NetScaler® Console サービス

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

Contents

概要 65

NetScaler Consoleの仕組み 66

機能とソリューション 66

リリースノート 71

新機能 71

September 27, 2026 71

管理と監視 71

September 15, 2026 75

修正された問題 75

September 01, 2026 76

新機能 76

修正された問題 78

August 19, 2026 79

管理と監視 79

August 04, 2026 80

新機能 80

修正された問題 80

July 14, 2026 81

新機能 81

修正された問題 82

June 30, 2026 83

管理と監視 83

June 17, 2026 86

修正された問題 86

June 03, 2026 87

修正された問題 87

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

May 19, 2026 87
管理と監視 87
修正された問題 92
March 31, 2026 93
管理と監視 93
修正された問題 94
March 23, 2026 95
管理と監視 95
March 09, 2026 96
新機能 96
修正された問題 97
February 20, 2026 98
新機能 98
修正された問題 98
February 04, 2026 99
その他 100
修正された問題 101
November 11, 2025 102
管理と監視 102
November 06, 2025 103
修正された問題 103
October 15, 2025 103
管理と監視 103
修正された問題 104
September 17, 2025 104
インフラストラクチャ 104
修正された問題 105
September 08, 2025 106

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

ライセンス 106
September 03, 2025 108
修正された問題 108
August 26, 2025 108
管理と監視 108
August 20, 2025 110
インフラストラクチャ 110
修正された問題 110
July 17, 2025 111
インフラストラクチャ 111
修正された問題 111
July 02, 2025 111
テレメトリ 111
セキュリティ 112
修正された問題 113
June 25, 2025 113
管理と監視 113
June 17, 2025 114
管理と監視 114
June 03, 2025 115
修正された問題 115
May 26, 2025 115
分析 115
修正された問題 116
May 06, 2025 117
修正された問題 117
April 15, 2025 117
ゼロタッチ証明書展開 117

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

パブリッククラウドにおけるNetScalerインスタンスのオートスケーリングの廃止 118
構成ジョブの改善 118
アップグレードジョブの改善 118
修正された問題 118
February 19, 2025 119
StyleBooks 119
修正された問題 119
分析 119
February 06, 2025 119
分析 119
インフラストラクチャ 120
修正された問題 120
January 15, 2025 120
テレメトリ 120
分析 121
インフラストラクチャ 121
StyleBook 122
修正された問題 122
December 03, 2024 123
移行された構成間での構成エンティティの共有 123
分析をポリシーベースからプロファイルベースの構成へ移行する 123
修正された問題 124
November 20, 2024 124
NetScaler Console GUIのユーザーエクスペリエンスの向上 124
NetScalerからSSL証明書を削除するオプション 125
修正された問題 125
November 12, 2024 126
管理と監視 126

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

October 15, 2024 127
テレメトリ 127
分析 127
修正された問題 127
インフラストラクチャ 128
October 03, 2024 128
ライセンス 128
StyleBook 128
注意事項 129
修正された問題 129
September 19, 2024 129
インフラストラクチャ 129
修正された問題 130
September 03, 2024 131
可観測性 131
修正された問題 131
August 27, 2024 131
分析 131
アプリケーション 132
StyleBook 132
修正された問題 132
July 25, 2024 133
修正された問題 133
July 15, 2024 134
インフラストラクチャ 134
ライセンス 134
修正された問題 134
July 09, 2024 135

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

CVE-2024-5491およびCVE-2024-5492の特定と修正のサポート 135
June 18, 2024 136
テレメトリ 136
June 11, 2024 136
分析 136
インフラストラクチャ 138
修正された問題 138
June 5, 2024 139
分析 139
プラットフォーム 139
StyleBook 139
修正された問題 140
アナリティクス 140
インフラストラクチャ 140
StyleBook 140
May 22, 2024 141
分析 141
ライセンス 141
StyleBooks 142
修正された問題 142
April 23, 2024 142
分析 142
インフラストラクチャ 143
修正された問題 143
インフラストラクチャ 143
ライセンス 143
セキュリティ 143
April 10, 2024 144

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

分析 144
インフラストラクチャ 144
修正された問題 144
インフラストラクチャ 144
ライセンス 145
セキュリティ 145
March 26, 2024 145
修正された問題 145
March 12, 2024 146
ライセンス 146
修正された問題 146
February 28, 2024 147
インフラストラクチャ 147
分析 148
StyleBook 148
修正された問題 149
February 06, 2024 150
アナリティクス 150
インフラストラクチャ 150
修正された問題 151
January 24, 2024 152
分析 152
インフラストラクチャ 152
修正された問題 152
January 16, 2024 152
CVE-2023-6548およびCVE-2023-6549の特定と修復のサポート 152
January 09, 2024 153
分析 153

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

インフラストラクチャ 154

修正された問題 155

ライセンス 155

既知の問題 155

ライセンス 155

管理と監視 156

インフラストラクチャ 156

データコンプライアンス 158

PCI DSS コンプライアンス 158

NetScaler® Application Delivery Managementサービス PCI DSSコンプライアンス 158

NetScaler® テレメトリプログラム 159

前提条件 159

データガバナンス 162

NetScaler®テレメトリプログラム 162

データの収集、保存、送信方法? 162

データカテゴリ 163

顧客コンテンツ 163

ログ 163

詳細な顧客コンテンツとログ 164

セキュリティ 166

NetScaler Console Serviceのデータ保持ポリシー 166

サードパーティサービス 167

参照 168

IoC情報の利用条件 169

はじめに 170

ステップ1：Citrix Cloud™ にサインアップする 170

ステップ2：Express アカウントで NetScaler Console を管理する 170

ステップ 3: NetScaler 展開タイプを選択する 171

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

ハイパーバイザーにエージェントをインストールする 172
パブリッククラウドに外部VMエージェントをインストールする 173
マイクロサービスとしてエージェントをインストールする 174
組み込みエージェントを使用する 174
インスタンスの追加 174
NetScaler Console GUIダッシュボードを使用してNetScalerインスタンスをオンボードする 175
エージェントのアクション 175
エージェントの診断を表示し、エンドポイント検証のアラートを受信する 176
メール通知 177
インスタンスを管理するように組み込みエージェントを構成する 177
前提条件 178
組み込みエージェントの構成 178
NetScaler®組み込みエージェントを介したライセンスサーバーの構成 181
トラブルシューティング 182
オンプレミスにNetScalerエージェントをインストールする 182
Microsoft AzureクラウドにNetScalerエージェントをインストールする 184
前提条件 185
Amazon Web Services (AWS) に NetScaler エージェントをインストールする 189
前提条件 189
Webサイトから起動 191
EC2で起動 192
GCPにNetScalerエージェントをインストールする 202
前提条件 203
GCPにNetScalerエージェントをインストールする 203
YAMLを使用してKubernetesクラスターにNetScalerエージェントをインストールする 204
OpenShiftコンソールを使用してNetScalerエージェントオペレーターをインストールする 205
前提条件 205
エージェントオペレーターをインストールする 207

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

エージェントインスタンスを削除する 208
エージェントオペレーターをアンインストールする 208
Helmチャートを使用してコンテナベースのエージェントをインストールする 208
ヘルプとサポートの利用方法 208
Citrix Cloudアカウントの作成 208
アカウントにサインインする 209
パスワードの変更 209
Citrix Cloud サポートフォーラム 210
サポート記事とドキュメント 210
Citrix Cloudリソースセンター 210
シトリックス テックゾーン 211
テクニカルサポート 211
サービス稼働状況ダッシュボード 211
サービス稼働状況のサブスクリプション 212
強化されたグラフィカルユーザーインターフェース 213
ホバーで表示されるメニュー 213
効率化されたメニュー階層 213
更新されたサブメニューラベル 214
インフラストラクチャ > 構成 214
NetScalerライセンス > プールライセンス 214
ゲートウェイ > HDX Insight 215
設定 215
折りたたみ可能なメニュー 216
展開されたメニュー 216
折りたたまれたメニュー 216
サイドバーの切り替え 216
サイドバーを表示 216
サイドバーを非表示にする 216

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

ホーム画面として設定 216
お気に入りの項目をピン留めする 216
Console Advisory 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 218
概要: NetScaler Console オンボーディングワークフローのコンポーネント 218
オンボーディングのクイックツアー 220
Console Advisory Connect を使用して NetScaler インスタンスをオンボードする 221
ステップ 1: 開始する 222
ステップ2：NetScalerおよびGatewayインスタンスに関するインサイト 223
ステップ3：オンボードするNetScalerおよびGatewayインスタンスを選択する 225
ステップ4：NetScalerインスタンスをNetScaler Consoleにオンボードする 226
組み込みエージェントを使用してNetScalerインスタンスをオンボードする 226
外部エージェントを使用してNetScalerインスタンスをオンボーディングする 228
パブリッククラウドにエージェントをインストールする 229
NetScalerインスタンスのオンボーディング準備状況をテストする 230
メール設定 230
メール設定の構成 231
すべての管理者にメールを有効にする 232
組織内の特定の管理者に対してメールを有効/無効にする 233
すべての管理者のメールを無効にする 234
診断ツールまたはNetScaler Console GUIを使用して問題をトラブルシューティングする 234
診断ツールを手動で使用する 235
診断ツールを使用してNetScalerインスタンスのオンボーディング準備状況を検証する236
NetScaler Console GUI で NetScaler 診断情報を表示する 236
トラブルシューティング 237
無効なユーザー名またはパスワード 237
DNS構成エラー 237
インターネット接続なし 237
NetScaler Consoleエンドポイントへの接続なし 237

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

組み込みエージェントのドライランタイムアウト 238
デバイスプロファイルのドロップダウンに表示される赤い枠線 238
組み込みエージェントから外部エージェントへの移行 238
開始する前に 238
組み込みエージェントから外部エージェントへの移行 239
NetScaler Console に ID プロバイダーとして SAML を接続する 240
前提条件 240
クラウドコネクタ 240
Active Directory 241
SAML SSO 設定 241
システム要件 247
サポートされるブラウザ 247
エージェントのインストール要件 247
プールまたはフレックスライセンス用の軽量エージェント 249
サポートされているポート 250
NetScalerエージェント用のポート 250
NetScalerインスタンスのポート 252
NetScaler組み込みエージェントのポート 252
NetScaler Console Analytics ソリューションの要件 254
必要なCitrix Virtual Apps and Desktopsの最小バージョン 254
HDX™ Insightでサポートされるシンクライアント 254
HDX Insightに必要なNetScalerインスタンスライセンス 254
サポートされているオペレーティングシステムとCitrix Workspaceのバージョン 255
ライセンス 256
NetScaler Console機能に必要なNetScalerライセンス 256
仮想サーバーサブスクリプションの有効期限チェックを表示 258
仮想サーバーで有効になっている分析の種類を表示 259
アップグレードアドバイザリ 260

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

アップグレードアドバイザリを表示 261
推奨ビルドを設定する 261
NetScalerインスタンスをアップグレードする 262
セキュリティアドバイザリ 265
セキュリティアドバイザリのランディングページ 265
セキュア構成の推奨事項 267
CVE検出 267
ファイル整合性監視 267
今すぐスキャン 267
スキャン履歴 268
影響を受けるNetScaler 268
設定 268
セキュアな構成の推奨事項 269
重要度に基づく優先順位付け 269
詳細なインスタンスレベルビューの利点 270
構成の推奨事項を修正する 271
CVE検出 273
インスタンスビュー 274
CVEビュー 276
CVEリポジトリ 277
注意事項 277
ファイル整合性監視 279
コンソール検出 279
注意事項 281
デバイスレポート 281
NetScaler Consoleにおける侵害の痕跡の検出 281
前提条件 282
利点 282

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

脆弱性の修復 283
CVE-2026-88771の脆弱性を特定し、修正する 284
CVE-2026-88771を修正する 285
CVE-2026-88772の脆弱性を特定し、修正する 285
CVE-2026-88772を修正する 286
CVE-2026-88773の脆弱性を特定し、修正する 286
CVE-2026-88773を修正する 287
CVE-2026-88774の脆弱性を特定して修正する 287
CVE-2026-88774を修正する 288
CVE-2026-88775の脆弱性を特定して修正する 288
CVE-2026-88775を修正する 288
CVE-2026-88776の脆弱性を特定し、修復する 289
CVE-2026-88776を修復する 289
CVE-2026-88777の脆弱性を特定し、修正する 290
CVE-2026-88777を修正する 290
CVE-2026-88778の脆弱性を修正する 290
CVE-2026-88778を修正する 291
ステップ1：脆弱なNetScalerインスタンスをアップグレードする 291
ステップ2：構成コマンドを適用する 291
ステップ2：インスタンスを選択する 292
CVE-2026-19490 の脆弱性を特定して修復する 293
CVE-2026-19490 を修復する 293
CVE-2026-19489の脆弱性を特定し、修復する 293
CVE-2026-19489を修復する 294
CVE-2026-13474 の脆弱性を特定して修復する 294
CVE-2026-13474 を修復する 295
ステップ 1: 影響を受ける NetScaler インスタンスをアップグレードする 295
ステップ2：構成コマンドを適用する 295

