を維持します。最後のポリシーが削除されると、プールは別のポリシーが作成されて関連付けられるまで「pending_create」状態に戻ります。プール自体が削除された場合、それ以外で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。

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REDIRECT_TO_POOLを持つ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 ADM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REDIRECT_TO_URLを持つ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 ADM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REJECTを持つL7ポリシー	レスポンダーポリシー > リクエストを破棄	NetScaler ADM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 ADMは指定されたプールをロードバランシング仮想サーバーとともに実装します。NetScaler ADMは、L7ポリシーからコンテンツスイッチングポリシー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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。

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続して番号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ができます。ポリシーは常に優先順位の順に評価されます。特定の要求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、次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がります。
- 位置を指定せずに新しいポリシーを作成すると、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ると、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がある場合、ポリシーを作成して優先順位8を割り当てると、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が位置の値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番目の位置を占め、ポリシーDが3番目の位置を占めます。

NetScaler ADM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存在します。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とき、それらは常に、対応するL7ポリシーの優先順位よりも1つ高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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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は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は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 ADM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存在します。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とき、それらは常に、対応するL7ポリシーの優先順位よりも1つ高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は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は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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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に接続され、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。
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、レスポンダーポリシーである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。
特定URLにリクエストをリダイレクトする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レスポンダーアクションを作成し、アクション付きのレスポンダーポリシーを作成し、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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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、レスポンダー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>
```

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、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で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、OpenStackにNetScaler Application Delivery Management (ADM) を登録します
    a. NetScaler ADM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® ADMでOpenStackを設定するためのパラメータを設定できます。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Orchestration** \> **Cloud Orchestration** \> **OpenStack** に移動し、**Deployment Settings** をクリックします。

   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 ADMは、このプロファイルに含まれるパスワードを使用して、新しい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. 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 ADM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** - **インスタンスをオンデマンドで作成**を選択して、設定中にNetScalerインスタンスを作成します。

   d. **プラットフォームの自動プロビジョニング** - **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**セクションで、OpenStackテナントの下にある**追加**をクリックし、テナントを選択します。

   f. **続行**をクリックし、次に**完了**をクリックします。

5. **システム** \> **システム管理** \> **システム設定の変更**に移動し、ドロップダウンリストから**http**を選択します。

6. **インフラストラクチャ > インスタンス > NetScaler VPX**に移動します。

7. **NetScaler VPX**ページで、**管理者**ドロップダウンリストをクリックし、**デバイスのプロビジョニング**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)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **デバイスのプロビジョニング**ページで、デバイス名を入力し、前のステップ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. **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** \> **リクエスト**タブに移動します。リクエストを選択し、**タスク**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**完了**に変わると、NetScaler VPXがNetScaler ADMにプロビジョニングされたことを意味します。
9. **インフラストラクチャ > インスタンス** \> **NetScaler VPX**に移動して、NetScaler VPXインスタンスがNetScaler VPXページに表示され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。NetScaler VPXインスタンスがブラウザウィンドウで開いたら、インスタンスにログオンします。**構成** \> **システム** \> **ライセンス**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ライセンスの概要」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の再起動(/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、「Configuring LBaaS V2 using Command Line」を参照してください。

StyleBookを使用したOpenStackでの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 Application Delivery Management (ADM) 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、構成パックが作成されます。

OpenStackワークフローで構成にStyleBookを使用すると、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM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構成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`構成パックを表示するにはスクロールします。
- インスタンスに展開されている構成を確認するには、`os-cs-lb-mon` StyleBookパネルで**View Definition**をクリックします。
- 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するには、**View Object**をクリックします。

StyleBookを使用してインスタンスをプロビジョニングする前に注意すべき点

NetScaler ADM 12.1ビルド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インスタンスを構成するためにNetScaler ADM StyleBookを使用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ビルド48.18からNetScaler ADM 12.1ビルド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の構成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 ADM 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 ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、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、NetScaler Application Delivery Management (ADM) は、**OpenStack Compute** を使用してサービスパッケージを選択すると、必要に応じてNetScaler VPXインスタンスを作成します。現在、NetScaler ADM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、オンデマンドで作成される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® ADMにライセンスをアップロードし、その後、OpenStackコンピュート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、帯域幅とインストールするライセンスエディションの種類を選択できます。

NetScaler ADMをプロバイダーとして最初のロードバランサーを展開すると、NetScaler ADM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 ADMに返却されます。これにより、NetScaler ADMで利用可能なライセンスを最適に利用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

NetScaler ADM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 ADMであるMAS-HA-1にアップロードされていると見なしてください。最初の要求を展開し、NetScaler ADM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 ADM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、したがって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。

このような場合、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 ADMをMAS-HA-2からMAS-HA-1に手動でフェイルオーバーします。この後、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 ADM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® Application Delivery Management (ADM) 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。

共有VLANアーキテクチャ(/en-us/netscaler-application-delivery-management-software/media/shared-vlan-diagram.png)

テナントがVIPまたはリスナーを構成すると、そのテナント用に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。テナントが共有ネットワークまたは外部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、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、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 ADM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 ADM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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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を設定します。
2. **Configure VLAN** ページで、**Partitions Sharing** 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。

   VLANの構成(/en-us/netscaler-application-delivery-management-software/media/shared-vlan-add-nmas.jpg)

OpenStackオーケストレーションからの共有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。
2. **Create Network** で、次のパラメータを設定します。
   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が共有されており、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 Application Delivery Management (ADM) 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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 ADM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 ADMをCitrix Licensing Portal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。

トライアルライセンスを持つNetScaler VPXインスタンスは、NetScaler ADMとHTTPのみで通信できます。NetScaler ADM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、負荷分散、SSLオフロード、コンテンツスイッチングなどのコアな負荷分散サービスを可能にします。LBaaSはREST APIを通じて管理され、このAPIによりテナントはLBaaSオブジェクトの作成、更新、削除を行うためのRESTコールを実行できます。LBaaSは負荷分散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記述には、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を使用すると、任意のNetScalerインスタンスで高度なアプリケーションデリバリーコントローラー（ADC）機能を構成できます。

NetScaler StyleBooks

NetScaler Application Delivery Management (ADM) StyleBooksは、NetScalerの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 ADMはすべてのNetScaler ADM 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 ADMに付属しているStyleBooksと、後でユーザーによって作成される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

次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。

Heatを使用してADCインスタンスを構成するワークフロー(/en-us/netscaler-application-delivery-management-software/media/openstack-heat-integration-workflow-kopis.png)

クラウド管理者として、次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 ADMで、**ダウンロード**に移動してNetScalerドライバーバンドルをダウンロードし、バンドルを解凍して、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、そのセクションで次のパラメーターを更新します。

   a. HTTP通信の場合、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. HTTPS通信の場合、パラメータは次のように更新されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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」に設定した場合、NetScaler ADMはリクエスト呼び出しでverify=Falseを送信し、これによりSSL証明書の検証が無効になります。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 ADM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 ADMはverify=Trueを送信します。

注

NetScaler ADM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 ADM 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® ADMをOpenStackに登録します。

   a. NetScaler ADMで、**Orchestration** \> **Cloud Orchestration** \> **OpenStack** 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。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、ユーザーごとにNetScaler ADMでテナントが作成され、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プラグインはこの情報を使用してNetScaler ADMに接続し、StyleBookをHeatリソースとしてOpenStackにインポートします。

   > **注**
   >
   > NetScaler ADMとOpenStackでのサービスパッケージの作成およびその他の事前設定タスクの詳細については、NetScaler ADMとOpenStackプラットフォームの統合を参照してください。

6. NetScaler ADMの関連するすべてのStyleBookが、リソースとしてOpenStack Heatにインポートされていることを確認します。また、NetScalerネットワークリソースとNetScaler証明書リソースが、リソースとしてOpenStack Heatにインポートされていることを確認します。

   > **注**
   >
   > 現在、NetScaler ADMに付属しているStyleBookのみを使用できます。

   テナントは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るようになりました。Heatスタックが展開されると、構成がNetScaler ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. OpenStack Horizonで、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を作成するには、次の2つの方法があります。

   - **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** - ウィンドウ内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

   スタックの展開が成功した後、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。

   テナントがスタックを展開した後、NetScaler ADMで**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 ADMで**Applications** \> **Configuration**に移動して、NetScalerインスタンスがStyleBook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 ADM StyleBookの例：

以下の画像は、NetScaler ADM 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 ADM 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 documentation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 Application Delivery Management (ADM) 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスが割り当てられます。割り当てられたこのNetScalerインスタンスは、他のテナントと共有されません。

サービスパッケージ - 専用インスタンスの割り当て(/en-us/netscaler-application-delivery-management-software/media/openstack-service-package-dedicated.png)

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、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。

サービスパッケージ - パーティションインスタンスの割り当て(/en-us/netscaler-application-delivery-management-software/media/openstack-service-package-partition.png)

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

サービスパッケージに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。

サービスパッケージ - 共有インスタンスの割り当て(/en-us/netscaler-application-delivery-management-software/media/openstack-service-package-shared.png)

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た柔軟な配置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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

柔軟なポリシーベースのデバイス割り当て

NetScaler Application Delivery Management (ADM) 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の関係が作成されます。この場合、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® ADM 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いずれか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 ADM 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。

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 ADM 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る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 ADM 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

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を以下に示します。

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 ADMホームページから、**Orchestration** > **Cloud Orchestration** > **Placement Policy** 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、ポリシーが互い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** の順に移動し、**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

      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の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)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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)

   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 ADM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 ADMは次のエラーメッセージを表示します。

   「テナント`admin`はいずれのサービスパッケージにも含まれておらず、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 Application Delivery Management (ADM) 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® ADM の両方で実行する必要があるタスクのリストを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、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 ADM 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 ADM ビルド 13.1 をインストールするタスクについては、「NetScaler ADM の展開」を参照してください。

VMware ESXi のハードウェア要件

次の表に、NetScaler ADM 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 ギガビット/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

上記で指定されている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 ADM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VLANタイプのポートグループを作成してください）。

   vSphere Clientでポートグループを設定する(/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、それを上記で作成したVLAN範囲トランクポートグループに接続します。

   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)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADMでのNetScaler VPXインスタンスの追加

NetScaler ADMに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 ADM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。

   オーケストレーション用のインターフェースを構成(/en-us/netscaler-application-delivery-management-software/media/orchestration-configure-vlan-range.png)
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。

   インターフェースのVLANを無効にする(/en-us/netscaler-application-delivery-management-software/media/nmas-vlan-mgmt-interface.jpg)
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。
7. NSX Managerで構成されたVLAN範囲を入力し、**OK** をクリックしてから、**閉じる** をクリックします。

   VLAN範囲の構成(/en-us/netscaler-application-delivery-management-software/media/nmas-vlan-ranges.jpg)

NetScaler ADMへのVMware NSX Managerの登録

VMware NSX ManagerをNetScaler ADMに登録して、両者間の通信チャネルを作成します。

1. NetScaler ADMで、**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、次のパラメータを設定します。

   a. NSX Manager IPアドレス - NSX ManagerのIPアドレス。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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 ADM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. Navigate to **Orchestration** \> **System** \> **Deployment Settings**. トランクポートグループで構成された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 ADM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 ADM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 ADMでのサービスパッケージの作成

1. NetScaler ADM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。

   a. 名前 – サービスパッケージの名前を入力します

   b. 隔離ポリシー – デフォルトでは、隔離ポリシーは「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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サービスパッケージ(/en-us/netscaler-application-delivery-management-software/media/nsx-orch-service-package-settings.jpg)

3. 「**デバイスの割り当て**」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、「**続行**」をクリックします。
4. 「**サービスパッケージの公開**」セクションで、「**続行**」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「**完了**」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-manager-publish-service-package.jpg)

   サービスパッケージの公開(/en-us/netscaler-application-delivery-management-software/media/nmas-manager-publish-service-package-result.jpg)

   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 ADMにオフロードできます。
5. vSphere Web ClientでNSX Managerにログオンし、「**サービス定義**」 \> 「**サービス**」に移動します。

   NetScaler ADM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。

   ADMサービスパッケージの表示(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-service-defn-result.jpg)

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、「**ホーム**」 \> 「**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。

   NSXエッジズ(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-configure-nsx-edge.jpg)
2. 「**管理**」をクリックし、「**ロードバランサー**」タブで「**グローバル構成**」を選択し、「**編集**」をクリックします。

   グローバル構成(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-load-balancer-global-settings.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「**ロードバランサーを有効にする**」、「**ログ記録**」、「**サービス挿入を有効にする**」を選択して有効にします。

   a. 「**サービス定義**」で、NetScaler ADM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名の編集(/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。

   論理スイッチの選択(/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プールの選択**」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プールの選択(/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。VXLANをVLANにマッピングするために、NSX ManagerにL2ゲートウェイが作成されます。

   注

   すべてのデータインターフェースはランタイムNICとして接続され、DLRのインターフェースの一部です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. ランタイムの作成を確認するためにビューを更新します。

   NICの作成を表示するために更新します(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-refresh-runtime-nics.jpg)

   NICの作成を表示するために更新します(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-result-runtime-nics.jpg)

10. VMが起動すると、Statusの値は**In Service**に、Install Stateの値は**Enabled**に変わります。

    注

    NetScaler ADMで、**Orchestration** \> **Requests** に移動して、LBサービス挿入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。

   NSX ManagerでL2ゲートウェイを表示(/en-us/netscaler-application-delivery-management-software/media/nsx-manager-dlr-show.jpg)

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ースに対して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 ADM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を確認できます。IPアドレスのハイパーリンクをクリックして詳細を表示します。

   IPアドレスを構成する(/en-us/netscaler-application-delivery-management-software/media/nmas-ip-address.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

サブネットIPアドレスを構成する(/en-us/netscaler-application-delivery-management-software/media/nmas-subnet-ip-address.jpg)

2. **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。

StyleBookを使用したNetScaler VPXインスタンスの構成

1. NetScaler ADMで、**オーケストレーション** \> **SDNオーケストレーション** \> **NSX Managerの設定** \> **エッジゲートウェイ** の順に移動します。

   StyleBookを介した負荷分散構成を適用する必要がある、それぞれのEdge Gatewayに割り当てられているNetScalerインスタンスのIPをメモしておきます。

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。

   ロードバランサーのパラメーターを指定する(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebook-config-1.jpg)

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。

   ターゲットインスタンスを指定する(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebook-config-2.jpg)

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します(/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。

   構成パックを作成します(/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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ロードバランサー構成を表示します(/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(/en-us/netscaler-application-delivery-management-software/media/nmas-view-sg-config-view.jpg)

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の構成(/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 ADM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. **管理** \> **ロードバランサー** \> **グローバル構成**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 ADM の Edge Gateway は、NSX Manager のランタイムエントリに対応します。

   ☐ NetScaler VPX インスタンスはサービス対象外になります。

4. NetScaler ADM で、**Orchestration** \> **SDN Orchestration** \> **Configure NSX Manager** \> **Edge Gateways** に移動します。Edge Gateway と削除されたインスタンスのそれぞれの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 Application Delivery Management (ADM) 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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。この動的なプロビジョニングには、NetScaler ADMでのNetScaler VPXライセンス割り当ての自動化が必要です。NetScalerライセンスがNetScaler ADMにアップロードされると、NetScaler ADM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。

- 高可用性でセットアップされ、ESXにインストールされたNetScaler ADMバージョン13.0。
- 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 ADMおよびNetScalerインスタンスの高可用性展開

NetScaler ADM 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 ADMイメージファイルをインストールします。NetScaler ADM 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 ADMの展開」を参照してください。

NetScaler® ADM 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 ADMと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 ADM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 ADMでロードバランシング構成情報を提供するには:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler ADM HAノードで、**System** \> **Deployment** に移動します。
2. 右上隅の**HA Settings**をクリックし、**MAS-HA Settings**ページで**MAS-HA Endpoint Details**をクリックします。

3. **MAS-HA Endpoint Details**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、**OK**をクリックします。

VMware NSX ManagerをNetScaler ADMに登録する

2つのNetScaler ADM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 ADMサーバーノードにログオンし、HAモードのNetScaler ADMにVMware NSX Managerを登録して、それらの間に通信チャネルを作成します。

HAモードのNetScaler ADMにVMware NSX Managerを登録するには:

1. プライマリNetScaler ADMサーバーノードで、**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** に移動します。
2. **Configure NSX Manager Settings**をクリックします。
3. **Configure NSX Manager Settings**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 ADMアカウント」セクションで、NSX ManagerのNetScalerドライバーパスワードを設定します。
5. **OK**をクリックします。

NetScaler ADMでのライセンスのアップロード

NetScaler VPXライセンスをNetScaler ADMにアップロードすると、NetScaler ADM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 ADMにライセンスファイルをインストールするには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler ADM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。

   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すでにローカルコンピューターにある場合は、NetScaler ADM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**をクリックして、追加したいライセンスファイル（.lic）を選択します。その後、**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 ADMにライセンスを追加できます。

NetScaler ADM で NetScaler VPX イメージをアップロードする

NetScaler イメージを NetScaler ADM に追加します。これにより、NetScaler ADM はサービスパッケージで定義されているこれらのイメージを使用します。

NetScaler ADM で NetScaler VPX イメージをアップロードするには:

1. NetScaler ADM で、**Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **ESX NSVPX Images** 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から NetScaler VPX zip パッケージを選択します。

NetScaler ADM でサービスパッケージを作成する

NetScaler ADM でサービスパッケージを作成して、NetScaler リソースの割り当て方法を規定する SLA のセットを定義します。

NetScaler ADM でサービスパッケージを作成するには:

1. NetScaler ADM 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** ページの **Basic Settings** セクションで、次のパラメータを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 名前 - サービスパッケージの名前

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

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

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ています。

- 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、Premiumの3種類のライセンスを提供しています
- 2 number - このライセンスを使用すると、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、「**サービス定義**」\> 「**サービスマネージャー**」に移動します。NetScaler ADM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 ADM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 ADMの場合、ライセンスはNetScaler ADM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 ADMノードはアクティブ/パッシブモードです。

Edge向け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** 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。
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 ADMは、IPアドレスの手動または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、他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の値が「In Service」に、Install Stateの値が「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 ADM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 ADM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 ADMがNSX Managerに追加されたことを確認します。

   HAの場合、NetScaler ADM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 ADM HAノードがNSX Managerに追加されたことを確認します。
10. NetScaler ADM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 ADM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。

- [ ] サービス挿入が完了したら、StyleBook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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VMware NSX Manager GUIでNetScaler VPXの負荷分散サービスを構成する
- NetScaler ADM 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StyleBook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** の順に移動し、設定した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 - 「Select」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。

1. 「**管理**」をクリックし、ロードバランサーのタブで「**仮想サーバー**」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、次のパラメーターを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. アプリケーションプロファイル - デフォルトでは、NetScaler ADM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 - 「選択」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 ADMで、**オーケストレーション** \> **リクエスト**に移動し、1つまたは複数の選択したNetScalerインスタンスでのサービス作成完了の進行状況の詳細を確認します。
4. NetScaler ADMで、**アプリケーション** \> **構成**に移動し、`nsx-lb-mon`構成パックが作成されていることを確認します。

   構成パック(/en-us/netscaler-application-delivery-management-software/media/nmas-nsx-integration4.jpg)

NetScaler ADM GUIでのNetScaler VPXにおけるロードバランシングサービスの設定

NetScaler ADM 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モードのNetScalerインスタンスの両方に展開されます。

StyleBookを使用して構成パックを作成するには：

1. NetScaler ADMで、**アプリケーション** \> **構成** \> **新規作成**に移動し、リストから「**HTTP/SSL LoadBalancing (with Monitors) StyleBook**」を選択します。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するユーザーインターフェイスページとして開きます。
2. 必要なすべてのパラメーターの値を指定します。
3. NSX環境でプロビジョニングされているターゲットのNetScaler VPXインスタンスを選択し、「**作成**」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構成にある両方の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。右側のペインで、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 ADM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 ADM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 ADM を使用した Cisco ACI ハイブリッドモードでの NetScaler の自動化

Cisco ACI は、バージョン 1.3 (2f) でハイブリッドモードのサポートを導入しました。ハイブリッドモードでは、Application Policy Infrastructure Controller (APIC) を介してネットワーク自動化を実行できます。一方、L4-L7 の構成は、APIC でデバイスマネージャーとして機能する NetScaler Application Delivery Management (ADM) に委任されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ハイブリッドモードソリューションは、ハイブリッドモードデバイスパッケージと NetScaler ADM によってサポートされています。APIC にハイブリッドモードデバイスパッケージをアップロードする必要があります。このパッケージは、NetScaler からのすべてのネットワーク L2-L3 設定可能エンティティを提供します。アプリケーションのパリティは、NetScaler ADM から APIC への StyleBook によってマッピングされます。言い換えれば、StyleBook は、特定のアプリケーションの L2-L3 と L4-L7 構成間の参照として機能します。NetScaler 用に APIC からネットワークエンティティを構成する際に、StyleBook 名を指定する必要があります。

次の図は、ハイブリッドモードソリューションにおける NetScaler の概要を示しています。

ハイブリッドモードでは、NetScaler の構成は次の2つのフェーズで実行されます。

1. ネットワークのステッチングは Cisco APIC から行われます。
2. 構成は NetScaler® ADM から行われます。

特定のアプリケーションの場合、ネットワーク管理者は、Cisco APIC でのサービスグラフの作成と展開の一部として、IP アドレス、ポート、VLAN (自動化) などのネットワーク固有の詳細を提供する必要があります。これらの構成詳細は、デバイスパッケージを介して NetScaler ADM にプッシュされ、NetScaler ADM はそれらを内部的に処理して NetScaler を構成します。アプリケーション管理者は、NetScaler ADM の StyleBook を使用してアプリケーションの ADC 関連構成を作成し、これらの構成は NetScaler ADM から NetScaler にプッシュされます。Cisco APIC と NetScaler ADM は、管理ネットワークを介して ADC と通信します。

次の図は、ハイブリッドソリューションにおける NetScaler のワークフローを示しています。

前提条件

以下を確認してください。

- Cisco ACIコンポーネントとNetScalerの概念的な知識があること。
  - Cisco ACIとそのコンポーネントの詳細については、製品ドキュメントを参照してください: `<http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>`。
  - NetScalerの詳細については、NetScaler製品ドキュメントを参照してください: `<http://docs.citrix.com/>`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- データセンター内のCisco APICを含む、Cisco ACIの必要なすべてのコンポーネントがセットアップおよび構成されていること。Cisco ACIとそのコンポーネントの詳細については、製品ドキュメントを参照してください: `<http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>`。
- NetScaler 11.1以降がインストールされていること。
- Cisco APICを使用して管理できるように、Cisco ACIでNetScalerが構成されていること。
- 環境にNetScaler Application Delivery Management (ADM) が展開されていること。詳細については、NetScaler ADM 13.1を参照してください。
- APICからNetScaler® ADMおよびADCへの管理接続が確立されていること。
- 以下をメモしてください。
  - 管理およびデータパス接続に使用される接続インターフェイスとIPアドレス。
  - リーフスイッチの詳細: NetScalerのIPアドレス、ポート、インターフェイスなど。

> **注**
>
> このリリースでは、ハイブリッドモードソリューションはシングルコンテキストのNetScalerをサポートしており、管理パーティションはサポートされていません。

Cisco APICとNetScaler ADMを使用してNetScalerをハイブリッドモードで構成する

Cisco APICとNetScaler Application Delivery Management (ADM) を使用して、NetScalerをハイブリッドモードで構成するには、次のタスクを実行します。

1. ファブリック内のNetScalerインスタンスをNetScaler ADMに追加します。手順については、「NetScaler ADMへのインスタンスの追加」を参照してください。
2. NetScaler ADMを使用して、アプリケーションのStyleBookを作成します。手順については、「NetScaler ADMを使用したアプリケーションのStyleBookの作成」を参照してください。
3. NetScalerハイブリッドモードデバイスパッケージをCisco APICにインポートします。手順については、「NetScalerハイブリッドモードデバイスパッケージのCisco APICへのインポート」を参照してください。
4. NetScaler ADMをCisco APICのデバイスマネージャーとして追加します。手順については、「NetScaler ADMをCisco APICのデバイスマネージャーとして追加する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Cisco APICを使用して、Cisco ACIにNetScalerデバイスを追加します。手順については、「NetScalerをCisco ACIのデバイスとして追加する」を参照してください。
6. サービスグラフィックテンプレートを作成して展開します。手順については、「サービスグラフの作成と展開」を参照してください。
7. NetScaler ADMでStyleBookを使用してL4-L7パラメーターを構成します。手順については、「NetScaler ADMのStyleBookを使用したL4-L7パラメーターの構成」を参照してください。
8. Cisco APICからエンドポイントイベントをアタッチまたはデタッチします。詳細については、「APICからのエンドポイントイベントのアタッチまたはデタッチ」を参照してください。

NetScaler ADM を使用してアプリケーション用のStyleBookを作成する

StyleBookは、あらゆるアプリケーションのNetScaler構成を作成および管理するために使用できる構成テンプレートです。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特定のNetScaler機能を構成するためのStyleBookを作成できます。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を設計できます。詳細については、StyleBooksを参照してください。

アプリケーション用の独自のStyleBookを作成するか、NetScaler Application Delivery Management (ADM) に付属のAPIC-HTTP-LB StyleBookを修正して使用できます。

NetScaler ADMでアプリケーション用の独自のStyleBookを作成するには、独自のStyleBookを作成する方法を参照してください。

StyleBookを作成する際は、StyleBookでAPICのサービスグラフモデルに従っていることを確認してください。つまり、任意のアプリケーションのAPICのサービスグラフは、ADC機能を通じて接続されたコンシューマーとプロバイダーのモデルに従います。コンシューマーとプロバイダーはエンドポイントグループ (EPG) として表され、1対1の関係を持ちます。StyleBookでも同じモデルに従う必要があり、プロバイダーEPGはサービスグループとして表され、各エンドポイントはサービスグループのメンバーとして表される必要があります。ADC機能ノードは仮想サーバー (たとえば、ロードバランシング仮想サーバー) によって表される必要があり、仮想サーバーとサービスグループの間には1対1の関係が必要です。

これは本質的にサービスグラフの要点を捉えており、APICからのアタッチまたはデタッチイベントを処理できます。アタッチイベントはエンドポイントを対応するサービスグループにバインドし、デタッチイベントはそれをアンバインドします。ネットワークL2-L3からADC機能L4-L7構成へのシームレスな自動化のために、サービスグラフとStyleBookが同等であることを確認する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ハイブリッドモードデバイスパッケージを Cisco APIC にインポートする

ハイブリッドモードデバイスパッケージは、フルマネージドモードと比較して軽量なパッケージです。デバイスモデルを通じて利用できるのは、L2-L3ネットワークパラメータのみです。デバイスモデルには、1つの汎用ADC機能と、ファブリック内のNetScaler展開（例：ワンアーム、ツーアーム、およびRHIを使用した場合も同様）に基づいた4つの機能プロファイルのみが定義されています。ハイブリッドモードデバイスパッケージの名前は **NetScaler Hybrid Mode Device package 12.0 Build 56.20** です。NetScalerサイト でハイブリッドモードデバイスパッケージを検索し、ダウンロードして、APICにインポートします。

注

ハイブリッドモードデバイスパッケージは、フルマネージドモードデバイスパッケージと共存できます。

APIC GUI を使用してハイブリッドモードデバイスパッケージを APIC にインポートするには:

1. メニューバーで、**L4-L7 Services** タブをクリックし、**Packages** パネルを選択します。
2. **Navigation** ペインで、**L4-L7 Device Types** を右クリックし、**Import Device Package** を選択します。
3. **Import Device Package** ダイアログボックスで、**Browse** をクリックして、ダウンロードしたNetScalerハイブリッドモードデバイスパッケージを選択します。
4. **Submit** をクリックします。デバイスパッケージをAPICに正常にインポートした後、**Navigation** ペインでデバイス名をクリックすると、デバイスパッケージの詳細を表示できます。

重要

デバイスパッケージをインポートした後、APICに障害がないことを確認してください。障害は、Device Types ウィンドウの **Faults** タブをクリックして表示できます。

Cisco APIC で NetScaler ADM をデバイスマネージャーとして追加

May 24, 2018

NetScaler Application Delivery Management (ADM) は、Cisco ACI に展開された NetScaler の集中型デバイスマネージャーとして機能します。Cisco APIC で NetScaler ADM をデバイスマネージャーとして追加する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APIC GUI を使用して APIC に NetScaler ADM をデバイスマネージャーとして追加するには、次の手順を実行します。

1. メニューバーで、**Tenants \> All Tenants** に移動します。
2. **Work** ペインで、テナント名をダブルクリックします。
3. **Navigation** ペインで、***tenant_name* \> L4-L7 Services** を選択します。
4. **Device Managers** を右クリックし、**Create Device Manager** をクリックします。

5. **Create Device Manager** ダイアログボックスで、次の操作を行います。

   a. **Device Manager Name** フィールドに、デバイスマネージャーとして登録する NetScaler ADM 展開の名前を入力します。

   b. **Management EPG** ドロップダウンリストで、管理 EPG を選択します。

   c. **Device Manager Type** ドロップダウンリストで、**Citrix-DevMgr-1.0** を選択します。

   d. **Management** フィールドで、**+** をクリックし、NetScaler ADM 展開の IP アドレスとポートの詳細を追加します。

   e. **Username** フィールドに、NetScaler ADM にアクセスするためのユーザー名を入力します。

   f. 「**パスワード**」フィールドと「**パスワードの確認**」フィールドに、NetScaler ADMにアクセスするためのパスワードを入力します。

   g. **SUBMIT**をクリックします。

      ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/hybrid_mode_register_mas2.jpg)

NetScaler ADMがAPICにデバイスマネージャーとして正常に登録されると、デバイスマネージャーが追加され、**ナビゲーション**ペインに表示されます。登録済みのデバイスマネージャーを表示するには、ナビゲーションペインで「***tenant_name* \> L4-L7 Services \> Device Manager**」に移動します。

ローカライズされた画像(/en-us/netscaler-application-delivery-management-software/media/hybrid_mode_register_mas3.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

Cisco APICとNetScaler ADM間に接続の問題がないこと、およびNetScaler ADMへのアクセスに使用するのと同じ資格情報を提供していることを確認してください。また、アカウントに管理者権限があることを確認してください。

重要

デバイスパッケージをインポートした後、APICに障害がないことを確認してください。障害は、ウィンドウの**障害**タブをクリックして表示できます。

APIを使用してNetScaler ADMをデバイスマネージャーとして登録することもできます。以下は、APIを使用してNetScaler ADMをデバイスマネージャーとして追加する方法を示すXMLペイロードの例です。