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

CVE-2026-10817の脆弱性を特定して修正する 297
CVE-2026-10817を修正する 297
CVE-2026-10816の脆弱性を特定し、修正する 297
CVE-2026-10816を修正する 298
CVE-2026-8655の脆弱性を特定し、修復する 298
CVE-2026-8655を修復する 299
CVE-2026-8452の脆弱性を特定して修正する 299
CVE-2026-8452を修正する 300
CVE-2026-8451の脆弱性を特定して修正する 300
CVE-2026-8451を修正する 301
CVE-2026-4368の脆弱性を特定し、修正する 301
CVE-2026-4368を修正する 301
CVE-2026-3055の脆弱性を特定し、修復する 302
CVE-2026-3055を修復する 302
CVE-2025-12101の脆弱性を特定して修正する 303
CVE-2025-12101を修正する 303
CVE-2025-8424 の脆弱性を特定して修復する 304
CVE-2025-8424 を修復する 304
CVE-2025-7776の脆弱性を特定し、修正する 305
CVE-2025-7776を修正する 305
CVE-2025-7775の脆弱性を特定して修正する 306
CVE-2025-7775を修正する 306
CVE-2025-6543の脆弱性を特定し、修正する 307
CVE-2025-6543を修正する 308
CVE-2025-5349 の脆弱性を特定して修正する 308
CVE-2025-5349 を修正する 309
CVE-2025-5777の脆弱性を修正する 310
CVE-2025-5777を修正する 311

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

ステップ1：脆弱なNetScalerインスタンスをアップグレードする 311
ステップ2：構成コマンドを適用する 312
ステップ2: インスタンスの選択 313
CVE-2024-8535の脆弱性を修正する 313
CVE-2024-8535を修正する 314
ステップ1：脆弱なNetScalerインスタンスをアップグレードする 314
ステップ2：構成コマンドを適用する 315
Step 2: インスタンスを選択する 315
CVE-2020-8300 の脆弱性に対処する 316
CVE-2020-8300 の修正 317
ステップ 1: 脆弱なNetScalerインスタンスをアップグレードする 317
ステップ 2: 構成コマンドを適用する 317
ステップ2: インスタンスを選択する 320
NetScaler Console Expressアカウントに関する注意事項 321
シナリオ 322
CVE-2021-22927およびCVE-2021-22920の脆弱性を修正する 323
CVE-2021-22927およびCVE-2021-22920を修正する 324
ステップ1：脆弱なNetScalerインスタンスをアップグレードする 325
ステップ2：構成コマンドを適用する 325
ステップ2: インスタンスを選択する 327
シナリオ 328
CVE-2021-22956の脆弱性を特定して修復する 330
CVE-2021-22956の影響を受けるインスタンスを特定する 330
CVE-2021-22956を修復する 331
ステップ1：脆弱なNetScalerインスタンスをアップグレードする 331
ステップ2：構成コマンドを適用する 331
手順 2：インスタンスを選択する 332
CVE-2022-27509 の脆弱性を特定し、修正する 333

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

CVE-2022-27509の影響を受けるインスタンスを特定する 334
CVE-2022-27509を修正する 334
セキュリティアドバイザリでサポートされていないCVE 335
セットアップ 337
複数のエージェントを追加する 337
マルチサイト展開向けにエージェントを構成する 338
アーキテクチャ 339
エージェントフェイルオーバー 339
エージェントのアップグレード設定を構成する 341
エージェントを手動でアップグレードする 341
NetScaler ConsoleでのデュアルNICサポート 343
インスタンスの追加 345
NetScaler®プロファイルを作成する方法 346
NetScalerインスタンスをNetScaler Consoleに追加するには 348
NetScaler ConsoleでNetScaler CPXインスタンスを追加するには 349
NetScaler ConsoleでスタンドアロンのNetScaler BLXインスタンスを追加するには 350
NetScaler Consoleで高可用性NetScaler BLXインスタンスを追加するには 351
NetScaler ConsoleからインスタンスGUIにアクセスするには 352
インスタンスの警告を解決する 352
インスタンスでのsyslogの設定 353
Logstreamの概要 355
Logstreamをトランスポートモードとして有効にする 355
委任管理者ユーザーにより多くの権限を割り当てる方法 357
委任管理者へのスーパー管理者権限の割り当て 357
委任管理者へのカスタムロールの割り当て 358
ServiceNowインスタンスとの統合 358
NetScalerイベントのServiceNowインシデントを生成する 359
有効期限が近づいているSSL証明書のServiceNowインシデントを生成する 360

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

NetScaler Consoleライセンスの有効期限に関するServiceNowインシデントを生成する 360
NetScaler Consoleイベントポリシーをカスタマイズする 360
実行可能なタスクと推奨事項 361
タスク 362
推奨事項 365
ガイドミーワークフローを使用して推奨事項を完了する方法? 368
通知を設定する 368
よくある質問 369
インスタンスの主要メトリックの詳細を表示する統合ダッシュボード 371
アプリケーション 371
NetScalerインフラストラクチャ 372
アプリケーションセキュリティ 372
ゲートウェイ 373
API 分析 373
ダッシュボードのカスタマイズ 373
エージェントの詳細を表示 374
フィルターの作成と適用 374
フィルターの編集 375
インスタンスの主要なメトリックの詳細を表示するためのカスタムダッシュボードを作成する 376
ダッシュボードのその他のオプション 377
他のユーザーとダッシュボードを共有する 377
APIセキュリティ 378
APIセキュリティの利点 378
APIセキュリティの構成と管理の権限を付与する 379
API定義を作成またはアップロードする 380
OAS仕様をアップロードする 380
API定義を作成する 381
API定義を表示する 381

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

APIインスタンスを展開する 381
APIプロキシを追加する 382
APIプロキシを使用してAPIインスタンスを展開する 383
API分析を有効にする 384
API展開にポリシーを追加する 385
ポリシーの種類 386
認証と認可 387
レート制限 388
WAF 389
ボット 389
ヘッダー書き換え 390
URIパスの書き換え 390
拒否 391
API分析を表示 391
APIエンドポイントの分布 392
APIインスタンス 392
APIエンドポイント 392
認証の失敗 393
さまざまなAPIインサイトを表示 393
インスタンス内の上位APIエンドポイントを表示 394
最もアクセスされたAPIを表示 394
エンドポイントの地理的位置を表示 394
HTTPS応答ステータスを表示 394
APIリクエストの傾向を表示 395
エンドポイントの帯域幅消費量を表示 395
SSLエラーと使用状況を表示 395
APIエンドポイントの検出 395
APIエンドポイントの表示 396

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

検出されたAPIエンドポイントからAPI定義を作成する 397
検出されたAPIエンドポイントで既存のAPI定義を更新する 398
APIインスタンスのデプロイ解除 399
APIポリシーのデプロイ解除 399
APIデプロイのデプロイ解除 399
APIプロキシの展開解除 400
APIを使用してAPIセキュリティを管理する 400
ポリシータイプのAPI例 402
レート制限 402
オース 403
基本認証 405
認証なし 406
ボット 406
WAF 407
ヘッダー書き換え 408
URIパス書き換え 409
認証 412
拒否 413
StyleBook を使用して WAF および BOT プロファイルを作成する 414
StyleBook を使用して WAF プロファイルを作成する 414
StyleBookを使用してBOTプロファイルを作成する 415
アプリケーション 417
前提条件 417
アプリケーションの概要 417
ディスクリートアプリケーション 417
カスタムアプリケーション 418
注意事項 418
マイクロサービスアプリケーション 418

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

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 418
アプリケーションの管理 418
アプリケーションダッシュボード 419
ダッシュボードの列でデータを並べ替える 419
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 420
アプリケーションの管理 420
アプリケーションの詳細を表示 421
アプリケーションの追加 421
StyleBookを使用してアプリケーションを作成する 423
アプリケーションの編集または削除 424
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 424
アプリケーションの表示 425
マイクロサービスアプリケーションの表示 426
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 427
アプリケーションダッシュボードの概要 429
検索バーを使用して結果を検索およびフィルターする 431
フィルターを保存 432
アプリケーションにタグを作成して適用する 432
アプリケーションの詳細 433
アプリケーションのモニターの状態を確認する 436
App Scoreコンポーネントを選択し、しきい値を設定する 436
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 439
インテリジェントアプリ分析 441
インテリジェントアプリ分析を構成する 442
アプリケーション分析のパフォーマンス指標 443
応答時間 444
アクティブなサービス 444

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

平均CPU使用率 445
平均アプリケーションCPU使用率 445
メモリ使用率 445
NIC破棄 446
サービスフラップ 446
セッション再利用率の低下 447
不適切なパーシステンスタイプ 447
不安定なサーバー 448
SSLリアルタイムトラフィック 449
異常に大きいHTTPパケット 450
TCP再アセンブルキュー制限ヒット 451
サージキューの蓄積 451
SSL評価 452
Appダッシュボードのトラブルシューティング 452
トラブルシューティングのシナリオ 453
アプリケーションがライセンスされている 453
メトリックコレクターが有効になっている 453
47.xビルドより前のNetScalerインスタンス 454
47.xビルド以降のNetScalerインスタンス 455
アプリケーションの使用状況と異常 457
ピーク時と閑散時の使用状況分析 458
アプリのスケーリング制限を評価する 458
上位5つのアプリメンテナンス期間を特定する 458
アプリケーション使用状況分析 460
メトリックの詳細をグラフ形式で表示 466
SSL証明書管理を自動化する 470
NetScaler ConsoleでVenafiサーバーを構成する 470
SSL証明書のライフサイクルを管理する 471

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

A+ SSL評価分析 473
A+ SSL評価にアップグレードする 473
SSL評価をロールバックする 474
アプリケーショントラフィックに対するSSL評価の影響を判断する 475
Web Insight ダッシュボード 476
暗号関連の問題の詳細を表示 477
統合キャッシュリクエスト 478
その他のユースケース 479
アプリケーションの遅延の根本原因を分析する 479
アプリケーションのドリルダウン 480
応答時間 481
サービスグラフ 482
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 482
Kubernetesアプリケーションのサービスグラフ 483
3層Webアプリケーションのサービスグラフ 484
Kubernetesアプリ用サービスグラフ 485
サービスグラフ - 簡素化されたオンボーディング 486
Kubernetesジョブとしてエージェントを自動的に展開する 486
サービスグラフの手動設定 490
サービスグラフのセットアップ 493
ソフトウェア要件 493
シングルティアまたは統合イングレストポロジ 494
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 494
サービスメッシュトポロジ 495
サービスグラフで詳細を表示 497
サービスグラフダッシュボード 497
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 499
サービス応答時間のPxx値を表示 500

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

サービス詳細の表示 500

クライアントメトリクスの表示 500

TCPおよびSSLメトリクスを表示 501

フィルターを適用 502

設定オプション 503

エラーを分析する 503

HTTPトランザクションの詳細を表示 504

サービスグラフでしきい値を構成する 505

単一しきい値 506

二重しきい値 507

サービスの詳細を表示 507

メトリックの詳細 508

バックエンドPodの詳細を表示 509

ゴールデンシグナルメトリクスを使用してサービスを監視する 509

問題のトラブルシューティングのためにイングレスの詳細を表示する 510

分散トレース 514

前提条件 514

サービストレースの詳細を表示 518

トランザクションの詳細を表示 519

サービスグラフの部分的またはデータなしの診断詳細を表示 520

データなしの診断 521

部分的なデータに関する診断 521

トラブルシューティング 522

3層Webアプリケーションのサービスグラフ 523

アプリケーションビュー 523

ネットワーク機能ビュー 523

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 524

メトリックの分析 524

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

クライアントメトリクス 524
ネットワーク機能メトリクス 524
サービスメトリクス 525
NetScalerメトリック (GSLBアプリケーションのみ) 525
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 526
クライアントメトリックの表示 526
NetScalerの詳細を表示 526
個別のアプリケーションを表示 527
マイクロサービスアプリケーションの表示 529
結果をフィルタリングするための検索バー 529
StyleBooks 531
StyleBookのカテゴリ 533
デフォルトStyleBookとカスタムStyleBook 533
パブリックStyleBookとプライベートStyleBook 533
プライベートとしてマークされたStyleBookの例 534
StyleBookの表示 534
カスタムStyleBookをダウンロード 535
カスタムStyleBookを更新 536
カスタムStyleBookを削除する 536
StyleBookの依存関係を表示する 537
StyleBookの依存関係を表示するには 537
順方向の依存関係 537
逆方向の依存関係 538
設定パックに対するNetScaler構成の監査 538
構成パックのサポートバンドルをダウンロードする 538
StyleBookのタグを作成する 539
StyleBookをクローンする 540
外部リポジトリからStyleBookをインポートして同期する 541