```
&lt;polUni>

    &lt;fvTenant name="coke">

        &lt;vnsDevMgr name="MAS1">

            &lt;vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-
DevMgr-1.0" />

            &lt;vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>

            &lt;vnsCCred name="username" value="nsroot"/>

            &lt;vnsCCredSecret name="password" value="*****("/>

        &lt;/vnsDevMgr>

    &lt;/fvTenant>

&lt;/polUni>
```

APICを使用してCisco ACIにNetScalerをデバイスとして追加する

ネットワーク自動化のために、NetScalerをL4-L7デバイスとしてAPICに追加する必要があります。APICは、展開されたサービスグラフに基づいて、LeafとNetScalerデバイス間のネットワークスティッチングを実行します。構成管理IPアドレス、デバイスマネージャー、資格情報など、デバイス構成の基本設定を構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APIC GUIを使用してNetScalerをAPICにデバイスとして登録するには：

1. メニューバーで、**Tenants \> All Tenants** に移動します。
2. **Work** ペインで、テナント名をダブルクリックします。
3. **Navigation** ペインで、***tenant_name*** **\> L4-L7 Services \> L4-L7 Devices** を選択します。
4. Work ペインで、**Actions \> Create L4-L7 Devices** を選択します。
5. **Create L4-L7 Devices** ダイアログボックスの**General** セクションで、次の操作を行います。
   a. **Managed** チェックボックスをオンにします。
   b. **Name** フィールドに、デバイスの名前を入力します。
   c. **Service Type** ドロップダウンリストで、**ADC** を選択します。
   d. **Device Type** フィールドで、**Physical** を選択します。

   注

   VMware ESX の場合は、Virtual を選択し、それぞれのVirtual Machine Manager (VMM) ドメインを関連付けてください。

   e. **Physical Domain** ドロップダウンリストで、物理ドメインを選択します。
   f. 「**モード**」フィールドで、要件に応じて「**シングルノード**」または「**HAクラスター**」を選択します。
   g. 「**デバイスパッケージ**」ドロップダウンリストで、「**Citrix-NetScalerMAS-1.0**」を選択します。
   h. 「**モデル**」ドロップダウンリストで、デバイスモデルを選択します。たとえば、NetScaler-MPX、またはNetScaler-VPXです。
6. 「**接続**」セクションで、NetScalerがファブリックでどのように構成されているかに応じて、「**APICからデバイス管理への接続**」フィールドで「**帯域外**」または「**帯域内**」を選択します。
7. 「**資格情報**」セクションで、デバイスにアクセスするためのユーザー名とパスワードを指定します。
8. 「**デバイス1**」および「**デバイス2**」セクションで、それぞれ管理関連の設定を完了します。
9. 「**クラスター**」セクションで、クラスターの管理関連の設定を完了します。「**デバイスマネージャー**」ドロップダウンリストで、Cisco APICにNetScaler ADMをデバイスマネージャーとして追加するで作成したデバイスマネージャーを選択していることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 「**次へ**」をクリックします。「デバイス構成」ページが表示されます。ハイブリッドモードのデバイスパッケージは、高可用性、機能とモードの有効化/無効化、NTP、SNMP、SNMPアラームなどのデバイスおよびクラスター固有の構成詳細を提供しません。これらの構成はNetScaler ADMを使用して行う必要があります。
11. 「**完了**」をクリックします。APICにデバイスが正常に登録されると、デバイスが追加され、ナビゲーションペインに表示されます。登録されたデバイスを表示するには、ナビゲーションペインで「***tenant_name* \> L4-L7サービス \> L4-L7デバイス \> device_name**」に移動します。

重要

デバイスを登録した後、APICに障害がないことを確認してください。「**作業**」ペインの「**障害**」タブをクリックすると、障害を表示できます。

APIを使用してNetScalerデバイスを登録することもできます。以下は、L4-L7デバイスを追加するためのXMLペイロードのサンプルです。

```
&lt;polUni>

    &lt;fvTenant name="coke">

    &lt;vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

     &lt;vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

     &lt;vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

     &lt;vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
&lt;vnsCCred name="username" value="nsroot"/>

&lt;vnsCCredSecret name="password" value="*****"/>

&lt;vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

&lt;vnsCDev name="ADC1" devCtxLbl="C1">

&lt;vnsCIf name="1_1">

&lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/33]"/>

&lt;/vnsCIf>

&lt;vnsCIf name="1_2">

&lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/35]"/>

&lt;/vnsCIf>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
&lt;vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>

&lt;vnsCCred name="username" value="nsroot"/>

&lt;vnsCCredSecret name="password" value="****"/>

&lt;/vnsCDev>

&lt;vnsCDev name="ADC2" devCtxLbl="C1">

&lt;vnsCIf name="1_1">

&lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/34]"/>

&lt;/vnsCIf>

&lt;vnsCIf name="1_2">

&lt;vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/36]"/>

&lt;/vnsCIf>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
&lt;vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>

&lt;vnsCCred name="username" value="nsroot"/>

&lt;vnsCCredSecret name="password" value="*****"/>

&lt;/vnsCDev>

&lt;vnsLIf name="outside">

&lt;vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
mIfLbl-outside"/>

&lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
cIf-1_1"/>

&lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
cIf-1_1"/>

&lt;/vnsLIf>

&lt;vnsLIf name="inside">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     &lt;vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
mIfLbl-inside"/>



     &lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
cIf-1_2"/>



     &lt;vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
cIf-1_2"/>



     &lt;/vnsLIf>



     </vnsLDevV



     &lt;/fvTenant>



     &lt;/polUni>
```

サービスグラフを作成して展開する

NetScalerを作成および展開するには、APICでCisco APICサービスグラフテンプレートを使用する必要があります。サービスグラフを作成および展開する際は、ADC機能プロファイルを使用していることを確認してください。

APICでグラフが構成されると、APICは機能定義、ファブリックへのデバイス接続、およびグラフ展開の一部として構成されたエンティティに基づいてデバイス構成を自動化します。APICは、サービスグラフ作成の一部として、VLAN割り当てとそのバインディングなどのネットワーク構成も自動化し、APICからグラフを削除すると構成は削除されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サービスグラフは、アプリケーションの2つ以上の層として表され、それらの間に適切なサービス機能が挿入されます。サービスグラフは、コントラクトによって送信元EPGと宛先EPGの間に挿入されます。

APIC GUIを使用してサービスグラフを作成するには：

1. メニューバーで、**Tenants \> All Tenants** に移動します。
2. **Work** ペインで、テナント名をダブルクリックします。
3. **ナビゲーション** ペインで、***tenant_name*** **\> L4-L7 Services \> L4-L7 Service Graph Templates** を選択します。
4. **Work** ペインで、**Actions \> Create a L4-L7 Service Graph Template** を選択します。
5. **Create a L4-L7 Service Graph Template** ダイアログボックスの「Device Clusters」セクションで、デバイスクラスターを選択し、次の操作を行います。
   a. **Graph Name** フィールドに、サービスグラフテンプレートの名前を入力します。
   b. **Graph Type** フィールドで、**Create A New One** を選択します。
   c. **Device Cluster** セクションから、デバイスをドラッグし、コンシューマーエンドポイントグループとプロバイダーエンドポイントグループの間にドロップして、サービスノードを作成します。

   d. \<***L4-L7device_name information***\> セクションで、次の操作を行います。
      i. 「**ADC**」フィールドで、NetScaler がファブリックに展開されている方法に応じて、「**One-Arm**」または「**Two-Arm**」を選択します。
      ii. 「**Profile**」ドロップダウンリストで、デバイスパッケージで提供されている機能プロファイルを選択します。

      iii. 「**SUBMIT**」をクリックします。
6. 「**Navigation**」ペインで、サービスグラフィックテンプレートをクリックします。画面にサービスグラフィックテンプレートのグラフィックトポロジが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

Cisco APIC はコネクタの概念をサポートしており、これらのコネクタは ADCCluster ノードに表示されます。コネクタは、ネットワークトラフィックの方向と、接続が外部か内部かに応じて、割り当てられた VLAN を仮想 IP (VIP) またはサブネット IP (SNIP) アドレスに動的にバインドするデバイススクリプトを定義します。VLAN は、インバウンドおよびアウトバウンドトラフィックに使用される特定のインターフェイスにもバインドされます。

サービスグラフィックテンプレートをエンドポイントグループに適用する

サービスグラフィックテンプレートを作成したら、APIC GUI を使用して作成したサービスグラフィックテンプレートを適用する必要があります。

サービスグラフィックテンプレートを適用するには：

1. メニューバーで、**Tenants \> All Tenants** に移動します。
2. 「**Work**」ペインで、テナント名をダブルクリックします。
3. ナビゲーションペインで、***tenant_name*** **\> L4-L7 Services \> L4-L7 Service Graph Templates** を選択します。
4. ***template_name*** を右クリックし、「**Apply L4-L7 Service Graph Template**」をクリックします。

5. 「**Apply L4-L7 Service Graph Template To EPGs**」ダイアログボックスの「**EPG Information**」セクションで、次のフィールドに入力します。
   a. 「**Consumer EPG/External Network**」ドロップダウンリストで、コンシューマーエンドポイントグループを選択します。
   b. 「**Provider EPG/External Network**」ドロップダウンリストで、プロバイダーエンドポイントグループを選択します。
   c. 「**Contract Information**」セクションで、適切なフィールドに入力します。契約情報は Cisco APICに固有のものであり、EPGに関連付けられたセキュリティポリシーの一部として構成されます。

   d. 「**Next**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. 「**Graph Template**」ドロップダウンリストで、作成したサービスグラフテンプレートを選択します。

f. 「**Connector**」セクションで、次の操作を行います。

i. 「**Type**」フィールドで、「General」を選択します。

ii. 「**BD**」ドロップダウンリストで、ブリッジドメインを選択します。コネクタの詳細は、Cisco APICインフラストラクチャモデルの一部であるブリッジドメインの一部です。

iii. 「**Cluster Interface**」ドロップダウンリストで、選択したブリッジドメインに適切なクラスタインターフェースを選択します。

Cisco APICは、選択したサービスグラフテンプレートで必要とされるように、NetScalerデバイスとファブリック間のデータパス通信に選択されたブリッジドメインを使用します。

iv. 「**Next**」をクリックします。

「**Parameters**」画面の「**Required Parameters**」タブで、プロファイルで必須とされているIPアドレスなど、L2-L3固有の詳細を入力します。もう1つの主要なパラメータはStyleBook名です。これは、NetScaler Application Delivery Management (ADM) で提供されている組み込みのStyleBook「**APIC-HTTP-LB**」でも、NetScaler ADM を使用したアプリケーションの StyleBook の作成で作成したStyleBookの名前でもかまいません。

「

注

」

StyleBook名は、特定のアプリケーションに対してNetScaler ADMで作成されたL4-L7構成とサービスグラフの詳細をリンクします。

Cisco APIC GUIでは、機能（ロードバランシングなど）に基づいてパラメータをフィルタリングできます。必須パラメータはすべて「**Required Parameters**」タブで表示および設定でき、機能に関連するその他のパラメータはすべて「**All Parameters**」タブで表示および設定できます。

「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

」

デフォルトでは、組み込みのワンアームプロファイルでは、IPアドレスやネットマスクなどのSNIP詳細を指定する必要があります。その他のネットワークパラメータは、Cisco APIC GUIで「**All Parameters**」をクリックし、「**Configure Network**」ツリーを展開することで表示できます。これにより、NetScalerでサポートされているすべてのネットワークパラメータが一覧表示されます。Cisco APIC GUIから、任意のエンティティをインスタンス化し、リストされた属性に値を提供できます。

6. 「**Finish**」をクリックします。

「

重要

」

サービスグラフテンプレートを適用した後、展開されたグラフに障害がないことを確認してください。障害は、「**Work**」ペインの「**Faults**」タブをクリックして表示できます。

サービスグラフの展開の一環として、ハイブリッドモードデバイスパッケージはCisco APICからNetScaler ADMに構成詳細をプッシュします。NetScaler ADMは、これらの構成を内部的にそれぞれのNetScalerに処理し、APICに応答を返します。グラフの展開が成功すると、障害はなく、NetScalerは対応するグラフのファブリックと正常にネットワーク接続されます。

APICは、APIを使用してグラフを構成および展開するさまざまな方法をサポートしており、グラフの展開には、テナント、コントラクト、VLAN、名前空間などのAPIC固有のいくつかの構成要素に対するさまざまな依存関係が含まれます。

以下のサンプルアプローチは、APIC固有のアーティファクトがAPICにすでに構成されていることを前提として、APICのAPIを利用してL4-L7グラフを作成および展開する方法の1つを示しています。

重要

これらのXMLペイロードは参考として使用し、ご自身の環境で使用する前にXMLに適切な変更を加えてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以下は、APIを使用してサービスグラフを作成および展開する例です。

a. AppProfileの作成
b. サービスグラフの詳細の作成
c. サービスグラフを契約に添付する

以下は、AppProfileを作成するためのXMLペイロードのサンプルです。AppProfileにはEPGが含まれており、プロバイダーEPGにはNetScaler固有のエンティティ、属性、およびその値が含まれています。以下のサンプルXMLペイロードでは、NSIPなどのNetScaler固有のネットワークエンティティが、一連の属性とStyleBook名で作成されます。

```
<polUni>

    <fvTenant name="coke">

        <!-- Application Profile -->

        <fvAp dn="uni/tn-coke/ap-sap" name="sap">

            <!-- EPG 1  -->

            <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">

                <fvRsBd tnFvBDName="BD_web" />

                <!-- --------- CONFIG PAYLOAD ---------------- -->

                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network"
name="Network">

                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip1">

                        <vnsParamInst key="ipaddress" name="ip1"
value="110.110.110.2"/>

                        <vnsParamInst key="netmask" name="netmask1"
value="255.255.255.0"/>

                        <vnsParamInst key="type" name="tye"
value="SNIP"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        <vnsParamInst key="dynamicrouting"
name="dynamicrouting" value="DISABLED"/>

                        <vnsParamInst key="hostroute" name="hostroute"
value="DISABLED"/>

                    </vnsFolderInst>

                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip2">

                        <vnsParamInst key="ipaddress" name="ip2"
value="220.220.220.2"/>

                        <vnsParamInst key="netmask" name="netmask2"
value="255.255.255.0"/>

                        <vnsParamInst key="type" name="tye"
value="SNIP"/>

                        <vnsParamInst key="dynamicrouting"
name="dynamicrouting" value="DISABLED"/>

                        <vnsParamInst key="hostroute" name="hostroute"
value="DISABLED"/>

                    </vnsFolderInst>

                </vnsFolderInst>

                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
name="stylebook_1">

                    <vnsParamInst name="stylebookName" key="name"
value="APIC-HTTP-LB"/>

                </vnsFolderInst>

                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="internal_network"
name="internal_network">
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    <vnsCfgRelInst name="internal_network_key"
key="internal_network_key" targetName="Network/snip1"/>

                </vnsFolderInst>

                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="external_network"
name="external_network">

                    <vnsCfgRelInst name="external_network_key"
key="external_network_key" targetName="Network/snip2"/>

                </vnsFolderInst>

                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook"
name="mFCngStylebook_1">

                    <vnsCfgRelInst name="Stylebook_key"
key="Stylebook_key" targetName="stylebook_1"/>

                </vnsFolderInst>

                <!-- ------- END CONFIG PAYLOAD -------------- -->

                <fvSubnet ip="110.110.110.110/24" scope="shared"/>

                <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>

                <fvRsDomAtt tDn="uni/phys-sepg" />

                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>

            </fvAEPg>

            <!-- EPG 2 -->

            <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">

                <fvRsCons tnVzBrCPName="Ctrct1"/>

                <fvRsBd tnFvBDName="BD_app" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                <fvSubnet ip="220.220.220.220/24" scope="shared"/>

                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-
[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>

                <fvRsDomAtt tDn="uni/phys-sepg" />

            </fvAEPg>

        </fvAp>

    </fvTenant>

</polUni>
```

以下は、サービスグラフの詳細を作成するためのXMLペイロードのサンプルです。

```
<polUni>

    <fvTenant name="coke">

        <vnsAbsGraph name = "Graph1">

            <vnsAbsTermNodeProv name = "Input1">

                <vnsAbsTermConn name = "C1"></vnsAbsTermConn>

            </vnsAbsTermNodeProv>

            <vnsAbsNode name="ADC" funcType="GoTo">

                <vnsAbsFuncConn name = "outside" attNotify="true">

                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />

                </vnsAbsFuncConn>

                <vnsAbsFuncConn name = "inside" attNotify="true">

                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                </vnsAbsFuncConn>

                <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction"/>

                <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph-
Graph1/AbsTermNodeProv-Input1/outtmnl"/>

                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
ADCOneArmServiceProfileGroup/absFuncProf-A

DCOneArmFunctionProfile"/>

                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-ADCCluster1"/
>

            </vnsAbsNode>

            <vnsAbsTermNodeCon name = "Output1">

                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>

            </vnsAbsTermNodeCon>

            <vnsAbsConnection name = "CON1">

                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-
Graph1/AbsTermNodeCon-Output1/AbsTConn" />

                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-
Graph1/AbsNode-ADC/AbsFConn-outside" />

            </vnsAbsConnection>

            <vnsAbsConnection name = "CON2">

                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-
Graph1/AbsNode-ADC/AbsFConn-inside" />

                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-
Graph1/AbsTermNodeProv-Input1/AbsTConn" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            </vnsAbsConnection>

        </vnsAbsGraph>

    </fvTenant>

</polUni>
```

以下は、サービスグラフを契約に添付するためのXMLペイロードのサンプルです。

```
<polUni>

    <fvTenant name="coke">

        <vzBrCP name="Ctrct1">

            <vzSubj name="http">

                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>

            </vzSubj>

        </vzBrCP>

    </fvTenant>

</polUni>
```

NetScaler ADMからStyleBookを使用してL4-L7パラメータを構成する

May 24, 2018

NetScaler Application Delivery Management (ADM) では、**Cisco ACI** の下の **Orchestration** タブで、展開されたサービスグラフの詳細を表示できます。表形式ビューには、グラフ名、テナント名、コンテキスト、StyleBook名、ネットワーク構成ステータスなどのサービスグラフの詳細が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

グラフがCisco APICから削除されると、L4-L7構成を含む対応する構成がデバイスから削除されます。

さらに、表形式ビューでは、テーブルに表示されている任意の列でソートしたり、検索オプションを使用してデータをフィルタリングしたりできます。ドロップダウン列リストから列名を選択または選択解除することで、列の詳細をカスタマイズすることもできます。

また、**検索**ボタンをクリックして検索オプションを使用し、データをフィルタリングすることもできます。ドロップダウンボックスから任意の列を選択し、対応する値を入力して、テーブルに表示されるデータをフィルタリングできます。

注

検索機能では大文字と小文字が区別されるため、正確な検索条件を指定する必要があります。

NetScaler ADMでStyleBookを使用してL4-L7構成を展開するには：

1. 表形式ビューでURLとして表示されるStyleBook名をクリックします。
2. 「構成」ウィンドウで、**StyleBook** をダブルクリックします。
3. 「構成の展開」ウィンドウで、次の操作を行います。
   a. **アプリケーション名**フィールドに、APICのアプリケーションのサービスグラフに対応するADC機能構成の名前を入力します。
   b. 「サービス（ポート）設定」セクションで、**+** をクリックします。
   c. 「**サービスグラフで定義されたEPGとエンドポイント（ポート）の設定**」ウィンドウで、StyleBookから入力されたパラメータの値を入力し、**作成**をクリックします。
   d. **作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBookで指定されたL4-L7構成がNetScaler ADMに展開されます。**アプリケーション**タブから、**アプリケーション \> 構成**に移動して、StyleBook構成を表示できます。

APICからのエンドポイントイベントのアタッチとデタッチ

ハイブリッドモードソリューションは、Cisco APICからのエンドポイントのアタッチまたはデタッチイベントを暗黙的に処理します。Cisco APICがエンドポイントのアタッチイベントをトリガーすると、NetScaler Application Delivery Management (ADM) のStyleBookによってservicegroup_servicegroupmember_bindingが自動的にトリガーされ、デタッチエンドポイントイベント中にエンドポイントはバインド解除されます。

さらに、Cisco APICでアタッチまたはデタッチエンドポイントイベントがトリガーされる前にNetScaler ADMにL4-L7構成を展開していない場合、ソリューションはアタッチIPアドレスをデータベースに保持します。これらのIPアドレスは、サービスグループがStyleBookを通じて作成された後、対応するサービスグループにバインドされます。

APIC 障害レポート

Cisco ACI に NetScaler デバイスパッケージを展開すると、Cisco APIC はすべての障害を報告します。APIC の任意のレベル (デバイス、テナント、EPG、サービスグラフなど) で障害レポートを表示できます。以下のスクリーンショットは、デバイスレベルでの障害レポートを示しています。障害の詳細については、`<http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html>` を参照してください。

任意の APIC エンティティを選択し、**Faults** タブをクリックすると、そのエンティティについて APIC が報告した障害が表示されます。

NetScaler® ADM によって生成されたログ

NetScaler Application Delivery Management (ADM) は、問題のトラブルシューティングに役立つ広範なログを提供します。生成されたログ (**admin.log**) は、次の場所にあります: **/var/controlcenter/log/**

NetScaler ADM にログオンし、シェルを使用して NetScaler ADM ディレクトリ構造に移動できます。以下は、APIC のグラフ展開に関する NetScaler ADM ログのサンプルスニペットです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
2016-06-29 10:58:33,816 DEBUG APIC Config  = {(0, '', 5230): {'dn': u'uni/
vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-
cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant':
'coke_SDX2', 'ctxName': 'cokectx1', 'value': {(10, '',
'ADCHybridMode_1_Consumer_1'): {'state': 1, 'transaction': 0, 'cifs':
{'ADCHybridMode_1_Device_1': '1_1'}, 'ackedstate': 0}, (7, '',
'2129920_32778'): {'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0,
'transaction': 0}, (1, '', 5790): {'transaction': 0, 'ackedstate': 0,
'value': {(3, 'ADCFunction', 'N1'): {'state': 1, 'transaction': 0,
'ackedstate': 0, 'value': {(4, 'mFCngNetwork', 'mFCngnetwork'): {'state':
1, 'transaction': 0, 'ackedstate': 0, 'value': {(6, 'Network_key',
'network_key'): {'state': 1, 'transaction': 0, 'target': 'network',
'ackedstate': 0}}}, (4, 'internal_network', 'internal_network'):
{'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate': 0,
'value': {(6, 'internal_network_key', 'internal_network_key'): {'state':
1, 'transaction': 0, 'target': 'network/internal_snip', 'ackedstate':
0}}}, (2, 'external', 'consumer'): {'state': 1, 'transaction': 0,
'ackedstate': 0, 'value': {(9, '',
'ADCHybridMode_1_Consumer_1_2129920_32778'): {'state': 1, 'transaction':
0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate':
0}}}, (4, 'mFCngStylebook', 'mFCngStylebook'): {'state': 1, 'transaction':
0, 'ackedstate': 0, 'value': {(6, 'Stylebook_key', 'Stylebook_key'):
{'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate':
0}}}, (2, 'internal', 'provider'): {'state': 1, 'transaction': 0,
'ackedstate': 0, 'value': {(9, '',
'ADCHybridMode_1_Consumer_1_2129920_32778'): {'state': 1, 'transaction':
0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate':
0}}}}}}, 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/
tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-
coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]'}, (4,
'Network', 'network'): {'state': 1, 'transaction': 0, 'ackedstate': 0,
'value': {(4, 'nsip', 'internal_snip'): {'state': 1, 'transaction': 0,
'ackedstate': 0, 'value': {(5, 'type', 'type'): {'state': 1,
'transaction': 0, 'ackedstate': 0, 'value': 'SNIP'}, (5, 'hostroute',
'hostroute'): {'state': 1, 'transaction': 0, 'ackedstate': 0, 'value':
'DISABLED'}, (5, 'ipaddress', 'ipaddress'): {'state': 1, 'transaction': 0,
'ackedstate': 0, 'value': '10.1.1.1'}, (5, 'dynamicrouting',
'dynamicRouting'): {'state': 1, 'transaction': 0, 'ackedstate': 0,
'value': 'ENABLED'}, (5, 'netmask', 'netmask'): {'state': 1,
'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0'}}}}}, (8, '',
'ADCHybridMode_1_Consumer_1_2129920_32778'): {'state': 1, 'transaction':
0, 'vif': 'ADCHybridMode_1_Consumer_1', 'ackedstate': 0, 'encap':
'2129920_32778'}, (4, 'Stylebook', 'stylebook_1'): {'state': 1,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
'transaction': 0, 'ackedstate': 0, 'value': {(5, 'name', 'stylebookName'):
{'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-
LB'}}}}, 'txid': 10000}}

2016-06-29 10:58:33,816 DEBUG get Graph Return details = {'graphDN':
u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
coke_SDX2]-ctx-cokectx1', (1, '', 5790): {'state': 1, 'graphrn': u'vGrp-
[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-
coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]'},
'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB',
'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1',
'graphInstanceId': 5790}

2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0

2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2

2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1

2016-06-29 10:58:33,867 DEBUG
fn_wrapper:long_operation_thread_id:<eventlet.greenthread.GreenThread
object at 0x80aa5c7d0>

2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
Details  = 10.102.102.62 ++++++++++++++++

2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2

2016-06-29 10:58:33,867 DEBUG Host name from device = ADCHybridMode_1

"InProgress","message":null,"replication_status":"","target":"10.102.102.8
1","operation":"POST","entity_type":"apic","entity_id":null}}

2016-06-29 10:58:44,141 DEBUG  Save config  Response = { "errorcode": 0,
"message": "Done", "severity": "NONE" }

2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True

2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from Config ++
++++

2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {'state': 1,
'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230} ++++++
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
2016-06-29 10:58:44,142 DEBUG Service health details = {} collection
length = 0

2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down = 0

2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0

2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {((0, '',
5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {'faults': [], 'state':
0, 'health': ([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')],
0)}}

2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List = []

2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {'devs':
'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health': [([(0, '',
5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)]}

2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = { "errorcode": 0,
"message": "Done", "severity": "NONE" }, sessionId =
##D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7ED
F27646B2509164EEFBCB549EDAB6E6168ED0AEA68452DED6D30ACBED4BC34998DE818F7290
C9B44342054168DFB89DF1AFA9A4378F1DB07F03BF6C9B4F6A7A38E6A5F1BFED70C7225318
1397E305B14FF490861C3F8114948538

2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {'10.102.102.62':
{'10.102.102.62': {u'errorcode': 0, 'status_code': 201, u'message':
u'Done', u'severity': u'NONE', 'operation_name': 'add_op'}}, (7, '',
'2129920_32778'): {'vlan': {u'errorcode': 0, 'status_code': 201,
u'message': u'Done', u'severity': u'NONE', 'operation_name': 'add_op'}},
(((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, 'internal',
'provider')), 'nsip'): {'vlan_nsip_binding': {u'errorcode': 0,
'status_code': 201, u'message': u'Done', u'severity': u'NONE',
'operation_name': 'bind_op'}}, (((0, '', 5230), (4, 'Network',
'network')), (4, 'nsip', 'internal_snip')): {'nsip': {u'errorcode': 0,
'status_code': 201, u'message': u'Done', u'severity': u'NONE',
'operation_name': 'add_op'}}, (): {}, (8, '',
'ADCHybridMode_1_Consumer_1_2129920_32778'): {'vlan_interface_binding':
{u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
u'NONE', 'operation_name': 'bind_op'}}}

2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg =
Done, statusCode = add_op
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg =
Done, statusCode = add_op

2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op, erMsg =
Done, statusCode = bind_op

2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg =
Done, statusCode = add_op

2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op, erMsg =
Done, statusCode = bind_op

2016-06-29 10:58:44,238 DEBUG ++++++++++++++ ServiceAudit response =
{'faults': [], 'state': 0, 'health': []}

2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {'graphDN': u'uni/vDev-
[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-
cokectx1', (1, '', 5790): {'state': 1, 'graphrn': u'vGrp-[uni/tn-
coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-
coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]'},
'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB',
'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1',
'graphInstanceId': 5790}

2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task: create
apic_graph

2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2

2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2

2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector collection from
Config with type 22 for attach & detach event ++++++

2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {0: [], 1:
[], 3: []}

2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList = []

2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps attachIpList = []
dettachIpList = []

2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row =
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni/
vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-
cokectx1', 'apicGraphState': None, 'serviceGroupName': None,
'configPackId': None, 'tenantName': u'coke_SDX2', 'styleBookName': u'APIC-
HTTP-LB', 'graphInstanceName': u'HybridModeGraph_1', 'context':
u'cokectx1', 'serviceGroupPort': None, 'graphInstanceId': 5790,
'createDate': None, 'serviceGroupIP': None}
```

ハイブリッドモードデバイスパッケージによって生成されたログ

NetScaler Hybrid Mode デバイスパッケージは、構成関連ログと監視関連ログを生成します。生成されたログは、**/data/devicescript/ Citrix.NetScalerMAS.1.0/logs** にあります。

以下は、Cisco APIC の **debug.log** のサンプルスニペットです。

```
2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62, 24063]
Device manager details ip = 10.102.102.81, port = 80

2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62, 24063] ++
++++++++++++ serviceAudit  request +++++++++++++++++

2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62, 24063] ++
++++++++ getStyleBookObjects ++++++++++++

2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62, 24063]
NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 = {'state': 1,
'transaction': 0, 'ackedstate': 0, 'value': {(5, 'name', 'stylebookName'):
{'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'}}}

2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62, 24063]
NMAS collection styleBookName= APIC-HTTP-LB

2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62, 24063]
NMAS collection retCol= {'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '',
5230), (4, 'Stylebook', 'stylebook_1'))}

2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62, 24063]  +
+++ devMgrStyleBookUrl = http://10.102.102.81/stylebook/nitro/v1/config/
stylebooks/com.citrix.adc.stylebooks/1.1/APIC-HTTP-LB

2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62, 24063]  +
+++ Response from styleBookresCode serviceAudit = {u'stylebook':
{u'uses_builtin_namespaces': {u'netscaler.nitro.config': u'10.5'},
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace':
u'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-
LB\nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name:
"Sample StyleBook for APIC Load Balanced Application"\ndescription: "This
is a sample StyleBook for HTTP Load Balanced Application configuration via
APIC"\nschema-version: "1.0"\nimport-stylebooks: \n  - \n    namespace:
netscaler.nitro.config\n    prefix: ns\n    version: "10.5"\n  - \n
namespace: "com.citrix.adc.stylebooks"\n    prefix: "stlb"\n    version:
"1.1"\nparameters-default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n
lb-name(appname, port): $appname + "-" + str($port) + "-lb"\n  sg-
name(appname, port): $appname + "-" + str($port) + "-sg"\n
healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n  -
\n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
$parameters.app-services\n    repeat-item: app\n    properties: \n
name: $substitutions.lb-name($parameters.appname, $app.virtual-port)
\n      ipv46: $app.virtual-ip\n      port: $app.virtual-port\n
servicetype: $app.protocol\n      lbmethod?: $app.algorithm\n
persistencetype?: $app.persistence\n  - \n    name: svcgrp\n    type:
ns::servicegroup\n    repeat: $parameters.app-services\n    repeat-item:
app\n    properties: \n      name: $substitutions.sg-
name($parameters.appname, $app.virtual-port)\n      servicetype:
$app.protocol\n      useproxyport?: $app.sg-advanced.useproxyport\n
usip?: $app.sg-advanced.usip\n      cip?: $app.sg-advanced.cip\n
cipheader?: $app.sg-advanced.cipheader\n      healthmonitor?:
$substitutions.healthmonitor($app.skip_healthmonitor)\n    components:
\n      -\n        name: lbvserver-svg-binding\n        type:
ns::lbvserver_servicegroup_binding\n        properties: \n          name:
$substitutions.lb-name($parameters.appname, $app.virtual-port)\n
servicegroupname: $parent.properties.name\n      - \n        name: svg-
members\n        type:
ns::servicegroup_servicegroupmember_binding\n        condition:
$app.server-ips\n        repeat: $app.server-ips\n        repeat-item:
serverip\n        properties: \n          ip: $serverip\n          port:
$app.server-port\n          servicegroupname:
$parent.properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
$components.lbvserver\n  - \n    name: servicegroups\n    value:
$components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{u'version':
u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name': u'APIC-
ROOT'}]}}

2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62, 24063]  +
+++ Dev Mgr request details devMgrUrl = http://10.102.102.81/admin/v1/apic

2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62, 24063]  +
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
+++ Response from Device Mgr serviceAudit = {"APIC":[]}

2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62, 24063] ++
++++++++++++ serviceAudit response = {"APIC":[]}

2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62, 24063] ++
++++++++++++ serviceAudit response headers content type= application/json;
charset=utf-8

2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62, 24063] ++
++++++++++++ serviceAudit response headers = {'content-length': '11',
'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', 'x-content-type-
options': 'nosniff', 'transfer-encoding': 'chunked', 'connection':
'close', 'date': 'Wed, 29 Jun 2016 10:58:33 GMT', 'x-frame-options':
'SAMEORIGIN', 'content-type': 'application/json; charset=utf-8'}

2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62, 24063] ++
++++++++++++ pollingURL = http://10.102.102.81/admin/v1/journalcontexts/
ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea

2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62, 24063] ++
++++++++++++ pollingStatus = True, pollingTime = 0

2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62, 24063] ++
++++++++++++ pollingResponse json = {u'journalcontext': {u'status': u'In
Progress', u'scopes': [], u'entity_id': None, u'name': u'Create apic',
u'operation': u'POST', u'entity_type': u'apic', u'service_name': u'admin',
u'start_time': u'2016-06-29T10:58:33.760565', u'is_default': u'false',
u'end_time': None, u'target': u'10.102.102.81', u'message': None, u'id':
u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'replication_status': u''}}

2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62, 24063] ++
++++++++++++ pollingStatus = True, pollingTime = 1

2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62, 24063] ++
++++++++++++ pollingResponse json = {u'journalcontext': {u'status': u'In
Progress', u'scopes': [], u'entity_id': None, u'name': u'Create apic',
u'operation': u'POST', u'entity_type': u'apic', u'service_name': u'admin',
u'start_time': u'2016-06-29T10:58:33.760565', u'is_default': u'false',
u'end_time': None, u'target': u'10.102.102.81', u'message': None, u'id':
u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'replication_status': u''}}

2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62, 24063] ++
++++++++++++ pollingStatus = True, pollingTime = 2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62, 24063] ++
++++++++++++ pollingResponse json = {u'journalcontext': {u'status':
u'Finished', u'scopes': [], u'entity_id': None, u'name': u'Create apic',
u'operation': u'POST', u'entity_type': u'apic', u'service_name': u'admin',
u'start_time': u'2016-06-29T10:58:33.760565', u'is_default': u'false',
u'end_time': u'2016-06-29T10:58:44.486919', u'target': u'10.102.102.81',
u'message': u'Done', u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea',
u'replication_status': u''}}

2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62, 24063]
Attempts 1

2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62, 24063]
Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0, '', 5230)),
transaction: 0

2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62, 24063]
Attempts for {'name': 'ADCHybridMode_1', 'host': '10.102.102.62',
'virtual': False, 'devs': {'ADCHybridMode_1_Device_1': {'state': 0,
'virtual': False, 'manager': {'hosts': {'10.102.102.81': {'port': 80}},
'name': 'NMAS_1', 'creds': {'username': 'nsroot', 'password':
'<hidden>'}}, 'version': '11.0', 'host': '10.102.102.62', 'port': 80,
'creds': {'username': 'nsroot', 'password': '<hidden>'}}}, 'manager':
{'hosts': {'10.102.102.81': {'port': 80}}, 'name': 'NMAS_1', 'creds':
{'username': 'nsroot', 'password': '<hidden>'}}, 'contextaware': True,
'port': 80, 'creds': {'username': 'nsroot', 'password': '<hidden>'}} is 0

2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62, 24063]
Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0, '', 5230))

2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62, 24063]
pending: False, delete: False, txId: None

2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62, 24063]
Faults: []

2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62, 24063]
Health: []

2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62, 24063]
Send num: 761, type: 220, len: 382
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cisco ACIのクラウドオーケストレーターモードにおけるNetScalerデバイスパッケージ

Application Policy Infrastructure Controller (APIC) バージョン3.1により、Citrix NetScalerとCisco ACIは、共同統合ポートフォリオを拡張し、顧客のニーズに対応する新しいソリューションを提供します。新しい統合モードであるACIクラウドオーケストレーターモード*,*は、標準化されたパラメータを通じて構成の複雑さを抽象化することで、L4-L7統合を簡素化します。このソリューションは、L4-L7サービスをシームレスに自動化し、アジャイルなアプリケーション展開、運用上の柔軟性、シンプルさという目標を達成します。

NetScalerソリューションを使用するCisco ACIクラウドオーケストレーターモードは、以下の利点を提供します。

- L4-L7サービスの自動化により、ヒューマンエラーが削減されます。
- Cisco ACIソリューションの事前構築済み統合により、展開時間を短縮し、Webアプリケーション、仮想マシン、SQLなどのアプリケーションのパフォーマンスを向上させることができます。
- Webアプリケーション、仮想マシン、SQLなどのアプリケーションの健全性について、物理および仮想ネットワークコンポーネント全体にわたる完全に統合された可視性。

ACIクラウドオーケストレーターモードでは、新しい簡素化されたAPIC GUIを直接利用するか、Cisco Cloud Center、Windows Azure Pack、OpenStack、vRealizeなど、好みに応じて任意のクラウドオーケストレーターを選択するかの選択肢が増えました。この新しい変更は、一連のADC属性をADCスキーマとして公開することで実現されます。これらの属性は、デバイスパッケージの機能プロファイルにマッピングされます。クラウドオーケストレーター（Cisco Cloud CenterまたはWireless Application Protocol (WAP)）によってADCサービスをプロビジョニングする際に、これらの属性に値を提供できます。

次の図は、クラウドオーケストレーションソリューションにおけるNetScalerの概要を示しています。

Microsoft Azure Packを使用するクラウドオーケストレーターモードソリューションには、Azure PackからCisco APIC、Cisco APICからSystem Center Virtual Machine Manager (SCVMM)、Cisco APICからNetScalerなど、多くの統合ポイントが含まれます。プライベートクラウドのテナントとして、NATを有効にし、ネットワークサービスをプロビジョニングし、ロードバランサーを追加できます。

Azure Packはテナントポータルと管理者ポータルをサポートしており、それぞれが実行できる独自の操作セットを持っています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理者として、ACI登録、VIP範囲、仮想マシンクラウドとのNetScalerデバイス関連付け、テナントユーザーアカウント作成などの管理タスクを実行できます。
- テナントとして、Azure Packテナントポータルにログオンし、ネットワーク、ブリッジドメイン、Virtual Routing and Forwarding (VRF) を構成し、NetScalerのロードバランシング機能とRNAT機能を使用できます。

次の図は、クラウドモードソリューションにおけるAzure Packの概要を示しています。

重要

- クラウド管理者は、APICでサポートされているL4-L7スキーマを容易に利用でき、追加の変更はAPIC管理者がAPIC内で直接行うことができます。これにより、サポートされている機能セットと同等にNetScalerを構成および展開できます。
- テナントは、同じネットワークに対して、異なるポートを持つ複数のVIPアドレスを展開できます。IPとポートの組み合わせが一意であることを確認する必要があります。
- NetScalerデバイスパッケージは、シングルコンテキスト展開のみをサポートします。各テナントは専用のNetScalerインスタンスを取得します。
- ワイヤレスアプリケーションプロトコル (WAP) は、NetScaler MPXアプライアンスとNetScaler VPXアプライアンス (NetScaler SDXプラットフォームに展開されたNetScaler VPXインスタンスを含む) をサポートします。

クラウドオーケストレーターモードのデバイスパッケージは、フルマネージドモードとサービスマネージャーモードの両方をサポートします。フルマネージドモードパッケージは、シンプルな負荷分散、コンテンツスイッチング、SSLオフロード、その他のプロファイルなど、さまざまな機能プロファイルをサポートします。これらの機能プロファイルは、NetScalerの完全な機能セットと展開モードをカバーします。同様に、サービスマネージャーモードのデバイスパッケージは、APICを使用したNetScalerのワンアームおよびツーアーム構成と展開をサポートします。NetScaler Application Delivery Management (ADM) はAPICのサービスマネージャーとして機能し、NetScaler ADMを使用してNetScaler L4-L7パラメーターを構成できます。

注

サービスマネージャーモード (ハイブリッドモード) では、NetScalerアプライアンスにすでに存在する同じサーバーIPアドレスを再利用または再割り当てすることはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラウドオーケストレーターモードの機能プロファイルには、APICのADCスキーマにマッピングされた一連のパラメーターがあり、オーケストレーターはこれらのパラメーターを使用します。クラウドオーケストレーターは、ADCパラメーター (VIP、APICを介してNetScalerをプロビジョニングする際) の値を提供します。オーケストレーターはAPICのAPIと通信し、特定の機能プロファイルのペイロードの一部としてADC固有の詳細を渡します。内部的には、APICは値を抽出し、それらをデバイスパッケージに渡し、デバイスパッケージが内部でNetScalerを構成します。

Cisco APICでサポートされているADCスキーマの完全なリストの詳細については、Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x and earlierを参照してください。

フルマネージドモードのデバイスパッケージは、次の機能プロファイルをサポートします。

1. LB-HTTP-ワンアーム-プロファイルCM
2. LB-HTTP-ツーアーム-プロファイルCM
3. LB-HTTP-ツーアーム-サービスバックエンドプロファイルCM
4. CS-HTTP-LB-サービス-プロファイルCM
5. CS-SSL-LB-サービスプロファイルCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6ウェブインラインVサーバープロファイルCM

サービス管理モードのデバイスパッケージは、以下のクラウドモード機能プロファイルをサポートしています。

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScalerは上記の機能プロファイルをサポートしています。APICは、ADCスキーマ内のこれらのパラメータのサブセットをサポートしています。Cisco ACIでサポートされていない属性が機能プロファイルに存在する場合、クラウドオーケストレーターモードの機能プロファイルをクローンし、APICでサポートされていないすべての属性に値を提供して、その属性を保存する必要があります。その後、オーケストレーターは新しくクローンされた機能プロファイルを使用できます。

Citrix Cloud Mode Device PackageはNetScaler 12.0をサポートしており、サービスマネージャーモードもNetScaler ADM 12.0を使用しています。デバイスパッケージはモデルバージョンを1.0から2.0に変更しており、新規インストールとして使用できます。モデルバージョンが変更されたため、クラウドオーケストレーターモードのデバイスパッケージは以前のデバイスパッケージバージョンからアップグレードできません。

クラウドオーケストレーターモードのデバイスパッケージは、通常のデプロイメントでも使用できます。このパッケージは、ユーザーがNetScalerをクラウドオーケストレーター経由でプロビジョニングすることを義務付けません。このデバイスパッケージは、APIC単体、およびクラウドオーケストレーターと連携するAPICと互換性があります。

NetScaler® ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。ADC 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。ADC インスタンスは、クライアントから Kubernetes ク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スし、コンテンツルーティングできます。

注

- NetScaler ADM 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 ADM 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スします。

複数の ADC 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 ADM から Ingress を構成および展開することもできます。

ADM での Kubernetes 統合の次の側面を指定できます。

- **クラスター** – ADM 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 ADM 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 ADM 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 ADC 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADMに登録されているKubernetesクラスター。

シークレットトークンを使用してNetScaler ADMを構成し、Kubernetesクラスターを管理する

NetScaler ADMがKubernetesからイベントを受信できるようにするには、NetScaler ADM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、そのサービスアカウントにクラスター内で必要なRBAC権限を設定します。

1. NetScaler ADM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 ADM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 ADM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、`citrixadm-sa` サービスアカウントのトークンを表示するには、次のコマンドを実行します。

   ```
   kubectl describe sa citrixadm-sa
   ```

4. トークンのシークレット文字列を取得するには、次のコマンドを実行します。

   ```
   kubectl describe secret <token-name>
   ```

NetScaler ADM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 ADMにKubernetesクラスターを登録する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kubernetesクラスターを登録するには：

1. 管理者資格情報を使用してNetScaler ADM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. 「**クラスターの追加**」ページで、次のパラメータを指定します。

   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 ADM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 ADM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の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。

ビデオインサイト

ビデオインサイト機能は、NetScalerアプライアンスが顧客体験と運用効率を向上させるために使用するビデオ最適化技術のメトリックを監視するための、簡単でスケーラブルなソリューションを提供し、次のような利点をもたらします。

- ピーク時間帯の輻輳時にネットワークを管理します。
- ビデオ再生の一貫性を向上させ、ビデオのスタリングを減らします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 新しいビデオサービス提供 (例: Binge-onビデオサービス) を可能にします。
- 顧客が最適な持続可能なビデオ品質を選択できるようにします。
- 加入者向けに一貫したユーザーエクスペリエンスを提供します。

ビデオトラフィックを最適化する際、NetScalerアプライアンスは、ビデオビットレートを動的に調整する特別なメカニズムと、最適化技術による節約を推定するためのランダムサンプリング技術を使用します。NetScalerビデオ最適化機能の詳細については、「ビデオ最適化」を参照してください。NetScalerアプライアンスをNetScaler Application Delivery Management (ADM) と統合すると、NetScalerアプライアンスを流れるビデオデータから重要な情報が収集されます。この情報を使用して、ABRビデオトラフィックの最適化されたパフォーマンスと最適化されていないパフォーマンスを比較し、最適化による節約などを判断できます。

注

NetScaler ADMで提供される最適化されていないセッションの統計は、NetScalerアプライアンスでランダムサンプリング用に選択したセッションに対応します。ランダムサンプリングの詳細については、「ビデオ最適化」を参照してください。

NetScaler® ADMのビデオインサイトは、次の種類のビデオトラフィックのメトリックを提供します。

- HTTP経由のプログレッシブダウンロード (PD) ビデオ
- HTTP経由のABRビデオ
- HTTPS経由のABRビデオ
- QUIC経由のYouTube ABRビデオ

Video Insight の構成

注

Video Insight は、NetScaler Premium ライセンスを持つ NetScaler インスタンスでサポートされています。NetScaler Premium ライセンスは、NetScaler Telco プラットフォーム (VPX T1000 および VPX-T) でサポートされています。

NetScaler インスタンスで Video Insight を構成するには、まず AppFlow 機能を有効にし、AppFlow コレクター、アクション、およびポリシーを構成し、ポリシーをグローバルにバインド

© 1997–2026 Citrix Systems, Inc. All rights reserved.

します。コレクターを構成する際には、レポートを監視する NetScaler ADM サーバーの IP アドレスを指定する必要があります。

NetScaler インスタンスで Video Insight を構成するには、次のコマンドを実行して AppFlow プロファイルとポリシーを構成し、AppFlow ポリシーをグローバルにバインドします。

appflowコレクターを追加 \<name\> **-IPAddress** \<ipaddress\> **-port** \<port_number\> **-Transport** logstream

appflow®パラメーターを設定 -**videoInsight** ENABLED

AppFlowアクションを追加 \<name\> **-コレクター** \<string\> **-ビデオ分析** ENABLED

AppFlowポリシーを追加 \<name\> \<rule\> \<action\>

バインド appflow グローバル \<policyName\> \<priority\> \[\<gotoPriorityExpression\>\] \[**-type** \<type\>\]

イネーブル ns モード `ulfd`

機能を有効にする AppFlow

サンプル

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -Transport
logstream

set appflow param -videoInsight ENABLED

add appflow action act1 -collectors col1 -videoAnalytics ENABLED

add appflow policy appol true act1

bind appflow global appol 1

enable ns mode ulfd

enable feature appflow
```