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

リポジトリを追加 544
リポジトリオプション 544
GitHub/GitLabからStyleBookと設定パックをインポートする手順 545
デフォルトのStyleBookを使用する 545
NetScalerの機能 545
ウェブアプリケーションファイアウォール機能 547
アプリケーションセキュリティ機能 548
ボット管理機能 549
NetScalerネットワーク構成 550
次のステップ? 551
Webアプリケーションファイアウォール StyleBook 551
アプリケーションファイアウォール構成の展開 551
SNMP 設定スタイルブック 554
NetScalerネットワーク構成StyleBook 559
基本的なネットワークコンポーネントを展開する 560
高度なネットワークコンポーネントを展開する 562
Prometheus アナリティクス StyleBook 564
前提条件 564
StyleBooks Configuration Builder を使用した NetScaler アプリケーション構成の移行 565
移行された構成間での構成エンティティの共有 566
サポートされているNetScaler機能 567
NetScalerアプリケーション構成を移行するためのStyleBookの作成 567
制限事項 569
ビジネスアプリケーション StyleBook 570
SSO Google Apps スタイルブック 570
SSO GoogleアプリStyleBookを展開するには 571
SSO Office 365 スタイルブック 575
SSO Microsoft Office 365 StyleBookを展開するには 576

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

Microsoft Skype for Business スタイルブック 580
エンタープライズでのNetScalerインスタンスの構成 581
Microsoft Exchange スタイルブック 587
Microsoft Exchange StyleBookを使用して構成されるNetScaler機能 588
前提条件 588
Microsoft Exchange スタイルブックの構成 588
Microsoft Exchangeアプリケーションを構成するには 588
Microsoft SharePoint スタイルブック 590
前提条件 590
Microsoft ADFSプロキシStyleBook 595
NetScalerをADFSプロキシとして使用する利点 595
Oracle E-ビジネス スタイルブック 600
Oracle E-Business Suite 12.2の構成を作成するには 601
カスタムStyleBookの作成と使用 601
開始する前に 602
StyleBookの構造 603
構成パックの作成と編集 604
構成パックの作成 604
StyleBookの外部で作成された構成を再利用し、ConfigPack間で構成を共有する 605
構成パックのStyleBookを変更する 606
構成パックのエクスポートまたはインポート 608
構成パックを下書きとして保存する 610
設定パックのスケジュールを作成する 611
設定パックからターゲットインスタンスをデタッチする 612
StyleBookを作成する 612
ロードバランシング仮想サーバーを作成するためのStyleBook 616
ヘッダー 616
コンポーネント 622

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

StyleBookを構築する 623
基本的なロードバランシング構成を作成するためのStyleBook 626
ヘッダー 626
コンポーネント 629
出力 634
StyleBookを構築する 635
複合StyleBookを作成する 639
StyleBookを作成する 640
カスタムStyleBookでGUI属性を使用する 644
パラメータにツールチップ付きのラベルを追加する 644
パラメータの折りたたみ可能なペインを設定する 644
ユーザーオプションをラジオボタンとして設定する 646
カスタムStyleBookのインポート 647
StyleBookの説明とヘッダーでHTML書式設定タグを使用する 647
StyleBookをインポートするには 648
ファイルをアップロードするためのStyleBookを作成する 652
StyleBook構成 652
StyleBookを作成する - 1 652
StyleBookを作成する - 2 654
ファイルをアップロードするための構成を作成する 656
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 657
StyleBook構成 658
SSLファイルをアップロードするための構成の作成 661
StyleBookを構築する 662
StyleBook を使用して証明書ストアから SSL 証明書を管理する 666
パラメータ 666
コンポーネント 667
StyleBook を構築する 668

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

StyleBookで定義された仮想サーバーでアナリティクスを有効にし、アラームを設定する 672
インスタンスの役割 674
ターゲットロールセクション 675
役割「default」 676
ロールを持つコンポーネント 676
StyleBookを構築する 680
APIの使用 683
非CRUD操作を実行するStyleBookを作成する 685
非CRUD操作のサポート 685
DNSドメイン名を使用したGSLB構成の展開 687
管理者向けのワークフロー 688
管理ワークフロー用のNetScaler Console REST API 691
アプリケーション所有者向けのワークフロー 725
アプリケーション所有者ワークフロー用のNetScaler Console REST API 727
StyleBookを作成する 730
StyleBookで特殊文字をリテラル形式で許可する 740
複数の逐語的な文字列を連結する 743
データソースの管理 743
データソースとしてNetScalerインスタンスを使用する 744
コレクションなしで組み込みデータソースを使用する 745
コレクションで組み込みデータソースを使用する 748
ターゲットのNetScalerインスタンスをデータソースとして使用する 754
ターゲットNetScalerインスタンスをデータソースとして使用するStyleBookの例 755
カスタムデータソースを使用する 757
データソースタイプを追加する 757
データソースタイプの下にコレクションスキーマを追加する 757
データソースを追加する 758
コレクションデータを追加する 758

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

コレクションなしでカスタムデータソースを使用する 758

コレクションでカスタムデータソースを使用する 761

APIを使用してStyleBookから構成を作成する 764

例1 764

例2 768

例 3 770

例 4 772

構成の更新 774

構成の削除 776

API を使用して構成を作成する 777

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 781

APIを使用してカスタムStyleBookをインポートする 782

APIを使用してカスタムStyleBookを更新する 786

カスタムStyleBookをダウンロードするためのAPIの使用 787

依存StyleBookをダウンロードし、圧縮タイプを指定するためのAPIの使用 787

APIを使用してカスタムStyleBookを削除する 788

APIを使用して既存の構成パックを更新する 789

APIを使用してターゲットインスタンスを更新する 795

API を使用して構成を監査する 798

APIを使用して設定パックをエクスポートする 799

APIを使用して構成パックを新しいStyleBookにアップグレードする 800

APIを使用して、コンフィグパックからターゲットインスタンスをデタッチする 801

APIを使用して、config packからNetScalerインスタンスを強制的に削除する 801

API を使用して設定パックを削除する 803

StyleBookの文法 806

ヘッダー 808

StyleBookのインポート 810

パラメータ 812

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

'名前' 812
'ラベル' 812
'説明' 813
タイプ 813
'ネットワーク' 815
「ダイナミックアロケーション」 815
「キー」 816
'必須' 817
'許可される値' 817
'新しい値の許可' 819
'デフォルト' 820
パターン 821
最小値 821
最大値 822
「最小長」 822
「最大長」 823
「最小項目数」 823
「最大項目数」 824
「GUI」 824
「列」 824
「更新可能」 824
「collapse_pane」 825
「レイアウト」 831
「依存パラメータ」 831
`is_policy_expression` 833
Parameters-default-sources コンストラクト 834
Parameters-source コンストラクト 842
パラメータ条件 843

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

「show」または「hide」 844
「デフォルト設定」 844
'必須設定' 845
'許可値の設定' 846
'ラベルの設定' 849
'set-description' の設定 850
'collapse-pane' または 'expand-pane' のオプション 850
「セットパターン」 851
ネストされたパラメーター条件 851
置換 852
置換マップ 864
置換リストを反復処理する 865
コンポーネント 868
ヘルパーコンポーネント 871
オプションプロパティ 875
プロパティデフォルトソース構成要素 878
コンポーネントのプロパティの算出 881
ネストされたコンポーネント 882
条件コンストラクト 885
繰り返しコンストラクト 888
繰り返し条件」構成要素 893
ネストされた繰り返し 894
出力 898
パラメータ参照 900
親参照 903
コンポーネントリファレンス 906
置換リファレンス 909
変数参照 910

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

操作 912
分析 919
ターゲット仮想サーバーとインサイトタイプ 922
アラーム 923
式 927
算術式 927
文字列式 928
リスト式 928
関係式 928
論理式 - ブール 929
スプラット式 930
逐語的文字列式 931
ターゲット式 931
式の型検証 932
インプレース補間 937
補間内で許可される型 938
単純な補間 939
自動型変換 939
シーケンシャル補間 939
ネストされた補間 939
`quotewrap` を使用した補間 939
組み込み関数 940
文字列() 940
int() 関数 941
bool() 関数 941
長さ() 942
最小値() 942
マックス() 942

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

bin() 関数 943
oct() 関数 943
hex() 関数 943
lower() 関数 943
upper() 関数 944
sum() 関数 944
pow() 関数 944
ip() 944
ip_network() 945
network_ip() 945
subnets() 関数 946
netmask_ip() 946
is_netmask_ip() 946
broadcast_ip() 946
シーアイディーアール() 947
is_cidr() 947
is_in_network() 947
base64.encode() 947
base64.decode() 948
イグジスツ() 948
フィルター() 948
イフ・ゼン・エルス() 949
join() 関数 949
split() 関数 950
map() 関数 950
quotewrap() 関数 951
リプレース() 951
トリム() 953

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

トランケート() 953
ディスティンクト() 953
url.encode() 953
url.decode() 953
イズ・アイピーブイフォー() 954
イズ・アイピーブイシックス() 954
startswith() 関数 954
endswith() 関数 954
コンテインズ() 955
substring() 関数 955
マッチ() 956
sha256() 957
リレート() 958
マルチプル() 961
リバース() 962
依存関係の検出 962
循環依存関係 965
セキュリティ 968
アプリケーションセキュリティダッシュボード 968
脅威インデックスの詳細 969
安全性インデックスの詳細 970
統合セキュリティダッシュボード 971
保護されたアプリケーション 971
保護されていないアプリケーションの保護を設定する 971
アプリケーションのセキュリティ違反の詳細を表示 976
セットアップ 977
Webトランザクション設定を有効にする 977
アプリケーションの概要 978

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

違反カテゴリ 978
WAF違反の詳細を表示 980
ボット違反の詳細を表示 981
イベント履歴の表示 983
署名の自動更新 983
すべての違反 983
違反カテゴリ 983
セキュリティ違反ダッシュボード 985
違反の詳細 986
WAF学習 986
はじめに 987
WAFの推奨事項 989
前提条件 990
WAFスキャン設定を構成する 990
WAFスキャン推奨プロセス 992
スキャンレポートの表示 993
ゲートウェイ 996
ゲートウェイインサイト 996
Gateway Insightを有効にする 998
NetScaler Consoleで仮想サーバーのAppFlowを有効にする 998
GUIを使用してNetScaler GatewayアプライアンスでAppFlowユーザー名ログ記録を有効にする 999
Gateway Insightレポートの表示 999
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 999
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 999
ユーザー 1000
ユーザーの詳細を表示 1000
検索バーと地理マップビュー 1001

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

アプリケーション 1002
アプリケーションの詳細を表示 1002
ゲートウェイ 1003
ゲートウェイの詳細を表示 1003
レポートのエクスポート 1003
レポートのエクスポート 1004
Gateway Insightのユースケース 1004
1. ユーザーがNetScaler Gatewayアプライアンスまたは内部Webサーバーにログオンできない 1005
認証の失敗 1005
認証失敗の詳細を表示する 1005
EPAの失敗 1006
EPA失敗の詳細を表示する 1006
SSO障害 1006
SSO障害の詳細を表示 1007
アプリケーション起動失敗の詳細を表示 1007
アプリケーションが消費した合計バイト数と帯域幅を表示する 1008
リソースのユーザーアクセスを表示する 1008
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 1009
Gateway Insight の問題のトラブルシューティング 1009
Gateway Insight 構成チェックリスト 1009
NetScaler と NetScaler Console 間の接続チェックリスト 1010
NetScaler チェックリストでのレコード生成 1010
NetScaler Console での検証 1010
Gateway Insight の統計 1011
Citrixテクニカルサポートに連絡する 1011
既知の問題 1011
HDX™ インサイト 1012

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

パフォーマンス低下の根本原因の特定 1013
シナリオ1 1013
シナリオ2 1014
HDX Insight のジオマップ 1015
プライベート IP ブロックの作成 1016
ユースケース 1017
制限事項 1018
HDX™ Insight データ収集を有効にする 1018
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 1019
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 1020
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 1023
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 1028
HDX™ Insight のしきい値を作成し、アラートを設定する 1031
使用例 1032
HDX™ Insight レポートとメトリクスを表示 1034
アプリケーションビューのレポートとメトリック 1035
デスクトップビューのレポートとメトリクス 1042
ユーザービューレポートとメトリクス 1054
インスタンスビューのレポートとメトリック 1065
ライセンスビューレポートとメトリクス 1069
HDX™ Insight の問題のトラブルシューティング 1070
HDX Insight 構成チェックリスト 1070
NetScalerとNetScaler Console間の接続チェックリスト 1071
NetScalerにおけるHDX/ICAトラフィックのレコード生成チェックリスト 1071
エラーカウンター 1079
nstraceの検証 1084

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

NetScaler Consoleチェックリスト内のレコードの入力 1084
Citrixテクニカルサポートに問い合わせる前に 1084
既知の問題 1084
しきい値のメトリクス情報 1085
Web 1085
セキュリティ 1087
APPANALYTICS 1088
HDX™ 1088
インフラストラクチャ 1089
インフラストラクチャ分析 1089
NetScaler Consoleのインフラストラクチャ分析 1090
インスタンススコア 1090
健全性インジケーターの説明 1090
NetScalerのキャパシティ問題を表示する 1092
ヘルスインジケーターの値 1093
インフラストラクチャ分析ダッシュボード 1093
サークルパックビュー 1094
インスタンスサークル 1094
グループ化されたインスタンスサークル 1095
クラスター化されたインスタンスの円 1095
Circle Pack の使用方法 1096
表形式ビュー 1096
検索バー 1096
サマリーパネルの使用方法 1097
インスタンス情報 1098
トラフィックプロファイル 1099
設定パネルの使用方法 1099
表示 1099

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

インスタンススコア計算のメトリックを選択し、重みをカスタマイズする 1100

通知を構成する 1100

ダッシュボードでデータを視覚化する方法 1101

Infrastructure Analytics でインスタンスの詳細を表示する 1101

NetScalerインスタンスのキャパシティ問題を表示する 1107

容量の問題を解決するための推奨されるアクションを表示 1107

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 1108

表形式ビュー 1110

異常の詳細を表示 1110

インスタンス管理 1111

インスタンスを追加する 1111

インスタンスダッシュボードの使用方法 1111

グローバルに分散されたサイトを監視する方法 1112

NetScaler Consoleでのグローバルに分散されたサイトの監視 1113

ユースケース 1113

Geomapの構成 1114

タグを作成してインスタンスに割り当てる方法 1118

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 1119

NetScaler VPXインスタンスを検索するには 1120

NetScaler® Console を介した GeoIP DB の一元的な更新 1121

制限事項 1121

NetScaler Console を介した GeoIP DB の一元的な更新の構成 1122

NetScalerインスタンスの管理パーティションを管理する 1124

管理パーティションを表示する 1124

リビジョン履歴の差分を表示する 1125

テンプレートと実行中の差分を表示する 1126

NetScalerインスタンスのバックアップと復元 1127

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

NetScaler Consoleを使用して、選択したNetScalerインスタンスのバックアップを作成する 1128
バックアップファイルを外部システムに転送する 1129
NetScaler Consoleを使用してNetScalerインスタンスを復元する 1130
このダッシュボードのレポートをエクスポートする 1132
セカンダリNetScalerインスタンスへのフェールオーバーを強制する 1132
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 1133
インスタンスグループの作成 1134
NetScaler Consoleを使用してインスタンスグループを作成するには 1134
マッピングされていないインスタンスを識別してグループに追加するには 1134
グローバルサーバー負荷分散サイトグループ 1135
GSLBサイトグループを作成する 1135
NetScalerエージェント用のSNMPマネージャーとユーザーを作成する 1136
SNMP v2マネージャーを追加する 1136
SNMP v3マネージャーを追加する 1137
SNMPユーザーを追加する 1137
SNMPビューの管理 1138
SDX 上での NetScaler VPX インスタンスのプロビジョニング 1139
ステップ 1 - VPX インスタンスを追加する 1139
ステップ2 - ライセンスの割り当て 1140
ステップ 3 - リソースの割り当て 1140
ステップ 4 - インスタンス管理の追加 1141
ステップ5 - ネットワーク設定の指定 1142
ステップ6 - 管理VLAN設定を指定します 1143
プロビジョニングされたVPXインスタンスを表示する 1144
複数のNetScalerインスタンスを再検出する 1144
ポーリングの概要 1144
NetScaler Consoleが管理対象インスタンスとエンティティをポーリングする方法 1145

© 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 1150
インスタンスの管理を解除する 1152
インスタンスへのルートをトレースする 1153
NetScalerが所有するIPアドレスの表示 1153
NetScalerが所有するIPアドレスのエクスポート 1154
NetScalerが所有するIPアドレスのエクスポートをスケジュールする 1154
NetScaler MPXまたはVPXのrootパスワードを変更する方法 1156
構成ジョブ機能を使用してパスワードを変更する 1156
NetScaler SDX nsroot パスワードを変更する方法 1158
パスワードの変更 1158
NetScaler® インスタンスのテクニカルサポートバンドルを生成する方法 1160
イベント 1162
イベントダッシュボードの使用 1163
イベントルールを作成する 1164
イベントルールを設定する 1165
ステップ1 - 名前とインスタンスファミリを指定する 1165
ステップ2 - イベント期間を設定する 1165
ステップ3 - イベントの重大度を選択する 1166
ステップ4 - イベントカテゴリを指定する 1167
ステップ5 - NetScalerインスタンスを指定する 1167
ステップ6 - 障害オブジェクトを選択する 1167
手順 7 - 高度なフィルターを指定する 1168
ステップ 8 - イベントルールアクションの追加 1169
イベントフィルターをスケジュールする 1176
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 1177
イベントの概要を表示 1177
イベントメッセージ 1178
イベントの重大度とSNMPトラップの詳細を表示する 1179

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

syslogメッセージの表示とエクスポート 1181
syslogメッセージの表示 1181
syslogメッセージの検索 1181
Syslogメッセージのエクスポート 1182
syslogメッセージの抑制 1183
フィルターを作成してsyslogメッセージを抑制する 1183
フィルターの無効化 1184
SSLダッシュボード 1185
ACMEプロトコルを使用した証明書の自動更新 1186
NetScaler® ConsoleでのACMEサポート 1186
ACME統合のための構成手順 1187
発行と更新 1195
証明書の発行 1196
サードパーティ統合 1198
制限事項 1200
自動証明書更新に関する問題のトラブルシューティング 1200
ゼロタッチ証明書管理 1201
証明書のアップロード 1202
ゼロタッチ証明書管理を有効にする 1202
SSLフィルターモードのサポート 1203
SSLダッシュボードを使用する 1205
SSL証明書を監視する 1205
SSL証明書の監査ログを表示する 1207
SSLダッシュボードでデフォルトのNetScaler証明書を除外する 1207
SSL証明書をダウンロードする 1207
SSLダッシュボードでSSL証明書を削除するには 1208
SSL証明書チェーンの表示 1209
SSL証明書の有効期限切れ通知を設定する 1210

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

インストール済みの証明書を更新する 1211
NetScalerインスタンスにSSL証明書をインストールする 1212
証明書署名要求 (CSR) を作成する 1213
SSL証明書をリンクおよびリンク解除する 1215
エンタープライズポリシーを構成する 1216
NetScalerインスタンスからSSL証明書をポーリングする 1217
NetScaler Console証明書ストアを使用してSSL証明書を管理する 1217
証明書ストアにSSL証明書を追加する 1217
証明書ストアでSSL証明書を更新する 1218
証明書ストアからSSL証明書を削除する 1218
NetScaler®インスタンスにSSL証明書をインストールする 1218
NetScalerインスタンスから証明書をインポートする 1219
中間アップロードなしでサーバー証明書を更新する 1219
構成ジョブ 1221
構成テンプレート 1221
インスタンス 1222
ファイル 1222
記録と再生 1223
このダッシュボードのレポートをエクスポートする 1223
関連資料 1223
構成ジョブの作成 1223
記録と再生を使用して構成ジョブを作成する 1227
構成ジョブを使用して、1つのインスタンスから複数のインスタンスへ構成を複製する 1230
構成ジョブで変数を使用する 1231
修正コマンドから構成ジョブを作成する 1234
1つの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 1236
実行済み構成ジョブを再利用する 1237

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

構成ジョブでSCP (put) コマンドを使用する 1238
構成テンプレートを使用する 1240
マスター構成テンプレートを使用する 1241
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 1247
NetScalerからPrometheusへのメトリクスエクスポートを設定するジョブをスケジュールする 1248
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 1250
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 1252
構成ジョブで構成監査テンプレートを再利用する 1252
構成テンプレートのインポートとエクスポート 1255
構成監査 1257
監査テンプレートの作成 1257
NetScaler インスタンスの構成監査をポーリングする 1259
監査レポートを表示 1260
ConfigChange SNMPトラップの構成監査差分を生成する 1264
インスタンス全体の構成変更を監査する 1265
ネットワーク構成に関する構成アドバイスを取得する 1268
アップグレードジョブ 1270
アップグレード前の検証 1271
NetScalerインスタンスのアップグレードをスケジュールする 1272
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 1275
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 1276
Autoscale™ グループのアップグレードをスケジュールする 1278
NetScalerインスタンスのHAペア構成をスケジュールする 1279
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 1281
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 1281
前提条件 1281
カスタマイズされたNetScaler構成のアップグレードに関する考慮事項 1282

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

NetScaler高可用性ペア 1283
NetScalerクラスター 1283
NetScalerアップグレードジョブの作成 1283
スケジュールされたアップグレードジョブの一時停止または再開 1288
失敗したアップグレードジョブを再試行する 1288
NetScalerディスク容量のクリーンアップ 1289
カスタムスクリプトを使用する 1290
NetScalerアップグレードオプション 1291
NetScaler高可用性ペアのアップグレードジョブのスケジュール設定 1292
NetScalerアップグレードジョブの統合差分レポートをダウンロードする 1293
ネットワーク機能 1294
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 1294
統合ロードバランシングレポートを生成する 1295
個別のロードバランシングエンティティレポートを生成する 1296
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 1297
ネットワークレポート 1299
ネットワークレポートダッシュボード 1299
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 1301
ネットワークレポートのエクスポート 1302
NetScaler Consoleでのネットワークレポートのしきい値の管理方法 1304
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 1306
ネットワークレポートのページ設定 1306
プロビジョニング 1307
AWSでのアプリベースのプロビジョニング 1307
前提条件 1308
クラウドアクセスプロファイル 1308
アプリケーション環境 1309
アプリケーション配信 1309

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

よくある質問 1310
Azureでのアプリベースのプロビジョニング 1312
前提条件 1313
クラウドアクセスプロファイル 1313
アプリケーション環境 1314
アプリケーション配信 1314
よくある質問 1315
NetScaler VPXインスタンスのプロビジョニング 1316
AWS 上での NetScaler VPX インスタンスのプロビジョニング 1317
Microsoft Azure 上での NetScaler VPX インスタンスのプロビジョニング 1327
Google Cloud で NetScaler VPX インスタンスをプロビジョニングする 1339
VMware ESX 上に NetScaler VPX インスタンスをプロビジョニングする 1347
NetScaler ハイブリッドおよびマルチクラウド展開のためのグローバル負荷分散 1353
NetScaler ハイブリッドおよびマルチクラウド GLB ソリューションのアーキテクチャ 1353
NetScaler Console StyleBookを使用した構成 1357
StyleBook を使用した GLB の構成 1359
StyleBook を使用して NetScaler LB ノードで GLB を構成する 1364
オーケストレーション 1366
サービスグラフ用のKubernetesクラスターを管理する 1366
開始する前に 1367
NetScalerエージェントを構成してKubernetesクラスターに登録する 1367
Kubernetesクラスターを管理するために、NetScaler Consoleをシークレットトークンで構成する 1368
NetScaler ConsoleにKubernetesクラスターを追加する 1368
NetScaler® ライセンス 1370
ライセンスアクティベーションサービス 1371
前提条件 1372
自動有効化と互換性 1373