NetScaler ADM で Video Insight メトリックを表示する

NetScaler ADM で Video Insight を有効にした後、ビデオ分類、データ量、ピークデータレート、ABR ビデオ再生などのビデオ最適化メトリックを表示できます。これらのメトリックは、ネット

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ワークを分析し、加入者のエクスペリエンス、運用効率、およびその他のパフォーマンス基準を向上させるためにビデオを最適化するのに役立ちます。

NetScaler ADMでVideo Insightメトリクスを表示するには：

1. Webブラウザで、NetScaler ADM仮想アプライアンスの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。
3. **Analytics \> Video Insight**に移動します。

注

グラフの凡例**OTHER**で提供される値は、選択したフィルターに応じて、ビデオトラフィック内の非ABRデータと非PDデータを表します。

- **すべて** – ビデオトラフィック内の非ABR（HTTP、HTTPS、QUIC）データと非PD（HTTP）データの合計。
- **HTTP** – ビデオトラフィック内の非ABRデータと非PDデータの合計。
- **HTTPS** – ビデオトラフィック内の非ABRビデオデータの合計。
- **QUIC** – ビデオトラフィック内の非ABRビデオデータの合計。

ネットワーク効率を表示

指定された期間について、NetScaler® Application Delivery Management (ADM) は、その期間における最適化されたビデオセッションと最適化されていないビデオセッションの比率を示すグラフを提供します。また、最適化によって節約された帯域幅の割合も表示します。節約された帯域幅の割合は、次の式で計算されます。

帯域幅の節約率 = 最適化されたABRビデオデータ量の平均 / 最適化されていないABRビデオデータ量の平均。

最適化によって節約された帯域幅の割合を表示するには：

1. **Analytics \> Video Insight** に移動し、**ABR Video** をクリックします。
2. 右側のペインで、リストから期間を選択します。期間スライダーを使用して、期間をさらにカスタマイズできます。
3. **Go** をクリックし、**Network Efficiency** タブを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最適化されたABRビデオと最適化されていないABRビデオが使用するデータ量を比較する

指定された期間について、NetScaler® Application Delivery Management (ADM) は、最適化されたABRビデオと最適化されていないABRビデオが使用するデータ量を表示し、両方のデータ量を比較できるようにします。

ABRビデオが使用するデータ量を確認するには：

1. **Analytics \> Video Insight** に移動し、**ABR Video** をクリックします。
2. 右側のペインで、リストから期間を選択します。期間スライダーを使用して、期間をさらにカスタマイズできます。
3. **Go** をクリックし、**Data Volume** タブを選択します。

Filters リストを使用して、HTTP、HTTPS、またはQUIC ABRビデオを選択できます。

フィルター(/en-us/netscaler-application-delivery-management-software/media/video_insight15.png)

Data Volume タブには、ABRビデオが使用する平均データ量、および選択した期間にネットワークから最適化されたABRビデオと最適化されていないABRビデオによって消費されたデータ量を説明する折れ線グラフと円グラフが表示されます。折れ線グラフにマウスポインターを合わせると、特定の期間に使用された平均データ量を確認できます。

データ量(/en-us/netscaler-application-delivery-management-software/media/videoinsight16.png)

ネットワークからストリーミングされたビデオの種類と消費されたデータ量を表示する

NetScalerアプライアンスは、ネットワーク内の暗号化または非暗号化されたビデオトラフィックと、ビデオストリーミングの種類（PDまたはABR）を検出します。NetScaler Application Delivery Management (ADM) は、これらのメトリックと、定義された期間にビデオトラフィックによって消費されたデータ量を表示します。

ビデオの種類と消費されたデータ量を確認するには：

1. **Analytics \> Video Insight** に移動し、**Video Classification** をクリックします。
2. 右側のペインで、リストから期間を選択します。期間スライダーを使用して、期間をさらにカスタマイズできます。
3. **Go** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Filters リストを使用して、HTTP、HTTPS、またはQUICトラフィックを選択できます。

フィルター(/en-us/netscaler-application-delivery-management-software/media/video_insight2.png)

Data Volume タブには、ネットワークからストリーミングされているビデオトラフィックの種類と、ネットワークによって消費されたデータ量を示す折れ線グラフと円グラフが表示されます。折れ線グラフにマウスポインターを合わせると、特定の期間に消費されたデータ量を確認できます。

データ量(/en-us/netscaler-application-delivery-management-software/media/video_insight3.png)

また、円グラフにマウスポインターを合わせると、特定の種類のビデオトラフィックによって消費されたデータ量の割合を確認できます。

ビデオトラフィックの種類(/en-us/netscaler-application-delivery-management-software/media/video_insight4.png)

ABRビデオの最適化された再生時間と最適化されていない再生時間を比較する

指定された期間について、NetScaler® Application Delivery Management (ADM) はABRビデオの再生時間を提供し、ネットワーク内の最適化されたABRビデオと最適化されていないABRビデオの再生時間を比較することもできます。

再生時間を表示するには：

1. **Analytics \> Video Insight** に移動し、**ABR Video** をクリックします。
2. 右側のペインで、リストから期間を選択します。期間スライダーを使用して、期間をさらにカスタマイズできます。
3. **Go** をクリックし、**Play Time** タブを選択します。

   Filters リストを使用して、HTTP、HTTPS、またはQUIC ABRビデオを選択できます。

   フィルター(/en-us/netscaler-application-delivery-management-software/media/video_insight11.png)

選択した期間について、**Play Time** タブには、以下を説明する折れ線グラフと円グラフが表示されます。

- ネットワークからのABRビデオの総再生時間
- 選択した期間における、ネットワークからのABRビデオの最適化された再生と最適化されていない再生の総再生時間

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 暗号化されたABRビデオと暗号化されていないABRビデオの総再生時間
- ABRビデオの平均再生時間
- ABRビデオの最適化された再生と最適化されていない再生の平均再生時間
- 暗号化されたABRビデオと暗号化されていないABRビデオの平均再生時間
- 最適化されたABRビデオと最適化されていないABRビデオ間の再生時間の分布

最適化されたABRビデオと最適化されていないABRビデオの帯域幅消費量を比較する

指定された期間について、NetScaler® Application Delivery Management (ADM) は、最適化されたABRビデオと最適化されていないABRビデオによって消費された帯域幅を提供し、さらに、ネットワーク内の最適化されたABRビデオと最適化されていないABRビデオによって消費された帯域幅を、以下に基づいて比較できるようにします。

- 再生時間
- データ量

帯域幅の消費量を表示するには：

1. **Analytics \> Video Insight** に移動し、**ABR Video Analytics** をクリックします。
2. 右ペインで、リストから期間を選択します。期間スライダーを使用して、期間をさらにカスタマイズできます。
3. **Go** をクリックし、**Bandwidth** タブを選択します。

   Filters リストを使用して、HTTP、HTTPS、またはQUICのABRビデオを選択できます。

選択した期間について、**Bandwidth** タブには、以下を説明する折れ線グラフと円グラフが表示されます。

- 最適化されたABRビデオと最適化されていないABRビデオによって消費された平均帯域幅。
- 最適化されたABRビデオと最適化されていないABRビデオ間の再生時間分布に基づいて消費された帯域幅。
- 最適化されたABRビデオと最適化されていないABRビデオ間のデータ量分布に基づいて消費された帯域幅。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ABRビデオの最適化された再生回数と最適化されていない再生回数を比較する

指定された期間について、NetScaler® Application Delivery Management (ADM) はABRビデオの再生回数を表示し、ネットワーク内の最適化された再生回数と最適化されていない再生回数を比較できるようにします。

再生回数を確認するには：

1. **Analytics \> Video Insight** に移動し、**ABR Video Analytics** をクリックします。
2. 右ペインで、リストから期間を選択します。期間スライダーを使用して、期間をさらにカスタマイズできます。
3. **Go** をクリックし、**# of Plays** タブを選択します。

   Filters リストを使用して、HTTP、HTTPS、またはQUIC ABRビデオを選択できます。

# of Plays タブには、選択した期間におけるネットワークからのABRビデオの再生回数、およびネットワークからの最適化されたABRビデオと最適化されていないABRビデオの再生回数を説明する折れ線グラフと円グラフが表示されます。折れ線グラフにマウスポインターを合わせると、特定の期間の再生回数を表示できます。

また、円グラフにマウスポインターを合わせると、選択した期間における最適化された再生回数と最適化されていない再生回数の割合、および暗号化されたABRビデオと暗号化されていないABRビデオの割合を表示できます。

特定の時間枠のピークデータレートを表示する

NetScaler® Application Delivery Management (ADM) は、ネットワーク内のビデオトラフィックのピークスループットまたはデータレートを表示します。

ビデオトラフィックのピークデータレートを表示するには：

1. **Analytics \> Video Insight** に移動し、**Video Classification** をクリックします。
2. 右側のペインで、リストから時間枠を選択します。時間枠スライダーを使用して、時間枠をさらにカスタマイズできます。
3. **Go** をクリックし、**Peak Data Rate** タブを選択します。

Filters リストを使用して、HTTP、HTTPS、または QUIC トラフィックを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Peak Data Rate** タブには、ネットワークからストリーミングされるビデオトラフィックの種類のピークデータレートと、選択した時間枠におけるネットワーク上のビデオトラフィックのピークデータレートを説明する折れ線グラフと円グラフが表示されます。折れ線グラフにマウスポインターを合わせると、特定の時間枠におけるピークデータレートが表示されます。

- また、円グラフにマウスポインターを合わせると、選択した時間枠中にストリーミングされたビデオトラフィックの種類によって消費されたピークデータレートの割合が表示されます。

-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IPアドレス管理 (IPAM) の構成

ADM IPAMは、ADM管理対象構成でIPアドレスを自動割り当ておよび解放する機能を提供します。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アドレスを割り当てることができます。

- ADM組み込みIPAMプロバイダー。
- Infoblox IPAMソリューション。詳細については、「Infoblox DDI」を参照してください。

現在、ADM 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。
- **Kubernetes Ingress**: Kubernetesクラスター内のIngress構成に仮想IPアドレスを自動割り当てします。

ADMによって管理されている各ネットワークまたはIP範囲で、割り当て済みおよび利用可能な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

ADM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。ADMに外部IPプロバイダーソリューションを追加する場合は、次の手順を実行します。

1. **インフラストラクチャ > IPAM** に移動します。
2. **プロバイダー**で、**追加**をクリックします。
3. IP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** - ADM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IPアドレスベンダーを選択します。
    - **URL** - ADM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。
    - **User Name** - 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。
    - **Password** - 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. **追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワークを追加する

ADM管理構成でIPAMを使用するためにネットワークを追加します。

1. **インフラストラクチャ > IPAM**に移動します。
2. **ネットワーク**で、**追加**をクリックします。
3. 次の詳細を指定します。

   - **Network Name** - ADM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、ADM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範囲**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

     ADM IPAMはIPv4アドレスのみをサポートします。

     IP範囲の場合、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、ネットワーク値を次の形式で指定します。

     ```
     <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. **Infrastructure > IPAM**に移動します。
2. **Networks**タブで、**View All Allocated IPs**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アドレスを予約するADMモジュールを表示します。たとえば、IPアドレスがStyleBooksによって予約されている場合、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を表示します。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。
   - **リソースID**: リンク付きのリソースIDを表示します。このリンクをクリックすると、IPアドレスを使用す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、リソースIDは構成パックIDとして表示されます。

注

IPアドレスを解放したい場合は、解放したい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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インフラストラクチャの管理と監視にADM監査ログを使用する

NetScaler® ADMサービスを使用して、ADM上のすべてのイベントと、ADM管理のADC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。ただし、ログメッセージは確認して初めて優れた情報源となり、ADMはログメッセージの確認方法を簡素化します。

フィルタを使用して、ADM syslogおよび監査ログメッセージを検索できます。フィルタは、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。

ADM GUIから、次の種類のログメッセージを確認できます。

- ADCインスタンス関連の監査ログ
- ADM関連の監査ログ
- アプリケーション監査ログ

ADCインスタンス関連の監査ログ

ADMからADCインスタンス関連のsyslogメッセージを表示する前に、NetScaler ADM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ADMにリダイレクトされます。

ADMサービスをsyslogサーバーとして構成する

ADM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. ADM GUIから、**Infrastructure > Instances**に移動します。
2. syslogメッセージを収集してNetScaler ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

ADMでsyslogを構成する(/en-us/netscaler-application-delivery-management-software/media/configure-syslog-adm-citrix.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 ADMはsyslogメッセージの受信を開始します。メッセージを表示するには、「**Infrastructure > Events > Syslog Messages**」に移動します。「**Need Help?**」をクリックして、組み込みの検索ヘルプを開きます。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。

ADM上のsyslogメッセージ(/en-us/netscaler-application-delivery-management-software/media/adm-syslog-messages-citrix.png)

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。

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。

ADM関連の監査ログ

事前設定されたルールに基づいて、ADMはすべての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。ADM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、「**Settings > ADM Audit Log Messages**」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ADM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。

- ADM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、「**Infrastructure > Network Functions > Auditing**」に移動します。
- ADM内の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、「**Applications > Dashboard**」に移動し、仮想サーバーをクリックして「**Audit Log**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスライセンスの管理

NetScaler ADMを使用すると、NetScalerインスタンスのライセンスを管理および割り当てることができます。以下のトピックは、インスタンスライセンスの管理に役立ちます。

- NetScalerプール容量
- 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

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。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: 9月上旬からLASをサポートします。

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ご利用いただけない場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。
NetScalerプール型キャパシティを使用すると、異なるADC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った場合、割り当てられたキャパシティは共通プールに戻されます。解放されたキャパシティは、リソースを必要とする他のADC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、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。実行時にトラフィックに影響を与えることなく、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。

- NetScalerインスタンス。これは次のように分類できます。
  - ゼロキャパシティハードウェア
  - スタンドアロンVPXインスタンス、CPXインスタンス、または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 ADM

ゼロキャパシティハードウェア

NetScalerのプールされた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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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された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。異なる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方法で機能します。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。

ADC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、ADCプールされたキャパシティをサポートしています。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ているプールされたキャパシティ**を参照してください。

スタンドアロンNetScaler VPXインスタンス

以下のハイパーバイザーで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、プールされたキャパシティをサポートします:

- 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

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、プールされたキャパシティをサポートします:

- マイクロソフト ハイパーV
- AWS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- マイクロソフト アジュール
- グーグル クラウド

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、プールされたキャパシティをサポートします:

- 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 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 ADM 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 ADM 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、VPX にはプラットフォームライセンスは不要です。トラフィックを処理するには、帯域幅とインスタンスライセンスをプールからチェックアウトする必要があります。

スタンドアロンの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、CPX にはプラットフォームライセンスは不要です。最大 1 Gbps のスループットを消費する単一の CPX インスタンスは、ライセンスプールから 1 つの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 CPX インスタンスがあるとします。いずれかの CPX インスタンスが 500 Mbps のスループットを消費した場合でも、残りの 19 個の CPX インスタンスに対して帯域幅プールは 20 Gbps のままです。

同じ 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 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スタンドアロンの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不要です。トラフィックを処理するには、NetScaler BLX インスタンスは帯域幅とインスタンスライセンスをプールから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、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。

インスタンスプール

インスタンスプールは、NetScaler のプールされたキャパシティを通じて管理できる VPX インスタンス、CPX インスタンス、または BLX インスタンスの数、あるいは SDX-Z インスタンス内の 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、CPX、および 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 ADMライセンスサーバー

NetScalerプール型キャパシティは、ライセンスサーバーとして構成されたNetScaler ADM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プール型キャパシティライセンスを管理します。NetScaler ADMソフトウェアを使用すると、ADMライセンスなしでプール型キャパシティ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場合、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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。チェックアウトはすべて、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、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。

表1。MPXおよびSDXインスタンス用のサポートされているプール型キャパシティ

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	帯域幅の最小単位
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bps
MPX 8900Z FIPS	33	5	NA	NA	1 ギガbps
MPX 14000Z シリーズ	100	20	NA	NA	1 ギガbps
MPX 14000Z 40G シリーズ	100	20	N/A	N/A	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	帯域幅の最小単位
MPX 14000Z FIPS シリーズ	100	20	N/A	N/A	1 ギガbps
MPX 14000Z 40S シリーズ	100	20	N/A	N/A	1 ギガビット/秒
MPX 15000Z シリーズ	120	20	N/A	N/A	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
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 ギガビット/秒
MPX 25000ZA	200	100	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	帯域幅の最小単位
MPX 26000Z シリーズ	200	100	N/A	N/A	1 ギガビット/秒
MPX 26000Z 100G シリーズ	200	100	N/A	N/A	1 ギガビーピーエス
MPX 26000Z 50S シリーズ	200	100	N/A	N/A	1 ギガビーピーエス
SDX 8900Z	30	10	2	7	1ギガビット/秒
SDX 9100Z	95	20	4	7	1ギガビット/秒
SDX 14000Z シリーズ	100	10	2	25	1ギガビット/秒
SDX 14000Z 40G シリーズ	100	10	2	25	1 ギガビット/秒
SDX 14000Z 40S シリーズ	100	20	10	25	1 ギガビット/秒
SDX 14000Z FIPS シリーズ	100	10	2	25	1 ギガビット/秒
SDX 15000Z 50G	120	10	2 (注: 13.0 47.x より前のバージョ	55	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	帯域幅の最小単位
			ンでは5インスタンス)		
SDX 15000Z	120	10	2 注: 13.0 47.x より前のバージョンでは5インスタンス)	55	1 ギガビット/秒
SDX 16000Z シリーズ	200	15	10	55	1 ギガビット/秒
SDX 22000Z シリーズ	120	20	20	80	1 ギガビット/秒
SDX 25000Z 40G	200	50	10	115	1 ギガビーピーエス
SDX 25000ZA	200	50	10	115	1 ギガビーピーエス
SDX 26000Z 100G	200	50	10	115	1 ギガビーピーエス
SDX 26000Z	200	50	10	115	1ギガbps
SDX 26000Z 50S	200	50	10	115	1ギガbps
SDX 24000Z シリーズ	150	50	10	80	1 ギガビット/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 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VPXインスタンスでサポートされるプール容量

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
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

注記

最小購入数量は、最小システム要件とは異なります。

表4. BLXインスタンス向けに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	帯域幅とエディションの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	必要なライセンス	-
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
CPX	-	-	ライセンスが必要
BLX	-	ライセンスが必要	必要なライセンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler プールキャパシティの構成

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。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。

必要なNetScaler®の最小バージョンはLAS互換です:

- 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: 9月上旬からLASをサポートします。

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。
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お客様に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。
ADCプールキャパシティを使用するには、必要なADCインスタンスのライセンスサーバーとしてNetScaler ADMを構成します。ADCインスタンスはADM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。ADM GUIで次のタスクを実行できます:

- プールキャパシティライセンスファイル (帯域幅と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必要に応じてNetScalerインスタンスにライセンスを割り当てます。
- インスタンスの最小および最大キャパシティに基づいて、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler FIPSインスタンスのプールキャパシティを構成して、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.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

プールされた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。

ADCプール容量の状態

プールされた容量の状態は、ADCインスタンスのライセンス要件を示します。プールされた容量で構成されたADC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実行されています。
- **容量不一致**: 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実行されています。
- **猶予**: インスタンスは猶予ライセンスで実行されています。
- **猶予と不一致**: インスタンスは猶予期間で実行されていますが、ユーザーが構成した容量よりも少ない容量で実行されています。
- **利用不可**: インスタンスが管理のためにADMに登録されていないか、ADM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 - ADMでライセンスを適用する

1. NetScaler ADMで、**インフラストラクチャ > プールライセンス**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する**。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、ADM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**」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、「**Get Licenses**」を選択します。その後、「**Finish**」を選択します。

    「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

」

いつでも、「**License Settings**」からADMにライセンスを追加できます。

3. 「**Finish**」をクリックします。

   ライセンスファイルがADMに追加されます。「**License Expiry Information**」タブには、ADM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. 「**License Files**」で、適用するライセンスファイルを選択し、「**Apply licenses**」をクリックします。

   このアクションにより、ADC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。

   NetScaler ADMにプールされたライセンスを適用する方法の詳細については、関連ビデオこちらをクリックを参照してください。

ステップ2 - NetScaler ADMをライセンスサーバーとして登録する

ADM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
- CLIを使用

GUIを使用してADMをライセンスサーバーとして登録する

ADC GUIで、ADM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、リストからリモートライセンスモードを選択します。
5. 「**Server Name/IP address**」フィールドに、ADMサーバーのIPアドレスを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、「高可用性展開の構成」を参照してください。

スタンドアロンADMまたはエージェントを使用する展開については、「ライセンスの概要」を参照してください。

6. 「**Register with NetScaler ADM**」を選択します。
7. インスタンスをNetScaler ADMに登録するためにADMの資格情報を入力し、「**Continue**」をクリックします。

8. 「**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。

初めての場合は、NetScalerでライセンスを割り当てます。後でADM 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. 「**Get Licenses**」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。構成の変更は、インスタンスを再起動するまで有効になりません。

CLIを使用してADMをライセンスサーバーとして追加する

ADC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ADMサーバーをライセンスサーバーとして追加します。

1. ADCコンソールにログインします。
2. ADM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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このコマンドは、ライセンスサーバーを追加する際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：

指定されたライセンスモードが`Pooled`の場合、出力にはプールされたキャパシティ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**のいずれかです。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステップ 3 - プールされたライセンスをADCインスタンスに割り当てる

ADM 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 ADM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 > プールされた容量**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ADMにアップロードした場合にのみ表示されます。
3. 管理するライセンスプールをクリックします。

   注

   「**割り当て済み容量**」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、ADCのウォームリスタート後に有効になります。

   「**割り当ての詳細**」では、インスタンスの帯域幅割り当てを変更すると、「**要求済み**」フィールドと「**適用済み**」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ADCインスタンスを選択します。

   「**ライセンスステータス**」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:

   「**管理対象外インスタンス**」タブには、NetScaler ADMで検出されたが管理されていないインスタンスが表示されます。
5. 「**割り当ての変更**」または「**割り当ての解放**」をクリックして、ライセンス割り当てを変更します。
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. 「**割り当て**」リストオプションを設定して、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、「**割り当て**」をクリックします。
8. 「**ライセンス割り当ての変更**」ウィンドウ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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

-

注

ライセンスエディションを変更する場合は、インスタンスをウォームリスタートしてください。

帯域幅の割り当てを変更する方法の詳細については、関連ビデオのこちらを参照してください。

ADC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ADC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がライセンスサーバーに接続するには、プラットフォームライセンスが必要です。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、プールされたキャパシティ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。

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。再起動が必要となるのは、ライセンスエディションを変更する場合のみです。

注記:

インスタンスを再起動すると、設定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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。ADC 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。