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

LASのNetScalerバージョン互換性 1373
LASへの移行 1374
初めてのLASユーザー 1375
LASでNetScalerインスタンスをライセンス供与する 1375
既存のライセンスインスタンスをLASに移行する 1376
既存のLASユーザー 1376
LASでNetScalerインスタンスをライセンスする 1377
ライセンスされたNetScalerインスタンスをLASに移行する 1377
LASライセンスワークフロー中にLASに送信される情報 1378
LASに移行したNetScaler Consoleサービス環境を監視するためのベストプラクティス 1379
前提条件 1379
LASアクティベーションBLOBの有効期限の監視 1380
GUIを使用してNetScalerインスタンスを表示する 1380
CLIを使用してNetScalerインスタンスのステータスを表示する 1380
通知 1381
ライセンスエンタイトルメントの有効期限切れの監視 1382
通知 1382
ライセンス管理 1383
LASベースのライセンス 1384
ライセンスサーバーポート 1384
ライセンスの有効期限情報 1384
通知設定 1385
LASのRBACサポート 1387
手動で管理されるエンタイトルメント (ファイルベースのライセンス) 1388
ライセンスファイル 1388
ライセンスサーバーのポート設定 1391
ライセンスの有効期限情報 1391
通知設定 1392

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

チェックアウトの最小および最大容量 1395

表1. MPXでサポートされるFlexed容量 1397

表2A。ビルド13.0-47.xより前のNetScaler SDXバージョンでサポートされるFlexed容量1398

表 2B. NetScaler SDX バージョン 13 (ビルド 13.0-47.x 以降)、バージョン 13.1 (ビルド 51.x より前)、およびバージョン 14.1 (ビルド 12.x より前) でサポートされるFlexed容量 1399

表2C. NetScaler SDX バージョン 13.1 (ビルド 51.x 以降) およびバージョン 14.1 (ビルド 12.x 以降) のサポートされるFlexed容量 1400

表 3. NetScaler CPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス 1401

表4. ハイパーバイザーおよびクラウドサービス上のNetScaler VPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス 1402

表5. NetScaler BLXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス 1402

表6. 異なるフォームファクターのゼロキャパシティライセンス要件 1403

NetScalerエージェントの動作 1403

LASベースのライセンス 1404

手動で管理されるエンタイトルメント (ファイルベースのライセンス) 1405

NetScaler Console エージェントを LSA として手動で選択する 1405

複数のNetScalerエージェントの動作 1405

NetScalerエージェントのフェールオーバー動作 1406

NetScaler 組み込みエージェントを介したライセンスサーバーの構成 1407

Flexed ライセンス 1407

ゼロキャパシティハードウェア 1409

Z-capライセンスの管理とインストール 1409

スタンドアロンNetScaler VPXインスタンス 1410

スタンドアロンのNetScaler CPXインスタンス 1411

スタンドアロンのNetScaler BLXインスタンス 1411

帯域幅プール 1411

インスタンスプール 1411

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

ライセンスの構成 1412
LASベースのライセンス 1413
前提条件 1413
ステップ1 - エンタイトルメントの反映を検証する 1413
ステップ2 - NetScalerインスタンスをコンソールサービスに追加する 1413
ステップ3 - LASでライセンスをアクティブ化する 1414
ステップ4 - NetScalerインスタンスのフレックススループット容量を編集する 1414
外部エージェントを使用するライセンスなしのMPXアプライアンスの特別なライセンス 1414
手動で管理されるエンタイトルメント（ファイルベースのライセンス） 1415
開始する前に 1416
ステップ1 - NetScaler Consoleでライセンスを適用する 1416
ステップ2 - NetScaler Consoleをライセンスサーバーとして登録し、ライセンスを割り当てる 1417
ステップ3 - ライセンスの種類に基づいて、関連するライセンス手順に進みます 1419
NetScalerインスタンスでフレキシブルまたはプールされたキャパシティを構成する 1421
NetScaler高可用性ペアのライセンス要件（LASとファイルベースライセンスの両方に共通） 1422
NetScaler Flexedライセンスの状態 (LASとファイルベースライセンスの両方に共通) 1423
ライセンスダッシュボード 1423
NetScalerインスタンスで割り当てられたスループット容量を編集する 1426
NetScalerインスタンスでライセンスを解放する 1426
ライセンスの問題のトラブルシューティング 1426
ライセンスレポート 1427
Flexedライセンスへの切り替え 1430
LASベースのライセンス 1431
手動で管理されるエンタイトルメント (ファイルベースライセンス) 1432
プール型帯域幅ライセンスからFlexedライセンスへの移行 1432
プールされたvCPUからFlexedライセンスへ 1433

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

固定サブスクリプションまたは永続ライセンスからFlexedライセンスへ 1433
固定vCPUからFlexedライセンスへ 1434
CICOからFlexedライセンスへ 1435
セルフマネージド帯域幅ライセンスからFlexedライセンスへ 1435
セルフマネージドvCPUからFlexedライセンスへの移行 1436
FlexedまたはPooledライセンスの有効期限切れと接続性の問題の動作シナリオ 1436
LASベースのライセンス 1437
期間満了前 1437
期間の満了後 1438
接続の問題の動作シナリオ 1438
手動で管理されるライセンス（ファイルベースライセンス） 1438
Flexedライセンスのコンポーネント 1438
シナリオ: MPXフォームファクター 1438
シナリオ: SDXフォームファクター 1439
シナリオ：VPX/BLX/CPXフォームファクター 1440
接続の問題の動作シナリオ 1441
NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成する1442
前提条件 1443
NetScaler Console を Flexed または Pooled ライセンスサーバー専用として構成する方法 1444
レガシーライセンス 1445
プールされたキャパシティ 1446
NetScaler MPX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 1447
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 1450
NetScaler SDX の永続ライセンスを NetScaler Pooled capacity にアップグレードする 1453
NetScaler VPX チェックインおよびチェックアウトライセンス 1456
NetScaler Consoleにライセンスをインストールする 1457

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

NetScaler GUIを使用してNetScaler VPXインスタンスにNetScaler VPXライセンスを割り当てる 1457
NetScaler CLIを使用してNetScaler VPXライセンスをNetScaler VPXインスタンスに割り当てる 1458
NetScaler VPX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構成する 1459
NetScaler 仮想 CPU ライセンス 1459
NetScaler VPX の仮想 CPU ライセンス 1460
FAQとその他のリソース 1462
構成 1463
ライセンスサーバーエージェント 1464
一般的な問題 1465
移行 1465
プール容量ライセンスの問題をトラブルシューティングする 1466
ライセンスステータスの確認 1467
サーバーのステータスを確認する 1469
ライセンスの使用状況レポートを確認する 1469
プール容量ライセンスのカウンターと統計 1470
設定 1473
Cloud Connectを使用してConsoleサービスに接続されたオンプレミスConsoleインスタンス 1473
Console on-prem アップロード 1474
仮想サーバーでアナリティクスを構成する 1476
検出された仮想サーバーでアナリティクスを構成する 1477
アナリティクスを編集 1479
分析を無効にする 1479
グローバルアナリティクスを構成する 1480
カスタムポリシー 1481
グローバルポリシー 1482

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

注意点 1482

アナリティクスの移行 1483

ロールベースのアクセス制御を構成する 1483

NetScaler Consoleでユーザーを構成する 1485

NetScaler Consoleでアクセスポリシーを構成する 1487

ユーザーにStyleBook権限を付与する 1490

NetScaler Consoleでロールを構成する 1490

NetScaler Console でグループを構成する 1492

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 1498

制限事項 1499

管理対象のNetScalerインスタンスにネットプロファイルを割り当てる 1499

前提条件 1500

データストレージ管理 1500

データストレージを理解する 1501

データ取り込みアクティビティの状態 1502

総ストレージ消費量 1502

データプルーニングのステータス 1503

機能別のストレージ消費量 1505

ストレージスペースを管理する 1506

データプルーニングを実行する 1506

データ保持ポリシーの確認 1507

ストレージ制限超過時の通知 1508

データ保持ポリシー 1508

システムアラームの設定と表示 1509

アラームを設定する 1509

ディスク使用率アラームにしきい値制限を追加する 1510

可観測性統合 1511

Splunkとの統合 1511

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

SplunkがNetScaler Consoleからデータを受信するように構成する 1512
NetScaler Consoleを構成してSplunkにデータをエクスポートする 1515
Splunkでダッシュボードを表示する 1517
New Relicとの統合 1517
前提条件 1518
New Relic ダッシュボード 1520
Microsoft Sentinelとの統合 1520
Log Analyticsワークスペースを構成する 1521
Microsoft Entra アプリケーションを作成する 1522
データ収集エンドポイントを構成する 1523
データエクスポート用のテーブルを作成する 1523
NetScaler Consoleでサブスクリプションを作成する 1535
Microsoft Azureでログを表示する 1536
デフォルトスキーマを使用して、Prometheusへのインサイトのエクスポートのために NetScaler®インスタンスを構成する 1536
失敗した構成のログを表示 1537
NetScaler® のメトリクスと監査ログの Splunk へのエクスポートを構成する 1537
失敗した構成のログを表示する 1538
アナリティクス設定の構成 1538
アナリティクス用のしきい値とアラートの作成 1538
通知を構成する 1539
メール配布リストを作成する 1540
SMS配信リストを作成する 1541
Slackプロファイルの作成 1541
PagerDutyプロファイルの作成 1542
ServiceNow プロファイルを確認する 1542
レポートのエクスポートまたはエクスポートレポートのスケジュール設定 1543
レポートをエクスポートする 1543

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

エクスポートレポートのスケジュール設定 1544
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 1544
グローバル設定 1545
インスタンス設定 1545
インスタンス構成の管理 1545
インスタンスバックアップ設定の構成 1546
管理対象デバイスの通知を無効にする 1547
システム構成 1548
エージェントのキープアライブ間隔を設定する 1548
NetScaler Consoleのタイムゾーンを設定する 1548
メール購読 1548
メール通知の購読解除 1549
機能の有効化または無効化 1549
アプリケーションイベント通知を受信するためのアクションポリシーを構成する 1551
アクションポリシーを構成する 1552
検索バーを使用する 1562
監査ログオプションを使用する 1562
監査ログを使用してインフラストラクチャを管理および監視する 1562
NetScaler インスタンス関連の監査ログ 1563
NetScaler Console を syslog サーバーとして構成する 1563
NetScaler Console 関連の監査ログ 1564
アプリケーション関連の監査ログ 1564
IPアドレス管理 (IPAM) の設定 1564
外部IPアドレスプロバイダーを追加する 1565
外部プロバイダーとしてのInfoblox DDI 1566
ネットワークを追加 1567
割り当てられたIPアドレスを表示 1568
ハウツー記事 1570

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

インスタンス管理 1570
構成管理 1570
証明書管理 1571
StyleBooks 1572
イベント管理 1573
よくある質問 1574
いくつのエージェントをインストールする必要がありますか? 1574
複数のエージェントをインストールするにはどうすればよいですか? 1574
NetScalerエージェントはAMDプロセッサをサポートしていますか? 1574
組み込みエージェントから外部エージェントに移行できますか? 1574
アクティベーションコードを紛失した場合、新しいコードを取得するにはどうすればよいですか? 1574
エージェントVMにログオンするにはどうすればよいですか デフォルトの資格情報は何ですか? 1575
オンプレミスのハイパーバイザーにエージェントをインストールするためのリソース要件は何ですか? 1575
プロビジョニング中にエージェントに追加のディスクを割り当てる必要がありますか? 1575
複数のエージェントでアクティベーションコードを再利用できますか? 1575
誤った値を入力した場合、ネットワーク設定を再実行するにはどうすればよいですか? 1575
エージェントの登録が失敗した場合はどうすればよいですか? 1575
登録は成功しましたが、エージェントが正常に動作しているかどうかはどうすればわかりますか? 1576
プロキシサーバーを使用してエージェントをNetScaler Consoleに接続するにはどうすればよいですか? 1576
アナリティクスレポートが表示されません 1577
NetScaler ConsoleでサポートされているNetScalerインスタンスのバージョンは何ですか? 1577
NetScaler Consoleでダッシュボードレポートをエクスポートするにはどうすればよいですか? 1577
クライアント側測定を有効にするとどうなりますか? 1578
エージェントからNetScaler ConsoleサービスへのSSLトラフィックはSSLインスペクションを通過しますか? 1578

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

index 1579

ダッシュボード 1579

アウトバウンドトラフィックダッシュボード 1579

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 1580

ユーザーダッシュボード 1580

ユーザーアクティビティインベスティゲーター 1581

ユーザー トランザクション 1581

リスクスコア 1582

WAFインサイト 1583

WAFインサイトの仕組み 1583

WAFインサイトの構成 1584

セキュリティインサイトレポートの地理的位置を構成する 1585

IPレピュテーションの監視 1586

しきい値 1587

WAF Insight のユースケース 1587

脅威環境の概要を把握する 1587

アプリケーションの既存および不足しているセキュリティ構成を特定する 1588

即座に注意が必要なアプリケーションを特定する 1588

特定の時間における攻撃数を特定する 1588

学習プロファイルを構成する 1589

ネットワーク違反の詳細 1591

HTTP スローロリス 1591

DNS スローロリス 1592

HTTP スローポスト 1592

NXDOMAINフラッド攻撃 1593

HTTP デシンク攻撃 1594

ブライヒェンバッハー攻撃 1595

セグメントスマック攻撃 1595

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

SYNフラッド攻撃 1596
スモールウィンドウアタック 1596
WAF学習アクションの概要を表示 1597
失敗したルールを表示 1597
高度な検索 1597
結果をフィルタリング 1598
緩和ルール、アイドルルール、および拒否ルールを表示する 1598
拒否ルールを管理する 1600
SSLインサイト 1600
前提条件 1601
SSL Insightを構成する 1601
インサイトを有効にする 1602
NetScaler ConsoleからAppFlow機能を有効にする 1602
NetScaler GUI を使用して AppFlow 機能を有効にする 1603
ULFDモードを有効にする 1603
SSL Insightパラメーターを有効にする 1603
NetScaler構成ユーティリティからSSL Insightパラメーターを有効にする 1603
SSL Insightメトリックを表示する 1603
NetScaler ConsoleでSSL Insightメトリックを監視する 1604
ユースケース: SSLトランザクションの概要を取得する 1604
ユースケース: クライアントのSSLメトリック 1604
Webトランザクションの分析を表示する 1605
前提条件 1605
詳細なWebトランザクション 1606
イベントの表示 1607
イベントリストに列を追加 1608
高度な検索 1609
検索を保存 1610

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

データのエクスポート 1611
デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順 1611
NetScalerエージェントを構成する 1611
エージェントで静的ルートを構成する 1611
GitHub からサンプルデプロイファイルをダウンロードする 1613
CPX YAML ファイルにパラメータを追加する 1613
NetScaler ConsoleでVPX、SDX、MPX、またはBLXインスタンスを追加する 1614
NetScaler ConsoleでKubernetesクラスターを追加する 1615
サンプルのマイクロサービスアプリケーションを展開する 1616
CPXを展開し、NetScaler ConsoleにCPXを登録する 1616
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 1617
Webトランザクション設定とTCPトランザクション設定を有効にする 1617
マイクロサービスにトラフィックを送信する 1618
サービスメッシュトポロジをセットアップするための詳細な手順 1618
NetScalerエージェントを構成する 1618
エージェントで静的ルートを構成する 1619
必要なパラメータを設定する 1620
サンプルアプリケーションを展開する 1622
NetScaler ConsoleでKubernetesクラスターを追加する 1623
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 1625
Webトランザクション設定とTCPトランザクション設定を有効にする 1625
マイクロサービスにトラフィックを送信する 1626
シングルティアまたは統合イングレストポロジを設定するための詳細な手順 1627
NetScaler ConsoleでVPX、SDX、MPX、またはBLXインスタンスを追加する 1627
NetScaler ConsoleでKubernetesクラスターを追加する 1627
NetScaler® テレメトリプログラムのデータガバナンス 1628
必須のテレメトリデータ 1630
NetScaler MPXおよびVPXのrootパスワードを変更する方法 1630

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

構成ジョブ機能を使用してパスワードを変更する 1630
ステップ1. **構成テンプレート**を作成する 1631
構成ジョブを作成する 1631
管理者プロファイルの変更 1632
以前のリリース 1632
December 13, 2023 1633
インフラストラクチャ 1633
ライセンス 1633
アナリティクス 1634
インフラストラクチャ 1634
修正された問題 1635
November 29, 2023 1636
インフラストラクチャ 1636
修正された問題 1636
November 09, 2023 1636
アナリティクス 1636
修正された問題 1637
October 25, 2023 1638
分析 1638
インフラストラクチャ 1638
修正された問題 1639
October 10, 2023 1639
管理と監視 1639
September 26, 2023 1640
分析 1640
インフラストラクチャ 1640
修正された問題 1640
分析 1640

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

September 13, 2023 1640
インフラストラクチャ 1640
修正された問題 1641
August 31, 2023 1641
インフラストラクチャ 1641
セキュリティ 1642
修正された問題 1642
管理と監視 1643
August 11, 2023 1643
管理と監視 1643
August 09, 2023 1643
インフラストラクチャ 1643
セキュリティ 1644
修正された問題 1644
July 26, 2023 1645
分析 1645
インフラストラクチャ 1646
StyleBooks 1646
July 18, 2023 1646
管理と監視 1646
July 12, 2023 1647
修正された問題 1647
July 03, 2023 1648
分析 1648
インフラストラクチャ 1648
修正された問題 1648
June 14, 2023 1649
セキュリティ 1649

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

StyleBook 1649
修正された問題 1650
May 31, 2023 1650
アナリティクス 1650
修正された問題 1651
May 18, 2023 1652
アナリティクス 1652
インフラストラクチャ 1652
修正された問題 1652
May 09, 2023 1653
管理と監視 1653
April 25, 2023 1654
分析 1654
StyleBook 1654
修正された問題 1654
分析 1655
April 13, 2023 1655
分析 1655
インフラストラクチャ 1656
修正された問題 1656
April 05, 2023 1657
セキュリティ 1657
修正された問題 1657
March 14, 2023 1658
修正された問題 1658
March 02, 2023 1658
アナリティクス 1658
インフラストラクチャ 1659

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

管理と監視 1659
セキュリティ 1660
アプリケーションパフォーマンス分析 1661
その他 1661
修正された問題 1661
February 07, 2023 1662
分析 1662
管理と監視 1662
修正された問題 1663
January 24, 2023 1663
修正された問題 1663
January 10, 2023 1663
管理と監視 1663
StyleBooks 1664
fix 1665

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

概要

NetScaler Consoleサービス（旧NetScaler ADMサービス）は、NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler CPX、NetScaler BLX、およびオンプレミスまたはクラウドに展開されているNetScaler Gatewayを含むすべてのNetScaler展開を管理するためのウェブベースのソリューションです。

このクラウドソリューションを使用すると、単一の統合された一元的なクラウドベースのコンソールから、グローバルなアプリケーション配信インフラストラクチャ全体を管理、監視、トラブルシューティングできます。NetScaler Consoleは、NetScaler展開におけるアプリケーション配信を迅速にセットアップ、展開、管理するために必要なすべての機能を提供し、アプリケーションの健全性、パフォーマンス、セキュリティに関する豊富な分析機能も備えています。

NetScaler Consoleには、次の利点があります。

- **アジャイル** – 操作、更新、利用が簡単です。NetScaler Consoleのサービスモデルはクラウド経由で利用できるため、NetScaler Consoleが提供する機能を簡単に操作、更新、使用できます。更新頻度と自動更新機能の組み合わせにより、NetScalerの展開が迅速に強化されます。
- **価値実現までの時間短縮** – ビジネス目標の迅速な達成。従来のオンプレミス展開とは異なり、数回のクリックでNetScaler Consoleを使用できます。インストールと構成の時間を節約できるだけでなく、潜在的なエラーに時間とリソースを浪費することも回避できます。
- **マルチサイト管理** – マルチサイトデータセンターにわたるインスタンスを単一の画面で管理。NetScaler Consoleを使用すると、さまざまな種類の展開にあるNetScalerを管理および監視できます。オンプレミスとクラウドに展開されたNetScalerをワンストップで管理できます。
- **運用効率** – より高い運用生産性を達成するための最適化された自動化された方法。NetScaler Consoleを使用すると、従来のハードウェア展開の保守とアップグレードにかかる時間、費用、リソースを節約することで、運用コストを削減できます。
- **リアルタイムインターネットトラフィックの可視化** - リアルタイムインターネットトラフィック分析によるユーザーエクスペリエンスの向上。NetScaler Consoleを使用すると、クライアントがクラウド、データセンター、CDNを介してアプリケーションにアクセスする際のリアルユーザー監視データを収集し、インターネットの健全性の全体像を構築できます。トラフィックは、最適なユーザーエクスペリエンスを確保するために、最も低い遅延と最高の可用性を持つ場所に誘導されます。

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

- **マルチサイトアプリケーション** - 複数のサイトでアプリケーションを作成、構成、配信します。NetScaler Consoleを使用すると、高可用性と信頼性のために、複数のクラウド環境にわたってアプリケーションを構成、配信、管理できます。

NetScaler Consoleの仕組み

NetScaler Consoleは、Citrix Cloud上でサービスとして利用できます。Citrix Cloudにサインアップしてサービスの使用を開始した後、ネットワーク環境にエージェントをインストールするか、インスタンスに組み込まれているエージェントを起動します。その後、管理したいインスタンスをサービスに追加します。

エージェントは、NetScaler Consoleとデータセンター内の管理対象インスタンス間の通信を可能にします。エージェントは、ネットワーク内の管理対象インスタンスからデータを収集し、NetScaler Consoleに送信します。

インスタンスをNetScaler Consoleに追加すると、それは暗黙的にトラップ宛先として自身を追加し、インスタンスのインベントリを収集します。

サービスは、次のようなインスタンスの詳細を収集します。

- 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
- インスタンスで構成されたエンティティなど。

NetScaler Console は、管理対象インスタンスを定期的にポーリングして情報を収集します。詳細については、「データガバナンス」を参照してください。

次の図は、サービス、エージェント、およびインスタンス (MPX、VPX、CPX、BLX) 間の通信を示しています。

NetScaler Console にオンボーディングしてその仕組みを確認するには、「はじめに」とそのサブトピックを参照してください。

機能とソリューション

このドキュメントでは、NetScaler Console でサポートされている機能について説明します。

アプリケーション分析と管理

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

NetScaler Console のアプリケーション分析および管理機能は、アプリケーション中心のアプローチを強化し、さまざまなアプリケーション配信の課題に対処するのに役立ちます。このアプローチにより、アプリケーションの健全性スコアを可視化し、セキュリティリスクを特定し、アプリケーショントラフィックフローの異常を検出し、是正措置を講じることができます。

- アプリケーションパフォーマンス分析: アプリケーションスコアは、アプリケーションのパフォーマンスを定義するスコアリングシステムの成果です。応答性、脅威に対する脆弱性、すべてのシステムの稼働状況など、アプリケーションが適切に動作しているかどうかを示します。
- アプリケーションセキュリティ分析: アプリケーションセキュリティダッシュボードは、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。アプリケーションセキュリティダッシュボードには、検出されたNetScalerインスタンスの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。
- インテリジェントアプリケーション分析: インテリジェントアプリケーション分析機能は、NetScalerアプライア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。インテリジェントアプリケーション分析は、アプリケーショントランザクションのすべてのレベルを監視するだけでなく、機械学習技術を使用してネットワーク内の通常のトラフィックパターンを定義し、異常を検出します。この機能により、全体的なターンアラウンドタイムが短縮され、アプリケーションの全体的な稼働時間が向上します。

StyleBooks

StyleBooks は、アプリケーションの複雑な NetScaler 構成を管理するタスクを簡素化します。StyleBook は、NetScaler 構成を作成および管理するために使用できるテンプレートです。NetScaler の特定の機能を構成するための StyleBook を作成することも、Microsoft Exchange や Skype for Business などのエンタープライズアプリケーション展開用の構成を作成するために StyleBook を設計することもできます。

インスタンス管理

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

イベント管理

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変更が発生すると、イベントが生成され、NetScaler Consoleに記録されます。NetScaler Consoleを使用して構成または表示できる関連機能は次のとおりです。

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

- イベントルールの作成
- NetScaler Console を使用した syslog メッセージのエクスポート

「証明書管理」(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard.html)

NetScaler Consoleは、証明書管理のあらゆる側面を効率化します。単一のコンソールを通じて、適切な発行者、鍵強度、正しいアルゴリズムを保証するための自動ポリシーを確立できるほか、未使用または間もなく期限切れになる証明書を綿密に監視できます。

「構成管理」(/ja-jp/netscaler-console-service/networks/configuration-jobs.html)