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。再起動が必要となるのは、ライセンスエディションを変更する場合のみです。

注記:

インスタンスを再起動すると、設定されたプール容量ライセンスがADM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、ADM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。詳しくは、「ADM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ADC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。

ペア内の各ノードにプールライセンスを割り当てるには、「ADC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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ADMサーバーをプール型ライセンスサーバーとしてのみ構成する

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。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: 9月上旬からLASをサポートします。

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。
管理者は、ADMサーバーをプール型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、ADMサーバーはADCインスタンスからライセンスデータのみを受信します。

場合によっては、規制区域からADC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かもしれません。そのような状況では、管理、監視、分析機能を使用するために、規制区域にADMオンプレミスサーバーのローカルインスタンスを展開できます。プール型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ADMライセンスサーバー間でプー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ル型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ADCインスタンス全体にプール型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、ADMサーバーをプール型ライセンスサーバーとしてのみ構成してください。ADMサーバーはすべてのADC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ADCインスタンス全体にプール型キャパシティライセンス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、ADMサーバーをプール型ライセンスサーバーとしてのみ構成する方法について説明します。

ADMサーバーをプール型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、ADMサーバーにADC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、ADCインスタンスを追加してください。

プールされたライセンスサーバー専用のADMサーバーを構成するには、次の手順を実行します。

1. **設定 > 管理**に移動します。
2. **システム構成**セクションで、**システム展開**を選択します。
3. **ADM展開**で、**ADMのみをプールライセンスサーバーとして使用**を選択します。

   NetScaler ADMのみをライセンスサーバーとして使用(/en-us/netscaler-application-delivery-management-software/media/adm-only-as-a-license-server.png)
4. **OK**をクリックします。

   このアクションにより、プールされたライセンス機能のみが保持され、次のADM機能が無効になります。

   - ADMバックアップ
   - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

既定では、ADMアナリティクス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、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。

ADM GUIには、プールされたライセンス機能のみが表示されるようになりました。残りの機能は表示されません。

5. ライセンス機能のみにADMを設定した後、**インフラストラクチャ > インスタンス**ページでADCインスタンスを追加します。

注

- 1つ以上のADMサーバーにADCインスタンスを追加できます。そのようなADC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ているすべてのADMサーバーでパスワードを更新してください。
- ユーザーは、ADM 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ADC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の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 ADMでアクセスポリシーを構成する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX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。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: 9月上旬からLASをサポートします。

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、ADCプール容量ライセンスにアップグレードできます。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ADCインスタンスに対して、プール容量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インスタンスにプール容量ライセンスを構成する方法については、「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」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

VPXインスタンスをバージョン12.0.56.xにアップグレードしていることを確認してください。

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、`<http://192.168.100.1>`などのVPXインスタンスのIPアドレスを入力します。
2. 「**ユーザー名**」と「**パスワード**」フィールドに、管理者認証情報を入力します。
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を使用**」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. 「**NetScaler ADM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、インスタンスのプールライセンスをADM経由で管理したい場合は、NetScaler ADM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。

   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、アプライアンスを再起動するには**Reboot**をクリックします。

   ADCインスタンスを再起動する(/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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

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、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**フィールドと**Password**フィールドに、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. 「**NetScaler ADM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 ADM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、ADM資格情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

      「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。

      「インスタンスのウォーム再起動」(/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、**再起動**をクリックしてアプライアンスを再起動します。新しいライセンスでアプライアンスが稼働した後、`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ペアのプライマリおよび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ていることを確認するには、プライマリおよび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. **ようこそ**ページで、**続行**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 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。**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。

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、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: 9月上旬からLASをサポートします。

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 MPXアプライアンスは、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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インスタンスに対してNetScaler Pooled Capacityライセンスを構成するには、「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関し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アプライアンスをNetScaler Pooled Capacity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 Pooled Capacity にアップグレードするには:

1. 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. **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. **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（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。
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。

   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 ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

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. インスタンスのプールライセンスをNetScaler ADM経由で管理する場合は、「**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て、ADM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。

       「ライセンスの割り当て」(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-6.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。

       「ライセンスの取得」(/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アプライアンスが再起動したら、NetScaler MPXアプライアンスにログオンします。「**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler MPX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ADC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アプライアンスを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、`<http://192.168.100.1>` のようにアプライアンスのIPアドレスを入力します。
2. **ユーザー名**および**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. **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。

   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求められます。
7. アプライアンスを再起動するには、「**再起動**」をクリックします。
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 Pooled Capacityにアップグレードするには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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アプライアンスのIPアドレス（`<http://192.168.100.1>`など）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. 「**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。

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。

   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 ADM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、ADM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。

   b. **Allocate**メニューからNetScalerアプライアンスに帯域幅を割り当て、**Get Licenses**をクリックします。

   c. 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起動して実行されたら、`force ha failover`と入力してフェイルオーバーを強制します。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。

6. 既存のプライマリNetScaler MPXアプライアンスにログオンし、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、`<http://192.168.100.1>`のようにNetScalerアプライアンスのIPアドレスを入力します。
   b. **User Name**フィールドと**Password**フィールドに、管理者資格情報を入力します。
   c. **Welcome**ページで、**Continue**をクリックします。
   d. **Configuration**タブで、**System**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. **System**ページで、**Reboot**をクリックします。

f. **Reboot**ページで、**Warm reboot**を選択し、**OK**をクリックします。

プライマリNetScaler MPXアプライアンスが再起動すると、HAペアのセカンダリNetScaler MPXアプライアンスになります。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ペア構成に変更する場合は、フェイルオーバーを強制します。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
```

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。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 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、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。

- 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: 9月上旬からLASをサポートします。

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なしで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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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には適用されません。
永続ライセンスを持つNetScaler SDXアプライアンスは、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、ADC Pooled Capacity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、一方通行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。

- SDXアプライアンスを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。
- ADMでADC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。
- 現在のライセンスに影響がないことを確認するため、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と同じ数を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、SDXアプライアンスの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. **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。その後、**完了**をクリックします。

   ライセンスファイルのアップロード(/en-us/netscaler-application-delivery-management-software/media/upload-licenses.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

> **注**
>
> 古いライセンスファイルを削除するためにSDXアプライアンスを再起動する必要はないため、ダウンタイムはありません。詳細については、NetScalerサポートチーム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、以下を実行します。

   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。

      - ADMサーバーをライセンスサーバーとして構成する場合は、ADMサーバーのIPアドレスを指定します。
      - ADMサーバーと通信するためにエージェントを使用している場合は、ADMエージェントの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。

      - ADMサーバーの場合は、管理者資格情報を入力します。
      - ADM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。

   ライセンスサーバーの詳細を入力します(/en-us/netscaler-application-delivery-management-software/media/pooled-license-section.png)

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。

   SDXに割り当てられたライセンス(/en-us/netscaler-application-delivery-management-software/media/license-server-configured.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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アプライアンスを再起動する必要はありません。

クラスターモードのNetScalerインスタンスにおけるNetScaler pooled capacity

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。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。

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: 9月上旬からLASをサポートします。

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なしの状態になります。
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラスターとして構成されたNetScalerインスタンスでNetScaler pooled capacityを構成できます。クラスターモードのNetScalerインスタンスでpooled capacityを構成するための前提条件は次のとおりです。

- クラスターを形成するために、インスタンスは個別にプール型キャパシティ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。
- すべてのインスタンスは、同じNetScaler Application Delivery Management (ADM)からプール型キャパシティをチェックアウトしました。
- 新しいインスタンスは、そのキャパシティとNetScaler ADM構成がクラスター内の既存インスタンスのものと同じでない限り、既存のNetScalerクラスターに追加することはできません。

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。

ADCクラスターにADC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以下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**および**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. **構成**タブで、**システム \> ライセンス \> ライセンスの管理**に移動し、**新しいライセンスの追加**をクリックして、**プールライセンスの使用**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名前またはアドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. NetScaler ADM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NetScaler ADMに登録**チェックボックスをオンにし、ADM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、**ライセンスの取得**をクリックします。

7. **割り当ての変更**または**割り当ての解放**を選択して、ライセンスの割り当てを変更または解放できます。

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がポップアップウィンドウに表示されます。

> **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、必要なライセンスエディションと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 ADC プール容量を ADC クラスターに割り当てる

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。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\[S/E/P\]\[Bandwidth\]
```

ヘルスモニタリング

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。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: 9月上旬からLASをサポートします。

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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われます。
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。
ライセンスサーバーは、NetScalerのプール容量が有効なインスタンスの健全性を継続的に監視します。インスタンスは定期的なメッセージを通じてライセンスサーバーと通信します。連続するいくつかのメッセージが受信されない場合、ライセンスサーバーは接続が失われたことを報告します。

デフォルトのアラームを補完するために、カスタム通知を作成できます。

猶予期間

NetScalerのプール容量が有効な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、インスタンスは現在の容量で30日間動作を継続します。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、インスタンスはその容量を失い、トラフィックの処理を停止します。

通知とアラーム

インスタンスで実行されるすべてのアクションに対して、NetScaler Application Delivery Management (ADM) から通知を有効にできます。カスタム通知設定とは別に、一部のアラームはデフォルトで構成されています。例: 容量の一定の割合を使い果たしたプールを補充するためのアラームを構成するには、**Infrastructure > Pooled Licensing** に移動し、**Notification Settings** の下にある編集アイコンをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

問題発生時の予期される動作

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: 9月上旬からLASをサポートします。

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。
以下は、説明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

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日間動作を継続します。30日経過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。

ライセンスサーバーが応答を停止すると、接続が復元されるまでNetScalerインスタンスは猶予期間に入ります。

NetScalerプール容量対応インスタンスが応答を停止する

NetScalerプール容量対応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NetScalerインスタンスのすべて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プール容量対応インスタンスの両方が応答を停止する

ライセンスサーバーとNetScalerプール容量対応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、NetScalerプール容量対応インスタンスは再起動が完了した後に自動的にライセンスをチェックアウトします。

NetScalerプール容量対応インスタンスが正常にシャットダウンする

正常なシャットダウン中に、ライセンスをチェックインするか、正常な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プール容量対応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 Application Delivery Management (ADM) プールライセンスのインベントリをチェックし、利用可能な容量をチェックアウトします。NetScalerが構成どおりの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、プール容量対応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.

ネットワーク接続が失われる

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プール容量対応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、インスタンスは現在の容量で30日間動作し続けます。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、インスタンスはその容量を失い、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。

プール型キャパシティライセンスの有効期限チェックを設定する

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、LASはNetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、NetScaler Fixed term Bandwidth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: 9月上旬からLASをサポートします。

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なしで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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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ご利用いただけ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。
NetScalerプール型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。しきい値を設定することで、NetScaler Application Delivery Management (ADM) は、ライセンスの有効期限が近づくと、電子メールまたはSMSで通知を送信します。ライセンスがNetScaler ADM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 ADMで表示できます。

ライセンス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** ページで、**License Expiry Information** セクションの下に、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。
   - **数**: 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が切れるまでの日数。
3. **通知設定**セクションで、**編集**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された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. **メールプロファイル**: 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プロファイル**: 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が切れるまでの日数で、通知を送信するタイミングを指定します。
6. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

プールに新しいライセンスを追加すると、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。

NetScaler VPXおよび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製品アクティベーションを行う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: 9月上旬からLASをサポートします。

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、これらの要件への不遵守に対して、法律または衡平法に基づきCitrixが有する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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Application Delivery Management (ADM) からオンデマンドでVPXおよび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。ADM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 ADM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、インスタンスはそのライセンスをNetScaler ADMソフトウェアにチェックインします。

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ること。例: NSVPX-ESX-12.0-xx.xx_nc.zip
- バージョン12.0を実行しているNetScaler ADMをインストールしていること。例: MAS-ESX-12.0-xx.xx.zip

注

NetScaler ADMで既存のVPXライセンスを管理するには、ライセンスをNetScaler ADMに再ホストする必要があります。

NetScaler ADM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 ADM仮想アプライアンスを再起動してください。

NetScaler ADM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 ADM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。
3. **インフラストラクチャ > プールライセンス**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 ADMにアップロードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスファイルを追加するには、**参照**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。その後、**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され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 ADMにライセンスを追加できます。

検証

NetScaler ADM 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 ADM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. タブで、**Infrastructure > Pooled Licensing > VPX Licenses**に移動します。

4. 割り当て済みのライセンスは、利用可能なライセンスセクションの下のテーブルで表示できます。

NetScaler GUIを使用して、VPXおよびBLXライセンスをADC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. 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. **Server Name/IP Address**フィールドに、ライセンスサーバーの詳細を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 上記画面の**Username**と**Password**フィールドに、NetScaler ADMの資格情報を入力し、**Continue**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、**Get Licenses** をクリックします。

7. **Reboot** をクリックすると、NetScaler インスタンスが再起動します。
8. **System** \> **Licenses** \> **Manage Licenses** に移動し、**Change allocation** または **Release allocation** を選択することで、ライセンス割り当てを変更または解放できます。

9. **Change allocation** 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、**Get Licenses** をクリックします。

NetScaler CLI を使用して ADC インスタンスに VPX および 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。

```
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 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\[S/E/P\]\[Bandwidth\]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APIを使用してADCインスタンスにVPXおよびBLXライセンスを割り当てる

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 ADM IP\>”, “port”:”27000”}}\\r\\n
```

NetScaler ADM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で利用可能なライセンスを表示するには:

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 ADM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アプライアンス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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

{“nscapacity:{“platform”:”VE8000”}}\\r\\n
```

NetScaler ADMは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

VPXおよびBLXインスタンスのライセンスサーバーIPアドレスを、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。

CLIを使用した更新: 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を使用した更新: 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。詳細については、「NetScaler GUIを使用してADCインスタンスにVPXおよび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ことで、ライセンスの有効期限が近づくと、NetScaler ADMは電子メールまたはSMSで通知を送信します。ライセンスがNetScaler ADM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 ADMで表示できます。

ライセンスの有効期限チェックを構成するには：

1. **>** の順に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ページの 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。
   - **機能**: 有効期限が近づいてい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までの日数。
3. セクションで、 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された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. **メールプロファイル**: 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プロファイル**: 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、通知を送信するタイミングを指定します。
6. をクリックします。

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）、レガシー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: 9月上旬からLASをサポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pooled vCPU、CICO、perpetualなどの他のすべてのレガシー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:

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、スケーラビリティを向上させる新しいテクノロジーに移行しています。最新のデータセンターアーキテクチャには、少なくとも次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かつアジャイルである必要があります。ライセンスも、使用状況を完全に可視化できる一元的な管理ツールによって管理されることが期待されます。

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、帯域幅要件は少ないかもしれませんが、SSL TPS、圧縮スループットなどの他の L7 パフォーマンスに対する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 負荷の高い処理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM 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。

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 ADM 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があります。そのような場合は、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. **続行**をクリックします。

注

NetScaler VPXインスタンスは常にNetScaler ADMに登録する必要があります。まだ登録していない場合は、**NetScaler ADMに登録**を有効にし、NetScaler ADMのログイン資格情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. **ライセンスの割り当て**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。**ライセンスの取得**をクリックします。
8. 次のページで**再起動**をクリックして、ライセンスを適用します。

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 editionライセンスがすでに実行されているとします。そのライセンスを解放し、Advanced editionからチェックアウトできます。

CLIを使用したNetScaler VPXライセンスでのライセンスサーバーの構成

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

VPXインスタンスのライセンスサーバーIPアドレスを、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、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADMでの仮想CPUライセンスの管理

1. NetScaler ADMで、**インフラストラクチャ > プールされたライセンス > プールされた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。
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、ライセンスを管理するためにNetScaler ADMで実行されているライセンスサーバーに依存しています。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、環境にデプロイできます。

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. CPXおよびVPXでサポートされる仮想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. CPX専用の単一から複数の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。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。

© 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
```

NetScaler CPXインスタンスをプロビジョニングする際に、NetScaler Licensing Serverを、以下に示す**docker run**コマンドの環境変数として定義します。

```
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>
cpx:11.1
```

ここで、,

- \<*LS*_*IP*_*ADDRESS*\> はNetScaler Licensing ServerのIPアドレスです。
- \<*LS*_*PORT*\> はNetScaler Licensing Server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、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 Pooled Capacity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。

例：

```
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 (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。その後、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スのチェックアウトに対してn = 1を指定することです。マルチコアCPXのユースケースでは、「n」個のvCPU (「n」は1から7まで) 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
```

プールされた容量。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、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、以下の表に示すように、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/秒
2	2000 メガビット/秒
3	3500 メガビット/秒
4	5000 メガビット/秒
5	6500 メガビット/秒
6	8000 メガビット/秒
7	9300 メガビット/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

システム設定の管理

次の表は、**設定** > **管理** で利用可能なオプションのリストを示しています。

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、およびプロキシサーバー	IPアドレス	NetScaler ADMの展開に使用されるNetScaler ADMネットワーク構成のIPアドレスの詳細を表示します。
	セカンダリNIC	NetScaler ADM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 ADMにアクセスするためのデュアルNICの構成」を参照してください。
	ホスト名	NetScaler ADM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 ADM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	ADM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 ADM」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADMで使用するタイムゾーンを変更できます。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	ADM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 ADM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 ADM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。「**Enable Message**」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、「**Save**」をクリックします。
ADMフィンガープリントの表示		サービスグラフを開始するために、一意のNetScaler ADM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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

システム構成	オプション	説明
		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。

システムメンテナンス

システムメンテナンス	説明
NetScaler ADMのアップグレード	GUIを介してNetScaler ADM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 ADM を再起動	NetScaler ADM を再起動できます
NetScaler ADM をシャットダウン	NetScaler ADM 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
システムとインスタンスのデータプルーニング	システム	NetScaler ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データプルーニング	オプション	説明
	インスタンスイベント	NetScaler ADM 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」を参照してください。
	ネットワークレポート	NetScaler ADM に保存されるネットワークレポートデータを制限できます。

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」を参照してください。
	インスタンス	NetScaler ADM 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」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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	いくつかの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 Application Delivery Management (ADM) を設定して、電子メール、SMS、またはSlackのいずれかを通じ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。
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL設定	説明
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 ADMで機能を有効または無効にできます。詳細については、「ADM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の構成

NetScaler® Application Delivery Management (ADM) システムをバックアップおよび復元する前に、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の構成** 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の暗号化** 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 ADM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 ADM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。

NTPサーバーを構成する

NetScaler® Application Delivery Management (ADM)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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

することで、NetScaler ADM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なります。

NetScaler ADM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、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）にしたい場合は、「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）にしたい場合は、「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。
   - **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 ADMでNTP同期を有効にするには：

1. **Settings > NTP Servers**に移動します。
2. 「**NTP同期**」をクリックし、「**NTP同期を有効にする**」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。

   NTPを同期(/en-us/netscaler-application-delivery-management-software/media/ntp1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

NetScaler® Application Delivery Management (ADM) のアップグレード

各NetScaler ADMリリースでは、機能が強化された新しい機能や更新された機能が提供されます。強化点の包括的なリストは、リリース発表に付随するリリースノートに記載されています。ソフトウェアをアップグレードする前に、リリースノートをお読みください。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ライセンスの種類を理解することが重要です。

NetScaler ADMをアップグレードするには：

1. **Settings > Administration**に移動します。**System Maintenance**の下にある**Upgrade NetScaler ADM**をクリックします。
2. 「NetScaler ADMのアップグレード」ページで、**Local**（ローカルコンピューター）または**Appliance**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

   Applianceを選択する場合、NetScaler ADMの`/var/mps/mps_images`でアップグレードイメージが利用可能で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すると、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。

NetScaler® ADM のパスワードをリセットする方法

NetScaler ADM 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 ADM 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™:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. XenCenter を使用して Citrix Hypervisor にログオンします。
2. NetScaler ADM 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 ADM が再起動し、次のメッセージが表示されます。

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 ADM を再起動します。

9. NetScaler ADM 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 ADM を再起動します。

   - `rm /flash/mpsconfig/master.passwd`
   - `rm –rf /etc/passwd`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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 ADMが再起動します。
5. /u@プロンプトを表示するには、**Enter**を押します。
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 ADMを再起動します。
9. NetScaler ADM 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。

   注記

   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、NetScaler ADM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 ADM ノードを選択し、右クリックして、**再起動**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM が再起動します。

5. /u@ プロンプトを表示するには、**Enter** を押します。
6. 以下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
   ```

7. 以下のコマンドを使用してファイルを作成します。

   ```
   touch /flash/mpsconfig/.recover
   ```

   パスワードは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 ADMを再起動します。
9. NetScaler ADM 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、次のコマンドを実行してNetScaler ADM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サーバーにNetScaler ADMにログオンします。
2. NetScaler ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set console='comconsole,vidconsole'
```

5. NetScaler ADMを再起動するには、**boot -s**コマンドを実行します。
6. 「**Enter full path of shell or RETURN for /bin/sh:**」というメッセージが表示されたら、**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
   ```

   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. NetScaler ADMを再起動するには、**Reboot**コマンドを実行します。
10. NetScaler ADM GUIにアクセスし、再起動が完了するまで待ちます。

    GUIからログオンするには*nsroot/nsroot*資格情報を、SSHコンソールからログオンするには*nsrecover/nsroot*資格情報を使用できるようになりました。

    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、NetScaler ADMを再起動します。

    - `rm /flash/mpsconfig/master.passwd`
    - `rm –rf /etc/passwd`

NetScaler® ADM にアクセスするためのセカンダリ NIC の構成

NetScaler ADM への管理アクセスを分離するために、2番目のNICを構成できます。この2番目のNIC機能を使用すると、要件に応じて、NetScaler ADM 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 ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADM 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 ADM とその管理対象 NetScaler インスタンス間のトラフィックに1つのIPアドレスを構成する。
- NetScaler ADM ソフトウェアを管理するために別のIPアドレスを構成し、ソフトウェア内のすべての管理タスクを実行する。

注

NetScaler ADM が HA ペアとして構成されている場合、2番目の 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 ADM 13.0 Build 47.x 以降** を展開および構成し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2番目の NIC を追加し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 ADM で2番目の NIC を構成する

1. ADM GUIにログオンします。
2. **Settings > Administration**に移動します。
3. 「**ネットワーク構成**」で、「**IPアドレス、セカンダリNIC、ホスト名、プロキシサーバー**」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 ADM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 ADMにアクセスできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **Netmask** – ネットワークホストを指定する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 ADMのルートエントリを追加する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。

NICの構成(/en-us/netscaler-application-delivery-management-software/media/configure-nic.png)

ADMエージェントにアクセスするためのセカンダリNICを構成する

ADMエージェントで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、ADMエージェントは次のことができるようになります。

- ADMエージェントとADC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 ADMを介して送受信されるトラフィックを分離し、NetScaler ADMと別のネットワークにある管理対象のNetScalerインスタンスとの間で通信することもできます。
- ADMエージェントとNetScaler® ADM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 ADMを管理し、管理タスクを実行できます。

注

両方のNICの機能と構成を交換す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.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 ADM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 ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

ADM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、ADMエージェント、NetScaler ADM、およびADC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。
2. **nsrecover/nsroot**の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 – ADMエージェントとADC間の通信用
   - NIC 2 – ADMエージェントとNetScaler ADM間の通信用

   「ifconfig」のコードブロック(/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。

   「networkconfig」のコードブロック(/en-us/netscaler-application-delivery-management-software/media/code_block_networkconfig.png)

   注

   2番目のNICネットワークアドレスは、複数のIP値を取ることができます。
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、ロギングのための標準プロトコルです。Syslogには2つのコンポーネントがあります。Citrix Application Delivery Controller (ADC) 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) またはリモートシステムで実行できる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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。ロギング情報を統合し、収集されたデータからインサイトを導き出すことができます。また、Syslogを設定して、さまざまな種類のイベントをログに記録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® Application Delivery Management (ADM) 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。

- 一般的なSyslogデータ
- AppFirewallデータ
- NetScaler Gatewayデータ

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データを保持するように設定されたパージ間隔よりも優先されます。

NetScaler ADMのSyslogパージ間隔設定を構成するには：

1. **>** に移動します。 で をクリックし、 をクリックします。
2. ページで、 を指定します。NetScaler ADMが汎用Syslogメッセージを保持する日数を入力します。

システムプルーニングとイベントプルーニングの設定

NetScaler Application Delivery Management (ADM) 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、データをプルーニングできます。NetScaler ADM 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）にプルーニングされます。

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プルーニング設定を構成するには：

1. **設定** > **管理** に移動します。**データプルーニング** の下にある **システムおよびインスタンスデータプルーニング** をクリックします。
2. **システムプルーニング設定の構成** ページで、以下を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- データを保持する日数
- ディスクスペースの割合（プルーニングしきい値）

3. **OK** をクリックします。

自動データプルーニングを有効にする チェックボックスを選択すると、自動プルーニングを有効にできます。ディスク使用量が設定された **データプルーニングしきい値** 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。

注

プルーニングは、データプルーニングしきい値または保持するデータ（日数）のいずれかの条件が満たされたときに開始されます。最初に満たされた方が、もう一方よりも優先されます。

アラーム設定を構成および有効にするには：

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。

- **重大度** — 重大度レベルを選択します。
- **アラームしきい値** — イベントの重大度が計算される値を入力します。
- **時間** — アラームをトリガーするまでの時間（分）を入力します。

アラームの自動パージを設定する(/en-us/netscaler-application-delivery-management-software/media/configure-alarm-automatic-purging.png)

NetScaler® ADM を使用してイベントの削除設定を構成する

NetScaler ADM 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 ADM 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）に削除されます。

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 ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デフォルト以外のユーザーのシェルアクセスを有効にする

NetScaler® Application Delivery Management (ADM) で、デフォルト以外の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、デフォルト以外のユーザーのシェルアクセスは無効になっています。

NetScaler ADM でデフォルト以外のユーザーのシェルアクセスを有効にするには:

1. NetScaler ADM で、**System** \> **System Administration** に移動します。
2. **System Settings** で、**Change System Settings** をクリックします。
3. **Modify System Settings** ページで、次のパラメータを設定します。
   - **インスタンスとの通信** - 通信プロトコルを選択します。
   - **セキュアアクセス** - NetScaler ADM のセキュアアクセスを有効にします。
   - **セッションタイムアウトを有効にする** - 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。
   - **基本認証を許可する** - 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。
   - **nsrecover ログインを有効にする** - 管理サービスで `nsrecover` ログインを有効にします。
   - **証明書のダウンロードを有効にする** - 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。
   - **非nsrootユーザーのシェルアクセスを有効にする** - NetScaler ADM でデフォルト以外の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時にユーザー資格情報を要求する** - NetScaler ADM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。
4. **OK** をクリックします。

アクセスできない NetScaler® ADM サーバーを復旧する

NetScaler Application Delivery Management (ADM) 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。NetScaler ADM

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーティリティツールを起動して、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、データベースにアクセスできるようにすることができます。NetScaler ADMリカバリスクリプトは、古いまたは未使用のデータベーステーブルとファイルをクリアすることで、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、連続するステップ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 ADMスタンドアロン展開におけるNetScaler ADMデータベースリカバリスクリプトの使用方法

シングルサーバーのNetScaler ADM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、データベースにアクセスできるようにし、その後、復旧操作を実行します。

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 ADM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 ADM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」と入力して**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断している間、次の画面が表示されます。

3. 画面には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. クリーンアップする必要がある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します。**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」と入力して**Enter**キーを押し、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 ADM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格納するNetScaler ADM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、時間とともに肥大化したり、無効な行が蓄積される可能性のあ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 ADM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を提供します。「1」から「9」までの数字を入力して任意の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

番号「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しておらず、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 ADMを再起動します。

   システムクリーンアップ後にNetScaler ADMを再起動してください。NetScaler ADMが再起動した後、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 ADM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度実行し

© 1997–2026 Citrix Systems, Inc. All rights reserved.

て、さらにスペースを解放してください。NetScaler ADMが稼働している場合、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ゼロ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 ADM高可用性展開でNetScaler ADM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 ADM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 ADM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. で利用可能な手順2から手順に従います(#how-to-use-citrix-adm-database-recovery-script-for-a-citrix-adm-standalone-deployment)

NetScaler® ADMサーバーにホスト名を割り当てる

NetScaler Application Delivery Management (ADM) 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。ホスト名は、NetScaler ADM のユニバーサルライセンスに表示されます。

NetScaler ADM サーバーにホスト名を割り当てるには:

1. NetScaler ADM で、**システム** \> **システム管理** に移動します。
2. **システム設定** で、**ホスト名の変更** をクリックします。
3. **ホスト名の構成** ページで、ホスト名を入力し、**OK** をクリックします。

© 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® ADMサーバーのバックアップと復元

NetScaler ADM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ADMサーバーを復元することをお勧めします。たとえば、ADMバージョンが13.0の場合、13.0 ADMバックアップを使用してサーバーを復元します。

ADM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。**Settings > Backup Files**ページは、すべてのADM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ADM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ADM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 ADM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 ADM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。
- データベースに保存されているシステムデータ:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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ている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の詳細など。
  - 管理者によって作成され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、ADM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 ADM構成をバックアップする

デフォルトでは、NetScaler ADM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。バックアップのスケジュールを設定し、時間を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 ADM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、Citrixでは、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)ことを推奨しています。

NetScaler ADM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 ADM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。構成を復元する場合は、まずファイルをNetScaler ADM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 ADM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する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、次のパラメータを指定します。
   - **サーバー** - 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。
   - **ユーザー名とパスワード** - 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資格情報。
   - **ポート** - ファイルの転送先システムのポート番号。
   - **転送プロトコル** - 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** - バックアップされたファイルが新しいシステムに転送される場所。
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 ADM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。

   新しいバックアップファイル(/en-us/netscaler-application-delivery-management-software/media/backup-mas-system-citrix.png)

> **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、**Settings > Backup Files**に移動し、コピーするファイルを選択して、**Download**をクリックします。

バックアップファイルからNetScaler ADM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 ADM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場合、またはバックアップファイルの内容が変更された場合、復元操作は失敗します。

バックアップファイルからNetScaler ADM構成を復元するには：

1. **Settings > Backup Files**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、**Restore**をクリックします。

   バックアップファイルを復元する(/en-us/netscaler-application-delivery-management-software/media/mas-restore-system-citrix.png)
3. 確認ダイアログボックスで、**Yes**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ADM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® ADM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 ADM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 ADMサーバーのスナップショットを取得する

次の順序でNetScaler ADMサーバーのスナップショットを取得します。

1. NetScaler ADMセカンダリサーバー
2. NetScaler ADMプライマリサーバー

NetScaler ADMサーバーのスナップショットを取得するには：

1. ハイパーバイザーで、仮想マシンのリストからNetScaler ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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 ADMサーバーのスナップショットを復元するには、次の手順を使用します。

1. NetScaler ADMプライマリサーバー
2. NetScaler ADMセカンダリサーバー

NetScaler ADM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 ADM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に復元されます。
3. NetScaler ADM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。

- NetScaler® ADM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）やログイン成功があった場合、その詳細をイベントとして表示できます。

管理者は、これらのログを使用してセキュリティを維持し、失われたトランザクションを回復できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADMでsyslogサーバーを構成するには：

1. **設定 > ADM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、**追加**をクリックします。
3. **Syslogサーバーの作成**ページで、次の値を入力します。
   - **名前** - syslogサーバーの名前。
   - **IPアドレス** - syslogサーバーのIPアドレス。
   - **ポート** - 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. **作成**をクリックします。

NetScaler ADMでsyslogの日付と時刻の形式を構成するには：

1. **設定 > ADM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、syslogサーバーを選択し、「**Syslog Parameters**」をクリックします。
3. 「**Configure Syslog Parameters**」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 ADMでsyslogメッセージを表示するには：

「**Settings > ADM Audit log messages**」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
- ソース

詳細については、「Syslog message references」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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® Application Delivery Management (ADM) 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 ADM のSSL設定を構成するには:

1. **システム** > **システム管理** に移動します。**システム設定** で、**SSL設定の構成** をクリックします。
2. **SSL設定** 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、**設定の編集** \> **プロトコル設定** に移動し、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、**設定の編集** \> **暗号スイート** に移動し、必要な変更を行います。
5. **OK** をクリックし、次に **閉じる** をクリックします。

CPU、メモリ、ディスクの使用状況を監視する

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® Application Delivery Management (ADM) 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、ディスクの使用状況を監視するには、,

- **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、ディスク容量、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。

通知設定を構成する

以下の機能について通知を受け取るには、通知タイプを選択できます。

- **イベント** – NetScalerインスタンスに対して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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 ADM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。

ADMは以下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

各通知タイプについて、ADM GUIには構成済みの配信リストまたはプロファイルが表示されます。ADMは、選択された配信リストまたはプロファイルに通知を送信します。

メール配信リストを作成する

ADM機能のメール通知を受信するには、メールサーバーと配信リストを追加する必要があります。

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. 「**設定 > 通知**」に移動します。
2. 「**メール**」で、「**追加**」をクリックします。
3. 「**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場合は、「**追加**」をクリックします。
   - 「**差出人**」 - ADM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**」 - ADM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**」 - ADM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**」 - ADM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。
4. 「**作成**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。「**メール**」タブには、ADM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

ADM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** - ADM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、ADM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

ADM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。
   - **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**」 - ADM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、外部ソースからのメッセージをSlackに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。そして、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>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Slackチャネルを追加(/en-us/netscaler-application-delivery-management-software/media/upgrade-slack-citrix.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、ADMに存在するすべてのSlackプロファイルが表示されます。

PagerDutyプロファイルを作成する

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、登録された番号に電子メール、SMS、プッシュ通知、および電話で通知を設定できます。

NetScaler ADM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。統合のためにPagerDutyでサービスを作成する際は、「**Generic Events API Integration**」オプションを使用します。
4. 「**作成**」をクリックします。

詳細については、PagerDuty ドキュメントのサービスと統合を参照してください。

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、ADM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ADM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 ADMをServiceNowと統合する必要があります。詳細については、NetScaler ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **設定 > 通知**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. **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。

   NetScaler® ADM 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

Citrixでは、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® Application Delivery Management (ADM) 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 ADMサーバーの場合、いずれ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では、テクニカルサポートファイルを生成するためにロードバランシング仮想サーバーのIPアドレスを使用しないことを推奨しています。

NetScaler ADMからテクニカルサポートファイルを構成して送信するには：

1. **System \> Diagnostics \> Technical Support** に移動し、**Generate Technical Support File** をクリックします。
2. **Generate Support File** ページで、次のオプションを選択します。

- **Collect Debug Logs** – このオプションを選択して、`afdecoder` ログを収集します。
- **Duration** – デバッグログを収集する期間を入力します。このオプションは、**Collect Debug Logs** オプションを有効にした場合にのみ表示されます。
- **Collect Data Distribution** – 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. ADM 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. ADMコンソール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 Web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、ADMコンソールにログオンします。

      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、ADMからローカルシステムにテクニカルサポートファイルをダウンロードしてCISに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、ADMコンソール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信頼していない場合に発生する可能性があります。） ADM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

ADM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、ADM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CISにアップロードすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

暗号グループを構成する

暗号グループは、Citrix Application Delivery Controller (ADC) 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® ADM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** – をクリックして、 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 リストに移動します。
5. **作成** をクリックします。

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® ADM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 ADM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。その後、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 ADM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。
   - **Version。** 使用するSNMPバージョンを選択します。
   - **Destination Server。** トラップ宛先の名前またはIPアドレス。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Port。** 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。
- **Community。** 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。
3. 必要に応じて、「**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、「**ネットマスク**」（SNMPマネージャーネットワークのサブネットマスク）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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

システムアラームの設定と表示

NetScaler® Application Delivery Management (ADM) 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取り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メールまたはSMSで通知を受け取るように設定できます。

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、および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 ADM 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 ADM で表示するか、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 ADM 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。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM 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** ページの **Audit Messages** で、**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。

   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。システム通知の設定方法については、「NetScaler ADM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。

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。
   - **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **Create** をクリックします。

SNMP v3マネージャーを追加する

NetScalerエージェントの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。

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。

SNMPユーザーを追加

SNMPマネージャーからのSNMP v3クエリに応答する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、次の手順を実行します。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Create SNMP User** ページで、次の詳細を追加します。

   - **Name**。ユーザー名を入力します。
   - **Security Level**。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のを制限します。

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ー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。
   - **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選択できます。
3. **Create** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

エージェント設定の構成

NetScaler® ADM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 ADM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 ADMサーバーに送信します。

1. **Settings > Administration**に移動します。
2. **System Configurations**の下にある**System, Time zone, Allowed URLs and Agent Settings**を選択します。
3. **Basic Settings > Agent Settings**で、キープアライブ間隔を30〜120秒の間で指定します。
4. **Save**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

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できるようにすることができます。

1. **Settings > Administration**に移動します。
2. **System Configurations**の下にある**System, Time zone, Allowed URLs and Agent Settings**を選択します。
3. **Basic Settings > Agent Settings > Remove current password prerequisite for agent password change**チェックボックスで、次のことができます。
   - チェックボックスをオンにすると、**Change Agent Password**ページから**Current password**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、**Change Agent Password**ページに**Current password**フィールドが保持されます。
4. **保存**をクリックします。

> **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® ADM を API プロキシサーバーとして

NetScaler Application Delivery Management (NetScaler ADM) 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だけでなく、管理対象インスタンスの REST API プロキシサーバーとしても機能します。REST API クライアントは、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、NetScaler ADM に送信できます。NetScaler ADM は、自身が応答する必要がある API リクエストと、変更せずに管理対象インスタンスに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 ADM は以下の利点を提供します。

- **API リクエストの検証**。NetScaler ADM は、構成されたセキュリティポリシーと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 ADM 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。
- **集中監査**。NetScaler ADM 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 ADM 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手間を省きます。

NetScaler ADM が API プロキシサーバーとして機能する方法

NetScaler ADM にリクエストを管理対象インスタンスに転送させたい場合は、API クライアントが API リクエストに以下のいずれかの HTTP ヘッダーを含めるように構成します。

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、ADM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ADC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ADC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

設定 > 管理 > システム構成 **> 基本設定**で、**インスタンスログインの資格情報を要求**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 ADM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します。ヘッダーの値は、NetScaler ADMがリクエストを転送すべき管理対象インスタンスを特定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 ADMはリクエストを次のように処理します。

1. リクエストを変更せずに、NetScaler ADM はリクエストをインスタンス API 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ないことを保証します。また、管理対象インスタンスが利用可能かどうかを判断するチェックなど、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 ADM 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を要求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。そのためには：

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 ADM 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 ADM 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 ADM は、リクエストを未変更のまま、IP アドレス 192.0.2.10 を持つ管理対象インスタンスに転送する必要があります。すべての例で _MPS_API_PROXY_MANAGED_INSTANCE_IP ヘッダーを使用します。

NetScaler ADM 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 ADM 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 ADM は、セッション ID を含む応答でログオン要求に応答します。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、次の形式の API リクエストを NetScaler ADM に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。そして、_MPS_API_PROXY_MANAGED_INSTANCE_IP の値は ADC 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、次の形式の API リクエストを NetScaler ADM に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、次の形式の API リクエストを NetScaler ADM に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、次の形式の API リクエストを NetScaler ADM に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: ADC 上の CLI 実行構成をダウンロードする

クライアントは、次の形式の API リクエストを NetScaler ADM に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 ADM) の機能に関する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ている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 ADM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 ADM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 ADM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** 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インスタンスの場合、NetScaler ADMには、Security Insightを明示的に有効にするオプションはありません。NetScaler ADM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、NetScalerインスタンスでAppFlowパラメータを構成してください。NetScalerインスタンスでAppFlowパラメータ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 ADMは分析情報の収集を自動的に開始しますか?

いいえ。NetScaler ADM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か?

いいえ。すべての構成は、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を一覧表示するNetScaler ADMユーザーインターフェイスから行われます。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 ADMユーザーインターフェイスには、分析を有効にするために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ト仮想サーバー

NetScaler ADMにディスクを追加する方法?

NetScaler ADMにディスクを追加するには：

1. NetScaler ADM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 ADM仮想マシンに接続します。

   例えば、120 GBのNetScaler ADM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 ADM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 ADM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 ADM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 ADMはインスタンスから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 ADMに追加されています。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 ADMにはトラフィックが流れません。セルフサービス診断がこの問題を検出し、「2つのインスタンスでコレクターが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、ADMはHTMLインジェクションを通じてHTMLページの読み込み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遅延の問題を特定できます。

認証

認証リクエスト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 ADMは外部認証サーバーに向けられる認証リクエストを負荷分散できます。認証サーバーの負荷分散により、認証負荷が複数の認証サーバーに分散されることが保証され、認証サーバーの過負荷を防ぎます。LDAP、RADIUS、TACACSなどの認

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証プ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する必要があるのはなぜですか?

カスケードされた外部認証サーバーは、中断のない認証処理を提供し、認証サーバーが失敗した場合でも正当なユーザーへのアクセスを許可します。カスケード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。

外部認証サーバーをいくつカスケードできますか?

NetScaler ADMでは、最大32台の外部認証サーバーをカスケードできます。

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。外部認証が失敗した場合、NetScaler ADM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 ADMで、**設定 > 認証 > 認証構成**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?

ユーザーを認証するために外部サーバーを追加した場合、既存のユーザーグループをNetScaler ADM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、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 ADM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のロードバランシング機能を使用している場合、NetScaler ADM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 ADMにログインし、NetScaler ADM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NetScaler ADMで管理され、外部サーバーでは管理されません。ユーザーは外部サーバー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 ADM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ロードバランス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引き続きNetScaler ADMで機能します。

構成管理

NetScaler ADM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 ADM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構成コマンドのセットです。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 ADM 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 ADM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 ADM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 ADMからSSL証明書を削除すると、NetScalerインスタンスから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 ADM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?

パスワードを変更するには：

1. NetScaler ADMで、**設定 > ユーザー管理 > ユーザー** に移動します。

   ユーザーページ が表示されます。
2. ユーザー名 **nsroot** を選択し、**編集** をクリックします。

   システムユーザーの構成 ページが表示されます。
3. **パスワードの変更** を選択し、任意のパスワードを作成します。
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

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は?

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ペアの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?

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、これらの2つのサーバーをHAペアに展開する際にどのような影響があります?

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、両方のサーバーにデフォルトのパスワードを設定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。原因は何ですか?

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。原因は何ですか?

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、プライマリノードとセカンダリノードを高可用性ペアとして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。

NetScaler ADMスタンドアロンおよびNetScaler ADM HAでサポートされているDB?

NetScaler ADMスタンドアロンとNetScaler ADM HAはどちらもPostgreSQLをサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 ADM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秒の期間がセカンダリノードへのデータ損失の可能性として考慮されます。

プライマリノードがダウンした場合、どうなりますか?

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。**設定 > 展開**に移動します。

   展開ページが表示されます。**HAの解除**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、NetScaler ADMを初期ネットワーク構成で設定します。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 ADMはSANストレージをサポートしていますか?

Citrixは、NetScaler ADM VHDをローカルストレージにホストすることを推奨しています。SAN内のストレージデバイスにホストされている場合、NetScaler ADM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ADM展開はサポートされていません。

NetScaler ADMは追加ディスクをサポートしていますか?

はい。NetScaler ADM 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HAペアを無効にした後、設定されたフローティングIPアドレスはどうなりますか?

フローティングIPアドレスにアクセスできなくなり、高可用性ペアを再デプロイする必要があります。

再デプロイ中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レプリカサーバーにすぎず、プライマリノードが何らかの理由で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。Citrixでは、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のいずれか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ている場合でも、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?

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. ユーザー名として `nsrecover` を使用し、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）を登録してデプロイする で利用可能な **ステップ3** から手順を実行します。

      初期ネットワーク構成中に、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、(https://docs.citrix.com/ja-jp/netscaler-application-delivery-management-software/13-1/deploy/high-availability-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

deployment.html#register-and-deploy-the-second-server-secondary-node)にある**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. **設定 > 展開**に移動します。

   展開ページが表示されます。

   a. **HA設定**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アドレスを構成**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。

ADM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 ADM 13.1ビルド4.43以降**。
- **NetScalerエージェント13.1ビルド17.42以降**。

展開（ディザスタリカバリ）

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。

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ペアを再展開する一環として、DRサイトを再構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イベント管理

NetScaler ADM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、エンティティ状態の変更などの詳細を、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 ADMイベントダッシュボードを使用して、すべてのNetScalerインスタンスで重大なイベントの重大度詳細について生成された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 ADMを使用すると、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。イベントルールにより、NetScaler ADM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。

特定の条件でルールを構成し、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、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、管理対象のNetScalerインスタンスからNetScaler ADMへのSNMPトラップの転送、およびSMS通知の送信です。

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ADCインスタンスがADMに接続できない場合はどうなりますか?

ADCインスタンスとADM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、プール容量ライセンスが機能し始めます。猶予期間中は、ADC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、ADC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 ADMのデータセンターとは何ですか?

NetScaler ADMデータセンターは、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 ADM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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ションとラフィックフロー、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 ADM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 ADMでサポートされているNetScaler ADC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 ADMから検出、管理、監視したいNetScaler ADC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 ADMサーバーに追加する必要があります。NetScaler ADMには、以下のNetScaler ADCアプライアンスと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

インスタンスは、NetScaler ADM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。

インスタンスプロファイルとは?

インスタンスプロファイルは、NetScaler ADM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 ADMで複数のNetScaler VPXインスタンスを再検出できますか?

はい、NetScaler ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure > Instances > NetScaler > VPX に移動し、再検出するインスタンスを選択して、**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 ADMを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、ADM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。

- 単一のインスタンスを追加する場合: ADC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。
- ADC 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>`
- ADC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。例の形式: NAT1, NAT2, NAT3,(CLUSTERIPのNATIP)。

詳細については、次のトピックを参照してください。

- NetScaler ADMへのインスタンスの追加
- 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、災害復旧ノードを登録するにはどうすればよいですか?

次のコマンドを使用して、災害復旧 (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 ADM DRノードを展開および登録するの手順に従ってください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

StyleBooksは、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するために使用できますか?

はい、異なるバージョン間でコマンドに不一致がない場合、StyleBooks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、どうなりますか?

NetScalerインスタンスへの構成の適用が失敗した場合、その構成は他のインスタンスには適用されず、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バックアップには、StyleBooksを介して適用された構成が含まれます?

はい

システム管理

NetScaler ADMサーバーにホスト名を割り当てることはできますか?

はい、NetScaler ADM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 ADM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 ADM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 ADMの構成をバックアップおよび復元できますか?

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および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 ADMが不安定になった場合、バックアップファイルを使用してNetScaler ADMを安定した状態に復元できます。

NetScaler ADM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 ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrixは、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 ADM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 ADM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。カウンターの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 ADMのテクニカルサポートファイルを生成できますか?

はい。Citrixでは、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 ADMのデータと統計情報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 ADMデータベースからの個別の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。

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 ADM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。ロギング情報を統合し、収集されたデータからインサイトを導き出すことができます。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データがが NetScaler ADMから削除されるまでの日数を指定できます。