NetScaler Consoleを使用すると、構成ジョブを作成して、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複数のインスタンスで簡単に実行できます。構成ジョブとテンプレートにより、最も反復的な管理タスクがNetScaler Console上の単一のタスクに簡素化されます。

「構成監査」(/ja-jp/netscaler-console-service/networks/configuration-audit.html)

インスタンス全体の構成における異常を監視および特定できます。

- 「構成アドバイス」(/ja-jp/netscaler-console-service/networks/configuration-audit/get-configuration-advice-on-network-configuration.html): 構成の異常を特定できます。
- 「監査テンプレート」(/ja-jp/netscaler-console-service/networks/configuration-audit/audit-templates.html): 特定の構成における変更を監視できます。

「ライセンス管理」(/ja-jp/netscaler-console-service/manage-licenses/legacy-license/pooled-capacity.html)

NetScaler Consoleをライセンスマネージャーとして構成することで、NetScalerライセンスを管理できます。

- 「NetScalerプール容量」(/ja-jp/netscaler-console-service/manage-licenses/legacy-license/pooled-capacity.html): NetScalerインスタンスが1つのインスタンスライセンスと必要な帯域幅のみをチェックアウトできる共通ライセンスプールです。インスタンスがこれらのリソースを必要としなくなると、それらを共通プールにチェックインし、必要とする他のインスタンスがリソースを利用できるようにします。
- 「NetScaler VPXチェックイン/チェックアウトライセンス」(/ja-jp/netscaler-console-service/manage-licenses/legacy-license/vpx-check-in-check-out.html): NetScaler Consoleは、NetScaler 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ます。NetScaler VPXインスタンスは、プロビジョニング時にNetScaler Consoleからライセンスをチェックアウトした

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

り、インスタンスが削除または破棄されたときにNetScaler Consoleにライセンスをチェックインしたりできます。

「ネットワークレポート」(/ja-jp/netscaler-console-service/networks/network-reporting.html)

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

「分析」(/ja-jp/netscaler-console-service/analytics.html)

NetScalerインスタンスのデータの様々なインサイトを簡単に、かつスケーラブルに調査し、アプリケーションのパフォーマンスを記述、予測、改善する方法を提供します。1つまたは複数の分析機能を同時に使用できます。

- HDX Insight: 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を使用すると、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。
- Web Insight: 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ます。これにより、IT管理者は、統合されたリアルタイムのアプリケーション監視を提供することで、NetScalerが提供するすべてのWebアプリケーションを監視できます。Web Insightは、近似アルゴリズムを使用してNetScalerからデータを処理します。エンタープライズ内のWebアプリケーションに関連する上位1,000件のメトリックレコードを提供します。
- Gateway Insight: 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障害の可視性を提供します。特定の時間にログオンしているユーザーのリスト、アクティブユーザー数、アクティブセッション数、およびすべてのユーザーが特定の時間に消費したバイト数とライセンス数を確認できます。
- Security Insight: 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 Insight: Web上のセキュアなトランザクション (HTTPs) の可視性を提供します。これにより、IT管理者は、統合されたリアルタイムおよび履歴のWebトランザクション監視を提供することで、NetScalerが提供するすべてのWebアプリケーションを監視できます。SSL Insightは、近似アルゴリズムを使用してNetScalerからデータを処理します。エンタープライズ内のWebトランザクションに関連する上位1,000件のメトリックレコードを提供します。

ロールベースのアクセス制御

ロールベースのアクセス制御 (RBAC) を使用すると、企業内の個々のユーザーの役割に基づいてアクセス権限を付与できます。Citrix Cloud™の資格情報でログオンする組織の最初のユーザーは、

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

デフォルトですべてのアクセス権限を持つスーパー管理者ロールを持ちます。管理者によって後で作成されるその組織の他のユーザーには、管理者以外のロールが付与されます。

サブスクリプション

購入したサブスクリプションのダッシュボードビューを提供します。

デフォルトでは、Expressアカウントに割り当てられます。このアカウントでは、限られたNetScaler Consoleリソースを管理できます。詳細については、「Expressアカウントを使用したNetScaler Consoleリソースの管理」を参照してください。

現在、以下のNetScaler Console機能は利用できません。

- 展開
  - シトリックス インサイト センターからネットスケーラー コンソールへの移行
  - ネットスケーラー コンソールとシトリックス バーチャル デスクトップ ディレクターの統合
- アナリティクス: TCPインサイトとビデオインサイト
- 制限されたシステム設定
- オーケストレーション
  - OpenStackおよびVMware NSX Managerとの統合
  - Cisco ACIのハイブリッドモードにおけるNetScalerの自動化
  - コンテナオーケストレーション: Mesos/MarathonおよびKubernetesとの統合

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

リリースノート

NetScaler Console（旧称：NetScaler ADMサービス）のリリースノートでは、サービスリリースで利用可能な新機能、既存機能の強化、修正された問題、および既知の問題について説明します。

詳細については、以下を参照してください。

- 新機能
- 以前のリリース

NetScalerエージェントは、デフォルトでNetScaler Consoleの最新ビルドに自動的にアップグレードされます。エージェントの詳細は、**Infrastructure > Instances > Agents** ページで確認できます。エージェントのアップグレードを実行する時間を指定することもできます。詳細については、「エージェントアップグレード設定の構成」を参照してください。

新機能

September 27, 2026

管理と監視

CVE-2026-88771の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88771の特定と修復をサポートするようになりました。

- CVE-2026-88771の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、CVE-2026-88771の修復を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

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

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、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。
- このCVEの詳細については、セキュリティ速報を参照してください。

CVE-2026-88772の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88772の特定と修復をサポートするようになりました。

- CVE-2026-88772の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、CVE-2026-88772の修復を参照してください。

  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がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerインスタンスをアップグレードするジョブを使用する」を参照してください。
- CVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-88773 の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88773 の特定と修復をサポートするようになりました。

- CVE-2026-88773 の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-88773 を修復する」を参照してください。

  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がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

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

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerインスタンスをアップグレードするジョブを使用する」を参照してください。
- CVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-88774 の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88774 の特定と修復をサポートするようになりました。

- CVE-2026-88774 の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-88774 を修復する」を参照してください。

  注:

  セキュリティアドバイザリは、End of Life (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- CVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-88775の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88775の特定と修復をサポートするようになりました。

- CVE-2026-88775の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-88775を修復する」を参照してください。

  注:

  セキュリティアドバイザリは、End of Life (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

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

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「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。
- CVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-88776の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88776の特定と修復をサポートするようになりました。

- CVE-2026-88776の特定にはバージョン スキャンが必要です。脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードすることで、修復できます。詳細については、CVE-2026-88776の修復を参照してください。

  注：

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、ジョブを使用してNetScalerインスタンスをアップグレードするを参照してください。
- このCVEの詳細については、セキュリティ速報を参照してください。

CVE-2026-88777の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88777の特定と修復をサポートするようになりました。

- CVE-2026-88777の特定にはバージョン スキャンが必要です。脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードすることで、修復できます。詳細については、CVE-2026-88777の修復を参照してください。

  注：

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

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

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、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。
- このCVEの詳細については、セキュリティ速報を参照してください。

CVE-2026-88778の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-88778の特定と修復をサポートするようになりました。

- CVE-2026-88778の特定にはバージョン スキャンが必要であり、修復には2段階のプロセスが必要です。

  a. 脆弱なNetScalerインスタンスを、修正を含むリリースとビルドにアップグレードします。

  b. 構成ジョブを適用します。

  詳細については、「CVE-2026-88778の修復」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- このCVEの詳細については、「セキュリティ速報」を参照してください。

September 15, 2026

修正された問題

分析

NetScalerによってメトリック更新が再送信されると、NetScaler Consoleでアプリケーションに表示される帯域幅とボリュームの合計が過少報告される場合があります。

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

インフラストラクチャ

Cloud Connectを使用すると、NetScaler Consoleオンプレミスで構成された顧客IDがNetScaler Consoleサービス内の顧客IDの大文字/小文字と一致しない場合、ライセンスエンタイトルメントの取得に失敗します。

Consoleの組み込みエージェントによって管理されているNetScaler HAセットアップでは、そのNetScalerが古いビルドを実行している場合、セカンダリノードで組み込みエージェントが起動に失敗する可能性があります。フェイルオーバーが発生した場合、NetScaler ConsoleでHAペアが「ダウン」と表示される可能性があります。

September 01, 2026

新機能

管理と監視

- **証明書ソースの可視性およびバインドされた証明書の保護**

  証明書ファイルにそのソースが表示されるようになり、管理者は以下を区別できるようになりました。

  - **ローカル**: NetScalerにローカルにインストールされた証明書 (直接、または証明書ストアを介してインストールされた証明書を含む)。
  - **リモート**: Zero Touch Certificate Management (ZTCM) を介して管理および取得された証明書。

  この機能強化により、証明書の発生元と管理ワークフローに関する可視性が向上します。

  バインドステータスインジケータは、証明書インベントリの新しいステータスインジケータであり、現在SSL構成にバインドされ、アクティブに使用されている証明書を識別します。この機能強化により、管理者はライフサイクル操作を実行する前に証明書の依存関係を明確に把握できます。

  安全な削除により、管理者は証明書インベントリから証明書ファイルを直接削除できます。サービスの中断を防ぐため、削除はバインドされていない証明書のみに制限されます。バインドを解除するまで、SSLエンティティにアクティブにバインドされている証明書や、証明書ワークフローによって管理されている証明書は削除できません。

- **SSL証明書向けの統合された証明書ソースエクスペリエンスと証明書インポートの事前チェック**

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

NetScaler Consoleは、異なるソースからの証明書ファイルを単一のビューに統合することで、統合された証明書選択エクスペリエンスを提供するようになりました。以前は、管理者は個別の**NetScaler上のファイル**と**Console上のファイル**オプションの間で選択する必要がありました。この機能強化により、証明書ファイルは単一の統合されたワークフローを通じて表示され、証明書の管理と選択が簡素化されます。さらに、ユーザーエクスペリエンスを合理化し、ソース選択の複雑さを軽減するために、証明書アップロードオプションはこのワークフローから削除されました。

NetScaler Consoleは、NetScalerインスタンス全体にSSL証明書とキーをインポートする前に、意図しないファイル競合や証明書の上書きを防ぐための事前検証チェックも実行します。

この機能に関連する主な機能強化は次のとおりです。

- **重複ファイル検出**: インストール前に、システムは証明書またはキーファイル名が宛先NetScalerインスタンスに既に存在するかどうかを検証します。ファイル名が競合する宛先は、展開前に特定され、フラグが立てられます。
- **上書き保護**: 証明書のインポートは、既存の証明書またはキーファイルを上書きしなくなりました。競合が検出された場合、インポートはブロックされ、管理者は別のファイル名を使用するか、重複を削除することで競合を解決する必要があります。
- **宛先ごとの検証**: 一括証明書インポートの場合、各宛先インスタンスは個別に評価されます。管理者は、どの宛先がインストールに適格であるか、または不適格であるかを確認し、有効なターゲットのみで続行できます。
- **バックエンドの安全性検証**: インストール中に、宛先の適格性が変更されていないことを確認するために、追加の検証が実行されます。証明書は、最終検証チェックに合格したインスタンスにのみインストールされます。

この機能強化の利点は次のとおりです。

- 既存の証明書と秘密鍵の偶発的な上書きを防ぎます。
- ファイルの置き換えによって引き起こされる証明書チェーンの中断のリスクを軽減します。
- 複数のNetScalerインスタンスにわたる展開準備状況の可視性を向上させます。
- より安全で予測可能な証明書展開エクスペリエンスを提供します。

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

修正された問題

アナリティクス

Web App FirewallおよびBOTしきい値違反の電子メールアラートが送信されません。これは、ジョブが常に空である誤ったIPアドレス列を読み取っているためです。

NetScaler Consoleアナリティクススケジューラは、最初のプッシュで構成が正常に適用された場合でも、NetScalerインスタンスに構成設定を繰り返しプッシュします。この問題により、すべてが正常に機能しているにもかかわらず、誤った障害アラートがトリガーされます。

NetScaler Consoleの監査ログは、文書化された`console_syslog_messages_CL`ではなく宣言されていないストリームに送信された場合、Microsoft Sentinelに到達しない可能性があり、Azureがすべてのバッチを拒否する原因となります。

インフラストラクチャ

スタイルブック操作の資格情報を要求オプションが有効になっている場合、ユーザーはNetScalerでWAFの推奨事項を適用できません。

Azure環境では、NetScalerからNetScaler Consoleクラウドエージェントに送信されたSNMPv3トラップが、「不明なユーザー名」認証エラーで失敗する場合があります。