NetScaler ADMでNTPサーバーを設定できますか?

NetScaler ADM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 ADM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、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM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を保証します。

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 ADMでNTPサーバーを設定する方法」を参照してください。

NetScaler ADM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 ADMのアクティブ-パッシブHA展開モードは、NetScaler ADM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 ADM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アプライアンスを設定していました。この構成を更新するにはどうすればよいですか?

NetScaler ADM 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。

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を使用してNetScalerインスタンス上でNetScaler ADM HAペアのロードバランシングを構成できますか?

いいえ、ポート443を使用してNetScalerインスタンス上でNetScaler ADM 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 ADM HAノードが正しく監視されません。

NetScaler ADMサーバーのバックアップファイルを使用して、別のNetScaler ADMサーバーの構成を復元できますか?

はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM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 ADM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 ADM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 ADM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 ADM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 ADM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。

NetScaler ADMでNetScalerインスタンスをバックアップする場合、結果は完全バックアップですか、それとも基本バックアップですか?

NetScaler ADMによるNetScalerインスタンスのバックアップは、完全バックアップです。

NetScaler ADM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 ADM HAフェイルオーバーが発生した場合、NetScalerインスタンスはどのように管理されますか?

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SNMPトラップの宛先として最新のプライマリノードの詳細で更新されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

新しいプライマリ（アクティブ）NetScaler ADM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ます。もしそうであれば、新しいプライマリは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を置き換えます。

NetScaler ADM HAノードがダウンから復旧した場合の動作?

サービスに復帰した後、アクティブノードがフェイルオーバーしない限り、NetScaler ADMノードはパッシブのままです。

NetScaler ADM HAノード間でのNetScalerインスタンスの分散方法?

すべてのNetScalerインスタンスは、プライマリNetScaler ADMノードによって管理されます。

NetScaler ADM 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 ADM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。代替案については、NetScalerサポートにお問い合わせください。

NetScaler ADM 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、しかしロードバランサーがない場合、NetScaler ADM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、Citrixはパッシブノードで構成を作成しないことを推奨しています。

NetScaler ADMは外部データベースをサポートしていますか?

いいえ

NetScaler ADMによって管理されているNetScalerインスタンスを、NetScaler ADM HAのロードバランサーとして使用できますか?

はい

NetScaler ADM HAノード間でどのようなデータが同期されますか?

NetScaler ADM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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- /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

- 適応型しきい値を設定する
- データベース集約を構成する
- SLA管理を構成する
- しきい値とアラートを作成する
- URLデータ収集を無効にする
- 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
- ネットワーク違反の詳細
- SSLインサイト
- TCP 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セットアップ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
- NetScaler® テレメトリープログラムのオプションのテレメトリーデータ
- NetScaler® テレメトリープログラムに必要なテレメトリーデータ
- データガバナンス
- HAペアでのNetScaler® ADM構成のバックアップと復元
- システム通知設定を構成する
- ジオマップのサイトを構成する

適応型しきい値を設定する

適応型しきい値機能は、各URLへの最大ヒット数に対するしきい値を設定します。URLへの最大ヒット数が、そのURLに設定されたしきい値よりも大きい場合、syslogメッセージが外部syslogサーバーに送信されます。しきい値の間隔は、日単位または週単位で設定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

しきい値は次のように計算されます。

しきい値 = 最大ヒット数 * しきい値乗数

ここで、:

- 最大ヒット数は、URLへの最大ヒット数です。
- しきい値乗数は、ユーザーが定義する整数値です (デフォルト: 2)。

NetScaler® ADM を使用して適応型しきい値を作成するには

1. **System** \> **Analytics Settings** \> **Adaptive Thresholds** に移動し、**Add** をクリックします。
2. **Create Adaptive Thresholds** ページで、次のパラメータを指定します。
   - **名前** - しきい値名
   - **エンティティ** - URL
   - **期間** - しきい値の期間 (日または週)
   - **しきい値乗数** - 指定されたURLの最大ヒット数に乗算され、そのURLの適応型しきい値を取得するために使用されるユーザー定義の整数。

データベース集約を構成する

NetScaler® ADM でデータベース集約を構成すると、NetScaler の分析データの履歴データを保存する期間をカスタマイズできます。分析の履歴データに対して、次のデータベース集約タイプを選択できます。

- 分単位のデータを保持する時間
- 時間単位のデータを保持する日数
- 日単位のデータを保持する日数

データベース集約を構成するには

1. **システム** > **分析設定** > **データベース集約** に移動します。
2. データベース集約を構成する Insight タイプをクリックします。

3. NetScaler ADM で Insight データを保持する期間を指定します。たとえば、Gateway Insight の場合、分析の分単位の履歴データを 2 時間、または時間単位のデータを 1 日間保存できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SLA管理を構成する

サービスレベルアグリーメント管理機能は、ドメイン使用全体におけるサーバー応答時間、ヒット数/秒、帯域幅使用量に関するSLAを管理するのに役立ちます。さまざまな違反に対してSLAを設定することで、NetScaler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。

以下のSLA違反を設定できます。

- サーバー応答時間
- 帯域幅のSLA違反頻度
- ヒット数のSLA違反頻度
- 応答時間のSLA違反頻度

アプライアンスがSLA違反を検出するたびに、各SLA違反の通知を設定できます。通知タイプをメール、SMS、またはSyslogとして設定し、それぞれ配布リストを設定できます。

NetScalerインスタンスのSLA違反を設定するには

1. **System** \> **Analytics Settings** \> **SLA Management** に移動します。
2. 表示されたリストから、SLAを管理したいアプライアンスのNetScaler® IPアドレスを選択します。
3. 新しい **SLA Group** を追加して違反定義を追加する場合は、**Add** をクリックします。または、すでにSLAグループを追加している場合は、リストからSLAグループを選択できます。
4. **SLA Group** フィールドに、新しいSLAグループの名前を入力します。
5. SLAモニターを有効または無効にするには、適切なチェックボックスを選択します。
6. 選択したオプションの適切な違反値を選択します。例: 最大サーバー応答時間 (ms)* = 22 ms。
7. 「**Notification Type**」および「**Interval**」リストから、通知タイプと通知間隔を適切に選択します。
8. 「Mail/SMS/Syslog Distribution List」メニューから、通知を送信する配布リストを選択できます。
9. 「**Create**」をクリックして、NetScalerアプライアンスにSLAグループを作成し、追加します。

   SLAグループ(/en-us/netscaler-application-delivery-management-software/media/sla-how-to.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

カウンターの値がしきい値を超えると、NetScaler® ADM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 ADM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 ADM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. 必要に応じて、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 では、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な、複数のしきい値を設定することもできます。

URLデータ収集を無効にする

NetScaler® ADMのダッシュボードのWeb InsightノードにURLレポートを表示したくない場合は、URLデータ収集を無効にできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADMからURLデータ収集を無効にするには

1. **System** \> **Analytics Settings** に移動し、**Configure Data Record Settings** をクリックします。
2. **Web Insight URL Data Collection Settings** セクションで、**Enable URL Data Collection** オプションがオンになっている場合は、チェックボックスをオフにします。
3. **OK** をクリックします。

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的なポイントです。IPFIXとLogstreamは、これらのAppFlowレコードをNetScalerインスタンスからNetScaler ADM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® ADMでより多くのリソースを処理することになります。
- Logstreamは、NetScalerインスタンスからNetScaler ADM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つとして使用される、Citrix独自のプロトコルです。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。

11.1 Build 47.14から11.1 Build 62.8までのNetScaler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。**12.0から最新バージョン**までのNetScaler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ADC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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**の間では、LogstreamはWeb Insight (HTTP) を有効にするためのデフォルトの転送モードであり、IPFIXは他のインサイトを有効にするための唯一の転送モードです。NetScalerのバージョン**12.0以降**では、転送モードとして**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-citrix.png)

   > **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 ADM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、分析を有効にすることはできません。エラーメッセージが表示されます

次の表は、転送モードとしてLogstreamをサポートするNetScaler ADMの機能について説明しています。

機能	IPFIX	ログストリーム
Web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	•	•

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能	IPFIX	ログストリーム
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® Application Delivery Management (ADM) 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Web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。

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。これは、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接続の数。
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接続の数。
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接続の数。
6. トラフィックの送信に使用されたポート、Web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Web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。

© 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(/en-us/netscaler-application-delivery-management-software/media/swg-analytics-1.png)

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の概要** ペインが含まれています。**アウトバウンドトラフィックの概要** ペインでは、NetScaler ADM 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の概要** 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。

アウトバウンドトラフィック(/en-us/netscaler-application-delivery-management-software/media/swg-analytics-2.png)

カテゴリをクリックすると、指定され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。
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Web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。

ユーザーダッシュボード(/en-us/netscaler-application-delivery-management-software/media/swg-analytics-3.png)

上位ユーザーペインでユーザーをクリックすると、指定された期間にそのユーザーが実行したWeb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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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Web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。選択された期間が1時間の場合、各凡例は1分間隔で集計され、選択された期間が1日の場合、1時間間隔で集計されます。

ユーザーアクティビティインベスティゲーター(/en-us/netscaler-application-delivery-management-software/media/swg-analytics-4.png)

これらの凡例は集約され、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約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

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
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

   ユーザー トランザクション(/en-us/netscaler-application-delivery-management-software/media/swg-analytics-5.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

概要パネル

概要パネルには、**トランザクション詳細**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。このパネルを使用すると、メトリックを選択または選択解除することで、**トランザクション詳細**ペイン内のトランザクションを並べ替えたり表示したりできます。**概要パネル**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。
バイトアウト	NetScalerアプライアンス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 ADM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 ADM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レピュテーションスコア」を参照してください。次の表は、NetScaler ADMによって割り当てられるリスクスコアについて説明しています。

リスクスコア	説明
1	ユーザーのWebアクティビティに認識された脅威はなく、異常でもありません。
2	ユーザーのWebアクティビティに認識された脅威はなく、異常でもありませんが、ユーザー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リスクスコア	説明
	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ていませんが、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と関連するサイトへのアクセスを試みました。
4	潜在的に侵害されたユーザー。
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**、および**ボット**のカテゴリに基づいた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® ADMでは、次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	スクレーパー
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
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	Cookieハイジャック	フィードフェッチャー
ブライヒェンバッハー攻撃	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワーク	WAF	ボット
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フォルト	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)
	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	ソースIP
	JSONクロスサイトスクリプティング	ホスト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワーク	WAF	ボット
	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ADC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ADC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 ADMは特定の期間の動作を監視し、異常な動作に対する違反を検出します。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。
    - 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ズームのリセットをクリックして、ズーム結果をリセットします。

- 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の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を完全に可視化できるアプリケーションが表示されます。合計違反数、合計WAFおよびボット違反数、国別違反数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、合計WAF違反数、および合計ボット違反数を表示します。

2 – WAFおよびボット違反の詳細を表示します。発生した合計違反数に基づいて上位5つのアプリケーションを表示するには、「**WAF**」タブと「**Bot**」タブをクリックします。すべてのアプリケーションの詳細を表示するには、「**すべて表示**」をクリックします。

3 – 発生回数と適用されたアクションに基づいて、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	BOT
クッキーハイジャック	フィードフェッチャー
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
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	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)
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
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

「**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て、WAFの詳細を表示します。

WAF(/en-us/netscaler-application-delivery-management-software/media/waf-details.png)

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**」の下で、以下を表示できます。

- アプリケーションの総違反数、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。

  WAFグラフ(/en-us/netscaler-application-delivery-management-software/media/waf-graph.png)

  「**View Details**」をクリックして、Application FirewallとNetScaler System Securityの構成の詳細を表示します。

  詳細を表示(/en-us/netscaler-application-delivery-management-software/media/sec-violations.gif)
- 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。

  WAFグラフの詳細(/en-us/netscaler-application-delivery-management-software/media/waf-violation-graph.png)

  「**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。

  ログ(/en-us/netscaler-application-delivery-management-software/media/waf-logs.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- アプリケーションに影響を与えた違反。「**Violation Details**」の下で、影響を受けた違反の詳細を表示できます。各違反をクリックして、次のような詳細を表示します。
  - **What Happened** – 総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、場所などの他の違反詳細を示す地理マップを表示します。

    WAF違反の詳細(/en-us/netscaler-application-delivery-management-software/media/waf-violation-details.png)

ボット違反の詳細を表示

ボットタブから、 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。

- アプリケーションにアクセスしているボットの総数、悪意のあるボットの総数、正常なボットの総数、および人間ユーザーとボットの総比率を示すグラフ。

  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正常なボットか悪意のある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)

  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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。違反の詳細の下で、影響を受けた違反の詳細を表示できます。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。
  - **発生した事象** – 総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や、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が表示されます。

注

WAFと**Bot**では、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。

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機させられ、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枯渇させ、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**：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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
- 不完全なリクエストの合計を**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枯渇させ、**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。

- 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、HTTP POSTヘッダーをターゲットアプリケーションに送信できるサービス拒否攻撃です。ヘッダーでは、本文メッセージの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。ターゲットアプリケーションは待機を余儀なくされ、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。

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スローポスト攻撃を引き起こす可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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ADC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もの）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ADC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すると、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アドレスを特定してブロックします。
- 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 デシンク攻撃

HTTP Desync Attack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であると解釈します。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。悪意のあるクライアントからの最初のクライアントリクエストが悪意のあるデータで処理された場合、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 Attackインジケーターを使用すると、NetScalerインスタンスが次の存在によりHTTP Desync Attackを受けている可能性があるかどうかを分析できます。

- 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されています。

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が表示されます。
- 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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すると、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。
- 仮想サーバー上の誤った暗号化データを持つハンドシェイク接続の合計数を示す、違反の検出メッセージ。

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さなサイズの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すると、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。

管理者として、NetScalerインスタンスがこれらの過剰な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、それ以上の操作は不要です。

「**イベント詳細**」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。棒グラフにマウスカーソルを合わせると、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「セグメントスマックアタック1」(/en-us/netscaler-application-delivery-management-software/media/segment-smack-attack1.png)

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アプライアンスでのSYN攻撃を防ぎます。デフォルトでは、ADC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が高いのは、SYNCOOKIEが無効になっている場合のみです。

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。

「SYNフラッド攻撃」(/en-us/netscaler-application-delivery-management-software/media/syn-flood.png)

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。
- 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可能性のあるサービス拒否 (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。同様の接続をできるだけ多くターゲットマシンに送信することで、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ーを使用すると、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、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IT管理者が監視できるようにします。これは、セキュアなWebトランザクションの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によって実現されます。この可視性により、管理者は以下を評価できます。

- **構成変更が顧客の使用状況に与える影響の判断**: 管理者は、SSLv3の無効化やRC4-MD5のような暗号の削除といった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実行できます。
- **クライアントパフォーマンスの定量化**: 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。
- **アプリケーションセキュリティ**: いずれかのアプリケーションで、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が実行され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 Application Delivery Management (ADM) Analyticsによってログに記録され、表示されます。

SSL Insightは、NetScaler® ADM 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSLフロントエンドおよびバックエンドエラー

注

正常なSSL接続の場合、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を構成する予定の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 ADM>`

   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、ADM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。

- NetScaler ADM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 ADM 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の構成

次の要素を有効にすると、SSL Insightメトリックが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パラメーターを有効にします。

AppFlow機能を有効にする

注

AppFlow機能は、NetScaler ADMまたは各NetScalerインスタンスから有効にできます。

NetScaler ADMからAppFlow機能を有効にするには：

NetScaler ADMが**13.0 Build 41.x以降**の場合：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

   > **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 ADM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 ADMは選択した仮想サーバーで分析を有効にする処理を行います。

NetScaler ADMが**13.0 Build 36.27以前**の場合：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Infrastructure > Instances > NetScaler**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。

   分析を構成する(/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**Application List**を選択します。

      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：Citrixは、転送モードとしてLogstreamを選択することを推奨しています。
   - 「**Web Insight**」を選択し、「**OK**」をクリックします。

     「トランスポートモード」(/en-us/netscaler-application-delivery-management-software/media/logstream.png)

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** をクリックして、**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 ADM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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 次のチェックボックスをオンにします: **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 ADM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、お客様の**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、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、ユーザーをグループに割り当てることができます。NetScaler ADM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Insight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。

NetScaler ADMでSSL Insightメトリックを監視するには:

次のSSLメトリックを表示できます。

- 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**タブを選択し、詳細なメトリックを表示します。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、**アプリケーション**タブと**クライアント**タブをクリックしてSSLメトリックを表示します。

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、SSLコンポーネントを監視するようにNetScaler ADMを構成しているとします。アプリケーションを頻繁に確認

© 1997–2026 Citrix Systems, Inc. All rights reserved.

して、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る必要があるかもしれません。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エラー**と**SSL使用状況**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
- SSL障害 – バックエンド

各タブをクリックして詳細を表示できます。

ユースケース: クライアント向けSSLメトリック

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。

メトリック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メトリックが表示されます。

TCP インサイト

NetScaler Application Delivery Management (ADM) のTCP Insight機能は、データ伝送におけるネットワーク輻輳を回避するためにNetScalerアプライアンスで使用される最適化技術と輻輳制御戦略（またはアルゴリズム）のメトリクスを監視するための、簡単でスケーラブルなソリューションを提供します。この機能は、TCP最適化の有無にかかわらずTCPファイルのダウンロードまたはアップロードパフォーマンスを測定する「TCP Speed Report」機能を使用します。

主要な**トランスポート層メトリクス**（データ量、スループット、速度など）を表示し、その情報を使用してNetScalerインスタンスによって処理されるトラフィック量を測定し、TCP最適化の利点を検証できます。上記のメトリクスについては、ストリームの方向（クライアントからNetScalerへ、NetScalerからオリジンサーバーへ）、TCPポート、および仮想LANごとの内訳が提供されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

TCP Insight機能を構成する前に、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。

- NetScalerインスタンスがソフトウェアバージョン11.1ビルド51.21以降で稼働していること。
- ソフトウェアバージョン11.1ビルド51.21以降で稼働するNetScaler ADMがインストールされていること。
- アプリケーション用に構成されたすべての仮想サーバーが、NetScaler® ADMでの管理および監視のためにライセンスされていること。NetScaler ADMのライセンスについては、ライセンスを参照してください。

TCP Insightの有効化

TCP Insightメトリクスを表示する前に、NetScaler ADMでこの機能を有効にする必要があります。

TCP Insightを有効にするには:

1. Webブラウザで、NetScaler ADM仮想アプライアンスの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。
3. **設定 > 分析設定**に移動し、**分析機能の有効化**をクリックします。
4. **分析機能の有効化**ページで、**TCP Insightの有効化**を選択します。
5. 確認ウィンドウで、**OK**をクリックします。

NetScaler ADMでTCP Insightメトリックを表示する

NetScaler ADMでTCP Insightを有効にすると、トラフィックモード（インターネットまたはモバイルデータ）、データ量、スループット、インターフェース、ポート、平均アップロード速度、平均ダウンロード速度などの主要なトランスポート層情報を表示できます。

NetScaler ADMでTCP Insightメトリックを表示するには：

Infrastructure > TCP Insightに移動します。

棒グラフにマウスポインターを合わせると、対応するトランスポート技術のデータ量を表示できます。また、グラフの下のテーブルでデータ量やその他のメトリックを表示することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

テーブルの設定アイコンを使用して、グラフに表示されるメトリックをカスタマイズできます。また、メトリックが関連する期間を選択し、タイムスライダーを使用して期間を調整することもできます。

TCP Insightリストから選択することで、インターフェース、ポート、ビットレートなどのメトリックも表示できます。

ユースケース

以下のユースケースは、NetScalerアプライアンスでTCP Insightを使用するいくつかの方法を示しています。

- TCP最適化の利点を評価する
- TCPパラメータを調整する
- トラフィック量に対するTCP最適化の影響を測定する

TCP最適化の利点を評価する

NetScalerのTCP最適化は、モバイル（無線）またはエンタープライズネットワーク（インターネット）に実際にどれほどの利益をもたらすでしょうか。TCP経由で行われるデータ転送の速度を表示し、最適化されていないパフォーマンスと最適化されたパフォーマンスを比較できます。これらの測定値は、ダウンロード方向とアップロード方向（常に無線/クライアント側）、および異なる宛先ポート、HTTP（80）とHTTPS（443）について個別に表示されます。 TCP Insightメトリックを調べることで、TCPフローを最適化することによって得られる速度向上を定量化できます。

これらのパラメータの概要を表示するには、NetScaler ADM にログオンし、**TCP Insight** タブをクリックします。次に、**Sides** をクリックし、棒グラフまたはグラフの下の表から **Internet** または **Radio** を選択します。

TCP最適化(/en-us/netscaler-application-delivery-management-software/media/tcp-2.png)

TCPパラメータを調整する

異なるTCPプロファイルを使用すると、同じトラフィックに対して異なる出力が得られる場合があります。このような状況では、NetScalerが異なるTCP最適化プロファイルを実行している期間の速度測定値を表示および比較したい場合があります。この結果を使用して、より高速な伝送のためにTCPパラメータを調整し、特定の顧客ネットワークでユーザーが体感するエクスペリエンスを最大化するTCPプロファイルを開発できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レポートを表示するには、NetScaler ADM にログオンします。次に、**TCP Insight** タブで **Bitrates** をクリックし、棒グラフまたはグラフの下の表から目的のビットレートを選択します。

TCPパラメータ(/en-us/netscaler-application-delivery-management-software/media/tcp-3.png)

トラフィック量に対するTCP最適化の影響を測定する

NetScalerインスタンスによって処理されるIP層のデータ量/スループットの測定値は、異なる期間間で比較でき、TCP最適化が加入者のデータ消費に与える影響を評価できます。測定値は、ネットワークの各側（無線側とインターネット側）、異なるトラフィックセグメント（異なるインターフェースまたはVLANによって区切られる）、各方向（ダウンリンクとアップリンク）、および異なる宛先ポート（HTTPとHTTPS）に対して個別に適用できます。この比較は、TCP最適化が加入者により多くのデータを消費するよう促すことを確認するために使用できます。

測定値の概要については、NetScaler ADM にログオンし、**TCP Insight** タブで **Sides** をクリックし、棒グラフまたはグラフの下の表から **Internet** または **Radio** を選択します。

時間リストから異なる期間を選択することもできます。期間スライダーを使用して期間をカスタマイズできます。

TCPトラフィック量(/en-us/netscaler-application-delivery-management-software/media/tcp-4.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 ADM 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、「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。

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。クリックすると、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® ADM Web Insight ダッシュボード (**アプリケーション > Web Insight**) でレポートが表示されない場合、問題は次のいずれかである可能性があります。

- Web Insight の構成の問題
- NetScaler と NetScaler ADM 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® パラメータの欠落の問題

設定の問題

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でWeb Insightの設定を確認します。
   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仮想サーバーで、バインドされたサービスおよびサービスグループとともに `appflowlog` パラメータを確認します。このパラメータが仮想サーバー、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 ADM間の接続の問題

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コレクタ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 **> >** 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 ADM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. 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」および「NetScalerとNetScaler ADM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、以下のカウンターを確認します。

   - `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ー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ーが欠落している場合は、サポートチームに連絡してください。

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ADM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。仮想サーバーがライセンスされていない場合、NetScaler ADM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ADM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. 設定が別のNetScalerからコピーされていないことを確認してください。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 ADMがAppFlowレコードを処理でき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。

AppFlowパラメータの欠落に関する問題

この問題は、データが欠落しているためにNetScaler ADM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ADM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. 設定が別のNetScalerからコピーされていないことを確認してください。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 ADMがAppFlowレコードを処理できなくなる可能性があります。
4. NetScalerで次のAppFlowパラメータ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て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破棄されたAppFlowレコード。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

この機能を使用すると、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、ADC、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

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。このようなトランザクションの場合、NetScaler ADMはRTT値を次のように表示します。

- **NA** – ADC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** – ADCインスタンスがRTTを0ミリ秒から1ミリ秒の間の小数で計算する場合に表示されます。例: 0.22ミリ秒。

次の**トランザクションサマリー**にアクセスできます。

- **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インスタンスとサーバーからのRTTや処理時間などの詳細を表示できます。

次の例は、問題がサーバーに起因す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。

特定の期間のトランザクションを表示するために、ドラッグして選択することもできます。

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。

イベントの表示(/en-us/netscaler-application-delivery-management-software/media/view-event.png)

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。

詳細なトランザクション(/en-us/netscaler-application-delivery-management-software/media/detailedevent.png)

SSLエラーがある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

  SSL(/en-us/netscaler-application-delivery-management-software/media/ssl-detailed-metrics.png)

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**と**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。

トランザクションの概要(/en-us/netscaler-application-delivery-management-software/media/transactionsummary.png)

- **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。例: Windows
- **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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。
- **フロントエンドSSL暗号強度**: SSL証明書のキーサイズ（高、中、低など）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証明書の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**: SSL証明書のキーサイズ（高、中、低など）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証明書の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**: サーバーが使用する証明書の種類。例: RSA、DSA、ECDSA、DH。

イベントリストに列を追加

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。検索の焦点を絞り込むために、検索クエリで演算子を使用することもできます。

検索クエリに使用できる演算子は次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

演算子	説明	例	出力
=	ある値と等しい	仮想サーバー = テスト	「test」という名前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	アプリ応答時間が500ミリ秒を超えるアプリケー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 >= 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 <= 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、300バイト未満の合計バイト数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。

   例](/en-us/netscaler-application-delivery-management-software/media/example1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

   例](/en-us/netscaler-application-delivery-management-software/media/example2.png)

3. 値300を入力します。

4. 期間を選択し、**検索**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。

   検索結果が表示されます。

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、**保存**をクリックします。

- 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。

- 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、**削除**をクリックします。

  また、ブックマークアイコンをクリックして**削除**をクリックすることもできます。

データのエクスポート

選択した期間のWebトランザクション分析データは、**Export**アイコンをクリックして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。**Export**オプションを使用すると、次のいずれかを実行できます。

- **Export Now**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。
- **Schedule Export**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セットアップ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 ADM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 ADM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 ADMとKubernetesクラスター）。
- NetScaler ADM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、(/ja-jp/netscaler-application-delivery-management-software/13-1/deploy/multisite-deployment.html)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® ADM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 ADMとNetScaler CPX間の通信を有効にするために、NetScaler ADMで(#configure-static-routes-in-citrix-adm)を構成済みであること
- (#download-the-sample-deployment-files-from-github)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 ADMへのCPXの登録を成功させるために、(#add-parameters-in-cpx-yaml-file)に必要なパラメーターを追加済みであること。
- NetScaler ADMに(#add-kubernetes-cluster-in-citrix-adm)を追加済みであること。
- (#deploy-a-sample-microservice-application)を展開済みであること。
- (#deploy-cpx-and-register-cpx-in-adm)を展開し、CPXをADMに登録済みであること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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。
- 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 ADM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 ADM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 ADMとKubernetesクラスター）。
- NetScaler ADM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設定し、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 ADM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 ADMとNetScaler CPX間の通信を有効にするために、NetScaler ADMで静的ルートを設定済みであること
- 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 ADMへのCPX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を追加済みであること。
- NetScaler ADM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ADMに登録済みであること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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。
- 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。
- **Istream.conf** ファイルを更新し、NetScaler エージェントが TCP メトリックを取得できるように TCP 設定を **All** に変更しました。

NetScaler ADM 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 ADM から Kubernetes クラスターへの通信を有効にするには、NetScaler ADM 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ポッド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 ADM 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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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

4. これらのルートコマンドを `/mpsconfig/svm.conf` ファイルに追記します。

   a. NetScaler ADM 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 からサンプル展開ファイルをダウンロードする

1. マスターノードで GitHub 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は、ADM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は、**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 ADMへのCPX登録を確実にするには、`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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"

  value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

- name: "NS_HTTP_PORT"

  value: "9080"

- name: "NS_HTTPS_PORT"

  value: 9443"

- name: "NS_MGMT_USER"

  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – NetScaler ADMのIPアドレスを示します

  注

  ADMエージェントが使用されている場合、これはオンプレミスエージェントのIPアドレスを示します。

- **NS_MGMT_FINGER_PRINT** – NetScaler ADM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 ADM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、**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** – CPXからADMにログデータを転送するために**Logstream**プロトコルを有効にする必要があるNetScalerエージェントのIPアドレスを示します

NetScaler ADM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 ADCインスタンスの分析を取得するには、NetScaler ADM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、**追加**オプションをクリックします。詳細については、NetScaler ADM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 ADM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 ADM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. **追加**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。

© 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.」**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 ADM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、:

   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. `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>`を実行して、クラスターロールをサービスアカウントにバインドします。

   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. `kubectl describe sa <name>`を実行してトークンを表示します。

   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.

トークンを生成(/en-us/netscaler-application-delivery-management-software/media/sg-generate-token.png)

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に追加したの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。

クラスターを追加(/en-us/netscaler-application-delivery-management-software/media/add-cluster.png)

サンプルマイクロサービスアプリケーションの展開

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、ADM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。

ライセンス付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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADMにKubernetesクラスターを追加した後、ライセンス付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。サービスグラフ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構成**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。

   TCP(/en-us/netscaler-application-delivery-management-software/media/tcp-setting-citrix.png)
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 ADMでサービスグラフを生成するために、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。

   NodePort(/en-us/netscaler-application-delivery-management-software/media/sg-nodeport.png)
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

NetScaler® ADM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アドレスを直接使用して通信を確立することはできません。NetScaler ADMからKubernetesクラスターへの通信を有効にするには、NetScaler ADM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 ADM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:

   ```
   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 ADM 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します

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に、ADM エージェント資格情報を持つ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 チャートで構成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	任意または必須 (HELM)
citrixCPX	NetScaler CPX	FALSE	NetScaler CPX に必須

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明	デフォルト	任意または必須 (HELM)
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 ADM IP アドレス	ヌル	NetScaler CPXには必須
ADMSettings.ADMFingerPrint	NetScaler ADMのフィンガープリント。**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) の条項。はいの場合、ユーザーはEULAの条項に同意します。	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チャートで構成可能なパラメーターとそのデフォルト値を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター	説明	デフォルト値
ADMSettings.ADMIP	NetScaler ADMのIPアドレス	NIL
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) の条項。はいの場合、ユーザーは EULA の条項に同意します。	いいえ
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。	はい

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`

   ステップ 3 と 5 を実行すると、NetScaler CPX が NetScaler ADM 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を展開する

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

任意のユーザー名とパスワードを指定できます。

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   注

   任意のユーザー名とパスワードを指定できます。

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 agent IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   注

   ADMフィンガープリントとADMエージェントまたはADM IPアドレスを指定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

   ADMフィンガープリントとADMエージェントまたはADM 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 ADM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 ADM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 ADM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、次の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にクラスター全体のアクセス権が付与されます。

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。

d. リストからエージェントを選択します。

注

ADM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 ADM 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。サービスグラフ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. **>** に移動します。
2. で、 と 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、 と を に変更します。

1. **>** に移動します。

   ページが表示されます。
2. をクリックします。
3. で、 を選択します。
4. で、 を選択します。

5. 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 ADMに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. イングレスIPとポートを特定する

   ```
   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。

サービスグラフを使用すると、メトリック、エラーなどのさまざまなサービス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。

NetScaler® テレメトリープログラムのオプションのテレメトリーデータ

NetScaler Console の機能使用状況

次の表は、NetScaler テレメトリープログラムの一部として収集されるオプションデータのリストを示しています。

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
展開	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_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 の展開が Kubernetes クラスター内にあるかを確認します
is_dr	災害復旧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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
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
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	Virtual Desktop を介して接続されているユーザー数
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
adm_analyt_vpn_users	VPN を介して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
異常インサイト	lb または cs 仮想サーバーでリクエスト機能が有効になっているかどうかを示します
数	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	負荷分散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分析機能

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
機能	VPN仮想サーバーで有効になっている分析機能
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（はいまたはいいえ）
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ユーザーがいるかどうかを示します
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	LBまたはCS仮想サーバーでセキュリティインサイトが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、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
	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
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	エージェントプラットフォームの種類
agt_pl_citrix_hypervisor	エージェントプラットフォームの種類
agt_pl_docker	エージェントプラットフォームの種類
agt_pl_esx	エージェントのプラットフォームタイプ
agt_pl_hyper_v	エージェントのプラットフォームタイプ
agt_pl_gcp	エージェントのプラットフォームタイプ
agt_pl_kvm	エージェントのプラットフォームタイプ
agt_pl_kubernetes	エージェントのプラットフォームタイプ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
agt_pl_unknown	エージェントのプラットフォームタイプ
agt_pl_aws	エージェントのプラットフォームタイプ
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
total_active_agents	UP状態のエージェントの総数
total_agents	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
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のディスク領域の総量（単位: バイト）
使用済み	NetScaler Consoleの使用済みディスク領域の総量
空き	NetScaler Consoleの利用可能なディスク領域の総量
total_api_requests	過去24時間におけるNetScaler ConsoleへのAPI経由のリクエスト総数。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を介したNetScaler Consoleへの合計リクエスト数
total_gui_requests	過去24時間にNetScaler Console GUIにログインした合計ユーザー数
total_users	NetScaler Consoleのローカルユーザーの合計数
total_config_audit	NetScaler Consoleで設定されたConfig Auditテンプレートの合計数
total_config_job	NetScaler Consoleで作成されたConfigジョブの合計数
total_ssl_certs	NetScaler Consoleで作成/変更/削除されたSSL証明書の合計数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
total_custom_event_rules	NetScaler Consoleで作成されたカスタムイベントルールの合計数
total_event_rules	NetScaler Consoleで作成されたイベントルールの合計数
total_ingress_deployed	Kubernetes内の合計イングレスコントローラー。
total_ipam	NetScaler Consoleに追加された合計IPAMプロバイダー
total_ipam_configured	NetScaler Consoleに追加された合計IPAMネットワーク
total_network_report	NetScaler Consoleで作成された合計ネットワークレポート
total_pager_duty_profile	NetScaler Consoleに追加された合計PagerDutyプロファイル
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で構成された合計RBACグループ
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から作成/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
設定パック	StyleBooksから保存された設定パックの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
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

NetScaler® テレメトリープログラムに必要なテレメトリーデータ

以下の表は、NetScaler テレメトリープログラムの一部として収集される必須データのリストを示しています。

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。

ライセンス

パラメータ	説明
flex_vpx_inst_entitled	資格のあるVPXインスタンスの合計
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	資格のある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	合計付与MPXインスタンス
flex_mpx_inst_allocated	合計割り当て済みMPXインスタンス
flex_plt_bw_entitled	付与されたプラチナ帯域幅
flex_plt_bw_allocated	割り当てられたプラチナ帯域幅
flex_ent_bw_entitled	付与されたエンタープライズ帯域幅

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
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	付与された標準帯域幅
flex_std_bw_allocated	割り当てられた標準帯域幅
flex_vpx_fips_inst_entitled	付与された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
license_name	ライセンスの種類または機能名
peak_license_usage	NetScalerインスタンスに適用されたライセンスのピーク使用量（割り当て）
peak_bandwidth_usage	NetScalerインスタンスからのピーク使用量
avg_license_usage	NetScalerインスタンスに適用されたライセンスの平均使用量（割り当て）
avg_bandwidth_usage	NetScalerインスタンスからの平均使用量
license_edition	Platinum/Enterprise/Standard帯域幅
機能名	ライセンス機能名
ホストID	デバイスのホストID
ライセンスシリアル番号	ライセンスのシリアル番号
ライセンス開始日	ライセンスの開始日
ライセンス終了日	ライセンスの終了日
ライセンスSA日付	ライセンスサブスクリプションアドバンテージ日付
テナントNSライセンスタイプ	CPL、CULなどのライセンスの種類
instance_id	インスタンスの一意の識別子

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
instance_mode	インスタンスがスタンドアロンかHAペアかを確認します
instance_state	インスタンスのステータス（稼働中/停止中）
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
is_pooled_license	ライセンスがプールライセンスであるかを確認します
license_edition	ライセンスの種類（Platinum/Standard/Enterprise）
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	デバイスの種類
plt_license_allocation	プラチナ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
ent_license_allocation	エンタープライズライセンスの割り当て
NSライセンスタイプ	ライセンスの種類（FlexedまたはFixed）
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（管理対象および管理対象外の両方）
perc_discovered_vservers	検出/付与された仮想サーバーの割合
perc_used_vservers	使用済み/付与済み仮想サーバーの割合
pool_cpxvcpu_entitled	付与されたプールCPX vCPUの合計
pool_cpxvcpu_used	使用されたプールCPX vCPUの合計
pool_entbw_entitled	付与されたプールEnterprise帯域幅の合計[MBps]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
pool_entbw_used	使用されたプールEnterprise帯域幅の合計 [MBps]
pool_entvcpu_entitled	付与されたプールEnterprise vCPUの合計
pool_entvcpu_used	使用されたプールEnterprise vCPU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	使用済みプールFIPSインスタンスの合計
pool_instances_entitled	付与されたプールインスタンスの合計
pool_instances_used	使用済みプールインスタンスの合計
pool_perc_bw_used	使用済み帯域幅の割合（%）
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（%）
pool_pltbw_entitled	付与されたプールPlatinum帯域幅の合計 [MBps]
pool_pltbw_used	合計プールプラチナ帯域幅使用済み [MBps]
pool_pltvcpu_entitled	合計プールプラチナvCPU割り当て済み
pool_pltvcpu_used	合計プールプラチナvCPU使用済み
pool_stdbw_entitled	合計プール標準帯域幅割り当て済み
pool_stdbw_used	合計プール標準帯域幅使用済み
pool_stdvcpu_used	合計プール標準vCPU使用済み
total_discovered_vservers	検出された仮想サーバーの合計
total_entitled_vservers	割り当てられた仮想サーバーの合計
total_used_vservers	使用済み仮想サーバーの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway の機能使用状況

以下のデータテレメトリは、NetScaler Gateway のオンプレミスバージョンが **14.1-25.53 以降** / **13.1-53.22 以降** のビルドである場合にのみ収集されます。

パラメータ	説明
accessMode	アクセスモードの種類。例: ICA、VPN
bytesTransferred	セッションごとに送受信された合計バイト数
epaScans	EPAスキャンの合計数
機能	NetScaler Gateway で有効になっている機能
id	使用イベントの一意の識別子
製品	使用イベントの発生元製品と展開の識別
prodVer	Gateway製品のバージョン
メール	Gatewayユーザーのメールアドレス（メールアドレスはハッシュ化されます）*
st	取得されるデータの現在時刻
タイプ	CASが管理対象Gatewayの使用イベントを識別するために使用するイベントタイプ
userName	Gatewayのユーザー名。注：名前はハッシュ化されます*。
バージョン	テレメトリイベントのバージョン

NetScalerの展開

パラメータ	説明
total_active_managed_devices	UP状態にあるNetScalerインスタンスの総数
total_nsap_device	NetScaler Console内の管理者パーティションインスタンスの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
total_managed_devices	NetScaler Console内の管理対象NetScalerインスタンスの総数
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)
dev_pl_aws	デバイスプラットフォームのタイプ
dev_pl_azure	デバイスプラットフォームの種類
dev_pl_citrix_hypervisor	デバイスプラットフォームの種類
dev_pl_esx	デバイスプラットフォームの種類
dev_pl_gcp	デバイスプラットフォームの種類
dev_pl_hyper_v	デバイスプラットフォームの種類
dev_pl_kvm	デバイスプラットフォームの種類
dev_pl_unknown	デバイスプラットフォームの種類
dev_pl_vpx_on_sdx	デバイスプラットフォームの種類
total_blx_device	NetScaler Console on-premで管理されているBLX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_ng_device	NetScaler Consoleで管理されているGatewayインスタンスの総数
total_ngvpx_device	NetScaler Consoleで管理されているGateway VPXインスタンスの総数
total_ns_device	NetScaler Consoleで管理されているMPXインスタンスの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
total_nssdx_device	NetScaler Consoleで管理されているSDXインスタンスの総数
total_nsvpx_device	NetScaler Consoleで管理されている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
device_id	VPXインスタンスの一意のID
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
状態	VPXインスタンスの現在のステータス (UPまたはDown)
aaa_vservers	AAA仮想サーバーの総数
cs_vservers	コンテンツスイッチング仮想サーバーの総数
gslb_vservers	GSLB仮想サーバーの総数
lb_vservers_http	HTTP LB仮想サーバーの総数
lb_vservers_ssl	SSL仮想サーバーの総数
バージョン	NetScalerインスタンスのビルドバージョン

NetScaler機能の使用状況

パラメータ	説明
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
aaa_as_Request_tot_blocked	AAAのappfwプロファイルによってブロックされたHTTPリクエストの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
aaatm_as_Request_tot_blocked	AAATM向けにappfwプロファイルによってブロックされたHTTPリクエストの合計数
バージョン	NextGen APIのバージョン
as_Requests_aaatm_lb	aaatm_lbモジュールに代わってappfwモジュールによって処理されたHTTPリクエストの合計数
as_Requests_vpn	vpnモジュールに代わってappfwモジュールによって処理されたHTTPリクエストの合計数
nsapisec_builtin_tot_hits	Project Shield向けの組み込みAPIセキュリティスキーマからの合計数
nsapisec_builtin_tot_validated_success	Project Shield向けの組み込みAPIセキュリティスキーマを正常に通過したリクエストの合計数
svpn_as_Request_tot_blocked	VPN向けにappfwプロファイルによってブロックされたHTTPリクエストの合計数
appfw.appfirewallrequests	appfwプロファイルを介したWAFリクエストの合計数
appfw.appfirewallrequestsrate	appfwプロファイルを経由するWAFリクエストの総レート
appfwprofile.appfw_block	プロファイルごとにブロックされたものの総数
appfwprofile.appfw_bypass	プロファイルごとに渡されたリクエストの総数
appfwprofile.appfw_drop	プロファイルごとにドロップされたものの総数
appfwprofile.appfw_reset	プロファイルごとにリセットされたものの総数
ボットリクエスト	appfwプロファイルを経由するボットリクエストの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
bot_signature_version	使用されているボットシグネチャのバージョン
ボットリクエストレート	ボットプロファイルを通じたボットリクエストのレート
waf_signature_version	使用されているWAFシグネチャのバージョン
waf.as_requests	デフォルトプロファイルも含む、すべてのWAFプロファイルを通じて行われたリクエストの総数
waf.as_req_bytes	デフォルトプロファイルを除外した、すべてのWAFプロファイルを通じて行われたリクエストの総数
ingress_controllers	イングレスコントローラーの総数
admin_partitions	パーティションの総数
gslb_site_tot_RequestBytes	GSLBプロファイルを通じて渡されるリクエストの合計バイト数
gslb_site_tot_Requests	GSLBプロファイルを通じて渡されるリクエストの総数
gslb_sites	gslbサイトの総数
gslb.services	gslbサービスの総数
analytics.profile	アナリティクスプロファイルの総数
appfw.policies	AppFlowポリシーの総数
appfw.profiles	AppFlowプロファイルの総数
bot.policies	Botポリシーの総数
bot.profiles	Botプロファイルの総数
カテゴリ	デバイスの分類。例: Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
cluster.nodes	クラスターノードの総数
cr	キャッシュリダイレクション仮想サーバーの総数
cs.all	コンテンツスイッチング仮想サーバーの総数
cs.gw	ゲートウェイとして使用されるコンテンツスイッチング仮想サーバーの総数
cs.used	localhostにバインドされておらず、WEBまたはTCPプロトコルであるアドレス指定可能なコンテンツスイッチング仮想サーバーの総数
deployment_type	NetScalerの展開タイプ (HAペアまたはスタンドアロン)
ha.node	HAペアのIPアドレス。注: IPアドレスはハッシュ化されます*。
lb.all	すべてのロードバランス仮想サーバーの総数
lb.gw	ゲートウェイとして使用されるロードバランス仮想サーバーの総数
lb.used	localhostにバインドされておらず、WEBまたはTCPプロトコルであるアドレス指定可能なロードバランス仮想サーバーの総数
エヌエスアイピー	NetScalerのNSIP。注: IPアドレスはハッシュ化されます*。
理由	分類に関する詳細な理由
サーバー	仮想サーバーの総数
serviceGroups	サービスグループの総数
サービス	サービスの総数
services.dns	ADNS/ADNS_TCPタイプのサービスの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
VPN	VPN仮想サーバーの総数
vpn.ica	ICA VPN仮想サーバーの総数
vservers.gw	ゲートウェイとして使用されるLB + CS + CR仮想サーバーの総数
vservers.used	localhostにバインドされておらず、WEBまたはTCPプロトコルであるアドレス指定可能なLB + CS + CR仮想サーバーの総数
waf_protection	WAF保護タイプ
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_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_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_icaproxy_devices	HDX Insightが有効になっているNetScalerインスタンスの総数
iprep_cur_ip_count	IPレピュテーションヒット数
total_gslb_devices	グローバルサーバー負荷分散仮想サーバーが構成されている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
total_lb_devices	負荷分散仮想サーバーが構成されているNetScalerインスタンスの総数
total_lb_devices_http	ロードバランシング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	ロードバランシングSSL仮想サーバーで構成された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
telemetry_collected_at	テレメトリースクリプトが実行された時刻
状態	VPXインスタンスの現在のステータス（稼働中または停止中）
exp.events	イベントのエクスポートに使用されるアナリティクスプロファイルの総数
exp.managementlogs	管理ログのエクスポートに使用されるアナリティクスプロファイルの総数
exp.metrics	メトリックのエクスポートに使用されるアナリティクスプロファイルの数
exp.auditlogs	Splunkへの監査ログのエクスポートに使用されるアナリティクスプロファイルの数
exp.prometheus	Prometheusへのエクスポートに使用されるアナリティクスプロファイルの数
telemetry_collected_at	テレメトリースクリプトが実行された時刻
状態	VPXインスタンスの現在のステータス（UpまたはDown）
バージョン	デバイスのビルドバージョン
exp.events	イベントのエクスポートに使用されるアナリティクスプロファイルの総数
exp.managementlogs	管理ログのエクスポートに使用されるアナリティクスプロファイルの総数
exp.metrics	メトリクスのエクスポートに使用されるアナリティクスプロファイルの数
exp.auditlogs	Splunkへの監査ログのエクスポートに使用される分析プロファイルの数
exp.prometheus	Prometheusへのエクスポートに使用される分析プロファイルの数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
gw_hdx_insights	HDX InsightとGateway Insightのエクスポートが有効になっているかどうか
collected_at	テレメトリースクリプトがデータを収集した時刻
total_audit_logs	NextGen APIを介して構成された監査ログの総数
total_backends	NextGen APIを介して構成されたバックエンドの総数
total_frontends	NextGen APIを介して構成されたフロントエンドの総数
total_health_check	NextGen APIを介して構成されたhealth_checkリソースの総数
total_http_redirects	NextGen APIを介して構成されたHTTPリダイレクトの合計数
total_http_responders	NextGen APIを介して構成されたHTTPレスポンダーの合計数
total_load_balancing_settings	NextGen APIを介して構成された負荷分散設定の合計数
total_routes	NextGen APIを介して構成されたルート（ポリシー）の合計数
total_tls_settings	NextGen APIを介して構成されたTLS設定の合計数
total_http_settings	NextGen APIを介して構成されたHTTP設定の合計数
total_value_set	NextGen APIを介して構成された値セットの合計数
total_wireshark_expressions	NextGen API を介して設定するために使用された Wireshark フィルターの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
last_login_time	NextGen API を使用したユーザーの最終ログインのタイムスタンプ
last_usage_time	NextGen API を使用したユーザーの最終インタラクションのタイムスタンプ
ngapi_version	NextGen API のバージョン
状態	現在の NextGen API ステータス
total_applications	NextGen API を介して設定されたアプリケーションの総数
total_certificates	NextGen API を介してインストールされた証明書の総数
total_failed_commit	コミット段階で失敗した NextGen API リクエストの総数
total_failed_install	インストール段階で失敗したNextGen APIリクエストの総数
total_login	NextGen APIインターフェイスへのログイン総数
total_request	NextGen APIインターフェイスを介して行われたリクエストの総数
total_resources	NextGen APIを介して構成されたNextGen APIリソース（アプリケーション、証明書、ヘルスチェックなど）の総数
svpn_tot_client_type_AGENT	Windows用Citrix Secure Accessクライアントの総数
svpn_tot_client_type_IOS	iOS用Citrix Secure Accessクライアントの総数
svpn_tot_client_type_MAC	macOS用Citrix Secure Accessクライアントの総数
svpn_tot_client_type_ANDROID	Android用Citrix Secure Accessクライアントの総数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明
svpn_tot_client_type_CVPN	クライアントレスVPNを介してCitrixリソースにアクセスするユーザーまたはデバイスの総数
svpn_tot_client_type_ICA	ICAアクセス用Citrix Secure Accessクライアントの総数
ns_svpn_tot_epa_failed	失敗したEPAチェックの総数
ns_svpn_tot_epa_quarantine	検疫を伴って失敗したEPAチェックの総数

*テレメトリを通じて収集される情報（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、論理的なアセットマッチングの目的でのみ使用されます。

データガバナンス

Citrixは、NetScaler® Application Delivery Management (ADM) の展開に関する統計情報を収集し、展開の使用状況と規模を把握しています。この統計情報には、お客様のオンプレミス環境におけるADM展開の健全性、ステータス、および使用パターンが含まれます。この統計情報は、Citrixがお客様のADM展開に関す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のに役立ちます。

- **Citrix Cloud™ で顧客IDを作成する** - オンプレミスADM展開から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情報をCitrix Cloudアカウントに送信するため。

  顧客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、オンプレミスADMとADMサービス間の接続を確立します。「顧客IDの構成」を参照してください。(#configure-customer-identity).
- **メンテナンススクリプトを構成する** - データベースを最適化するため。データベースの最適化では、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。メンテナンススクリプトの構成には、同じ「Cloud Connect」機能が使用されます。「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」を参照してください。(#database-optimization-using-maintenance-scripts).
- **顧客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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クスペリエンスを最適化できます。「顧客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。(#customer-user-experience-improvement-program).

顧客IDの構成

NetScaler Application Delivery Management (ADM) では、情報への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ます。詳細については、Citrix Cloudにサインアップするを参照してください。

NetScaler ADMで認証を行うにはさまざまな方法があります。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**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。

   顧客IDの構成ページが開き、Citrix Cloud資格情報で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、Citrix Cloudをクリックして登録してください。
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。

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、Citrix Cloudをクリックして登録してください。
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、「Submit」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。

診断とデータ収集

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。
  - 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ADC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。
  - ユーザー定義のスタイルブックの総数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理されている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、災害復旧、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、次のことに役立ちます:

- 適切なNetScaler ADMのサイジングと展開を推奨する。
- 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。

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。お客様の要求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/使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、法律で義務付けられているか許可されている期間、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。これを行うには、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改善プログラム

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改善プログラム (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すべてです。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、特定の機能でのクリック数まで、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。

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の検索機能。
- アプリ内からアンケートに参加して、製品の改善に協力する。
- 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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を無効にする方法?

CUXIPを無効にするには、ADM GUIで次の操作を行います。

1. **Settings > System Administration**に移動します。
2. **CUXIP Settings**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。

このプライバシーポリシーは、変更がないか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/>`

HAペアでのNetScaler® ADM構成のバックアップと復元

NetScaler Application Delivery Management (ADM) の現在の構成をバックアップできます。NetScaler ADM の HA 展開では、どちらかのサーバーから NetScaler ADM 構成をバックアップおよび復元できます。ロードバランシング仮想サーバー IP アドレスを使用してバックアップを取得する場合、バックアップファイルはどちらかのサーバーに保存でき、手動で確認する必要があります。

1つのノードのみがアクティブな状態で復元する場合、または復元中にフェールオーバーが発生した場合、復元プロセスは完了に失敗します。

NetScaler ADM 構成をバックアップするには:

1. **システム** \> **詳細設定** \> **バックアップファイル** に移動し、**バックアップ** 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、**ファイルをパスワードで保護** チェックボックスを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バックアップファイルから NetScaler ADM 構成を復元するには:

1. **システム** \> **詳細設定** \> **バックアップファイル** に移動します。
2. 復元したいバックアップファイルを選択し、**復元** をクリックします。

システムバックアップ設定を構成するには:

1. **システム** \> **システム管理** に移動します。**バックアップ設定** の下にある **システムバックアップ設定** をクリックします。
2. **システムバックアップ設定の構成** ページで、以下を指定します。
   - 保持するバックアップの数。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します。
   - 外部転送を有効にします。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 ADMサーバーにアップロードし、その後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 ADM 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。

   システムバックアップの構成(/en-us/netscaler-application-delivery-management-software/media/system-backup-settings-ha.png)

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® Application Delivery Management (ADM) を設定して、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 ADMにログオンしようとしてログオン試行が失敗した場合に、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADM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 ADM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
ライセンス	ライセンスの適用に失敗しました

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カテゴリ	原因
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の値が制限を超過しました
PerfCounterThresholdNormal	パフォーマンスカウンタの値は正常です
PolicyFailed	システムポリシーのいずれかが失敗しました
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

ジオマップのサイトを構成する

NetScaler Application Delivery Management (ADM) サイトは、特定の地理的場所に存在するCitrix Application Delivery Controller (ADC) インスタンスの論理的なグループです。サイト内には複数のNetScalerインスタンスを配置でき、それらはNetScaler ADMサーバーによって監視および管理されます。NetScaler ADMサーバーを使用して、syslog、AppFlow、SNMPなどのデータを管理対象インスタンスから管理できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サイトを作成するには：

1. 「**Infrastructure > Instances > Sites**」に移動し、「**Add**」をクリックします。
2. 「**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。

   c. **サイト名**：サイトの名前を入力します。
   d. **都市**：都市を入力します。
   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**: 国を入力してください
   h. **緯度**: 場所の緯度を入力してください。
   i. **経度**: 場所の経度を入力してください。
3. **作成**をクリックします。

   サイトを作成(/en-us/netscaler-application-delivery-management-software/media/createsite.png)

NetScalerインスタンスをNetScaler ADMに追加する方法の詳細については、NetScaler ADMへのインスタンスの追加を参照してください。

© 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.