管理対象のNetScalerインスタンスがファイル整合性監視スキャンに適格でない場合、NetScaler Consoleは誤った脆弱性通知を送信し、これらのスキャンに関するSlack通知は空白で、スキャン詳細がありません。

NetScaler Consoleエージェントが設定されたプロキシを介してトラフィックをルーティングできない場合があり、エージェントとNetScaler Console間の接続問題を引き起こす可能性があります。

GSLBサイトグループが設定されている場合、GSLB仮想サーバーエントリがNetScaler Consoleの仮想サーバーリストに表示されないことがあります。

NetScaler Consoleは、スループットレート制限によるパケットドロップを誤って表示します。

選択されたインスタンスの構成監査ポーリング中に、NetScaler Consoleは、代替構成をダウンロードする前にキャッシュされたインスタンス構成を削除しました。その結果、ポーリング期間中、構成は利用できませんでした。ポーリングが失敗した場合、構成は次の正常な実行まで利用できませんでした。

Azureデバイスでの`mastools`登録中に、NetScaler Consoleは`mastools_reg.py`ログにエラーを記録します。ただし、このエラーはAzureデバイスのmastools登録をブロックしません。

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

August 19, 2026

管理と監視

CVE-2026-19489の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-19489の特定と修復をサポートするようになりました。

- CVE-2026-19489の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-19489の修復」を参照してください。

  注記：

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、ジョブを使用してNetScalerインスタンスをアップグレードするを参照してください。
- CVE の詳細については、セキュリティ速報を参照してください。

CVE-2026-19490 の特定と修復のサポート

NetScaler Console サービス セキュリティアドバイザリは、CVE-2026-19490 の特定と修復をサポートするようになりました。

- CVE-2026-19490 の特定にはバージョン スキャンが必要です。修復には、脆弱な NetScaler インスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、CVE-2026-19490 を修復するを参照してください。

  注記：

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

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

- NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、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。
- CVE の詳細については、セキュリティ速報を参照してください。

August 04, 2026

新機能

管理と監視

- **NetScaler VPX Linuxベースプラットフォームのファイル整合性監視サポート**

  ファイル整合性監視機能が、Linuxプラットフォーム上のNetScaler VPXインスタンスでサポートされるようになりました。この機能により、不正なファイルや構成の変更を簡単に検出できます。

修正された問題

分析

NetScaler Consoleで設定されたWeb Application FirewallおよびBOTポリシーが数日後に消え、ポリシーを手動で編集または切り替えた後にのみ再表示されます。

インフラストラクチャ

NetScaler ConsoleでDNS-01ドメイン検証にInfoblox DNSプロバイダーを使用すると、ドメイン検証中にACME証明書の発行と更新が失敗します。

NetScaler Consoleの**ゼロタッチ証明書管理**ページで、**カスタム同期**から**グローバル同期**への変更が失敗する場合があります。インスタンスはカスタム同期のままになります。

SSLダッシュボードからSSL証明書をダウンロードしようとすると、`404 - File not found error`で失敗します。これは、証明書がNetScaler®に存在し、その詳細がNetScaler Consoleで表示されている場合でも発生します。この問題は、`/nsconfig/ssl/`の下のサブディレクトリに保存されている証明書に特に影響します。

インベントリコアダンプが発生すると、NetScaler Console はエージェントをダウンとして報告します。

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

July 14, 2026

新機能

管理と監視

- **NetScaler ConsoleとエージェントGeoIPデータベース同期**

  NetScaler Consoleサービスは、単一のワークフローからNetScaler Console、展開されたエージェント、および管理対象インスタンス向けの一元化されたGeoIPデータベース同期をサポートするようになりました。以前は、同期はNetScalerインスタンスのみに限定されていました。

  GeoIP同期機能には、次の機能が含まれています。

  - **統合同期**: 単一の操作でGeoIPデータベースファイルをNetScaler Console、エージェント、およびインスタンスに同期します。
  - **今すぐ同期**: オプションは2つのモードをサポートしています。
    - **すべて同期**: 管理対象のNetScalerインスタンス、NetScaler Console、およびエージェントなど、すべてのエンティティにファイルを自動的にプッシュします。
    - **カスタマイズ**: 特定のConsoleエージェントを選択します。
  - **スケジュールされた同期**: 任意のエンティティタイプの組み合わせを対象とする、1回限りまたは定期的な同期スケジュールを作成します。
  - **履歴ジョブログ**: 過去の同期ジョブのタイムスタンプ付きログを表示します。これには、スコープ、使用されたファイル、およびデバイスごとの結果（ステータス、開始時刻、終了時刻）が詳細に示されます。
  - **エンティティごとの同期ステータス**: メインページで展開可能なパネルにアクセスして、ステータス、IPアドレス、エンティティタイプ、またはバージョンでフィルタリング可能なデバイスごとの同期結果を表示します。
  - **最終同期の概要**：選択されたエンティティの総数、保留中、進行中、成功、失敗、および全体の完了率を表示する一目でわかる概要で、同期の状態を迅速に評価します。

テレメトリ

- **テレメトリ診断のサポート**

  NetScaler Consoleサービスは、管理対象のNetScalerインスタンス全体でテレメトリの収集とアップロードに関する問題を管理者が迅速に特定し、トラブルシューティングできるように、

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

テレメトリ診断をサポートするようになりました。この機能により、詳細なテレメトリの洞察、デバイスおよびエージェントレベルのステータス可視性、修復ガイダンス付きのエラーコード、およびライブ接続検証チェックが導入されます。

管理者は、テレメトリのアップロード失敗がデバイスの到達可能性、SSH接続、エージェント通信、テレメトリパッケージの問題、またはサービス接続の問題によって引き起こされているかどうかを簡単に判断できるようになりました。これにより、トラブルシューティングの時間を短縮し、テレメトリのカバレッジを向上させることができます。

主な利点は次のとおりです。

- 管理対象のNetScalerインスタンスのテレメトリステータスを表示します。
- エラーコードと軽減策のガイダンスを含む詳細な障害診断にアクセスします。
- エージェントのテレメトリの状態とパッケージの実行の詳細を監視します。
- テレメトリ関連のエンドポイントとサービスのライブ接続チェックを実行します。

修正された問題

分析

NetScaler Consoleオンプレミスをクラウドに移行した後、影響を受けるNetScalerの詳細なWebトランザクションレコードが表示されず、メトリックやボットデータなどの他の分析は通常どおり表示され続けます。この問題は、これらのトランザクションに必要なストレージが、移行されたテナントに対して完全にプロビジョニングされていなかったために発生しました。

インフラストラクチャ

NetScaler Consoleは、NetScalerインスタンス上で定期的にLASをアクティブ化します。これにより、トークン更新中に/nsconfig/license/下のファイルが変更され、Config Audit File Diffで誤検知の「Diff Exists」アラートが発生します。

NetScaler Consoleクラウドエージェントは、送信元IPアドレスを含まないイベントログを生成します。これらのイベントの送信元フィールドは、イベントを開始したエージェントまたはデバイスのIPアドレスを表示する代わりに、空白で表示されます。

証明書名が2つの16進文字（例：de、ab、ce、または25）で始まるSSL証明書をNetScaler Console SSLダッシュボードを使用してダウンロードすると、「404 - ファイルが見つかりません」エラーで失敗します。この問題は、SSL証明書がNetScaler上に存在し、その詳細がNetScaler Consoleで表示されている場合でも発生します。

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

NetScaler Consoleサービスで、ユーザーとロールの下のユーザーグループを編集する際に、「無効なリソース」エラーが発生する可能性があります。

その他

まれなシナリオでは、NetScaler Consoleがエージェント経由でNetScalerに接続できません。その結果、データベースの更新が正しくないために、NetScalerがGrace状態として報告される可能性があります。

June 30, 2026

管理と監視

CVE-2026-8451の識別と修正のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、現在、CVE-2026-8451の識別と修正をサポートしています。

- CVE-2026-8451の識別にはバージョンスキャンが必要です。修正には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-8451の修正」を参照してください。

  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がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- このCVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-8452の識別と修正のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、現在、CVE-2026-8452の識別と修正をサポートしています。

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

- CVE-2026-8452の識別にはバージョンスキャンが必要です。修正には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-8452の修正」を参照してください。

  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がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- このCVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-8655の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-8655の特定と修復をサポートするようになりました。

- CVE-2026-8655の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-8655を修復する」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- CVEの詳細については、「セキュリティ速報」を参照してください。

CVE-2026-10816の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-10816の特定と修復をサポートするようになりました。

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

- CVE-2026-10816の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-10816を修復する」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- CVEの詳細については、セキュリティ速報を参照してください。

CVE-2026-10817の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-10817の特定と修復をサポートするようになりました。

- CVE-2026-10817の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-10817の修復」(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-10817.html)を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、ジョブを使用してNetScalerインスタンスをアップグレードするを参照してください。
- CVEの詳細については、セキュリティ速報を参照してください。

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

June 17, 2026

修正された問題

分析

仮想サーバーでBOT Insightを有効にしてもメトリクスを有効にしない場合、NetScaler ConsoleはBOT違反を処理しません。この問題は、BOT違反の処理がメトリクスの有効化に依存しているために発生します。

「**Analytics**」ページで、ユーザーは、特定のユーザーに対して定義されたユーザー、ロール、グループ、およびアクセスポリシーに基づいてアクセスが許可されている特定のインスタンスに加えて、他のインスタンスも表示される場合があります。

インフラストラクチャ

「**Prompt credentials for stylebook operations**」オプションが有効になっている場合、ユーザーはNetScalerでWAFの推奨事項を適用できません。

まれに、最初にKB単位のサイズで生成されたバックアップファイルにアクセスまたはダウンロードしようとすると、エラーが発生します。

Microsoft Entra ID (Azure AD) ユーザーが、すでにオンボーディングされているCitrix Cloudテナントで NetScaler Consoleサービスにサインインすると、そのユーザーのMicrosoft Entra IDグループにマッピングされているロールではなく、デフォルトの `adminExceptSystem` ロールが割り当てられます。その結果、影響を受けるユーザーは意図したよりも広範な権限を受け取ります。

クラウドプロバイダーが過大なサイズの証明書を提示すると、NetScaler Consoleエージェントがクラッシュします。

NetScaler Consoleサービスでは、GoDaddy CAはサポートされていません。

ライセンス

NetScalerインスタンスが削除されてから再度追加された場合、NetScaler Consoleは、そのNetScalerインスタンスのLASライセンスを自動的に再開しません。

拡張ブロブ内のホストIDがNetScaler Console GUIのホストIDと(大文字と小文字を区別して)正確に一致しない場合、NetScaler Consoleは拡張ブロブを拒否します。

プールされたライセンスに異なるSubscription Advantage (SA)の日付を持つエンタイトルメントが含まれている場合、NetScaler Consoleは、有効期限切れ警告ごとに単一の通知を送信する代わりに、ライセンス有効期限切れアラートメールを繰り返し (数秒ごとに1回程度) 送信します。

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

June 03, 2026

修正された問題

インフラストラクチャ

NetScaler Consoleを介して開始されたNetScaler BLXインスタンスのアップグレードは、NetScaler BLXインスタンスが稼働中であっても失敗します。この問題は、アップグレード前のチェックがインスタンスに到達不能であると誤って報告するため発生し、アップグレードの正常な完了を妨げます。

NetScaler Console Security Advisoryページで、CVE検出は各インスタンスのCVE数を表示しますが、CVE数をクリックしても詳細が読み込まれません。

SSLダッシュボードで、ACMEワイルドカード証明書の発行が失敗する場合があります。

ライセンス

プールライセンスモードでは、NetScaler SDXデバイスの場合、Platinumエディションのみが割り当てられます。値が指定されていても、StandardおよびAdvancedエディションは割り当てられません。

May 19, 2026

管理と監視

重複する証明書の競合管理のサポート

NetScalerは、インストールおよび更新プロセス中に重複する証明書名とコンテンツによって引き起こされる競合の防止をサポートするようになりました。重複する証明書名またはコンテンツの管理は、証明書をインストールまたは更新する際に不可欠です。これらの重複は構成の競合につながる可能性があるためです。この機能により、システムはクリーンで一意の証明書リポジトリを維持し、管理タスクを簡素化し、システムの信頼性を向上させます。

中間アップロードなしでサーバー証明書を更新

中間証明書を再アップロードするという反復的な作業なしで、証明書を更新できるようになりました。この機能強化により、手作業が軽減され、構成エラーのリスクが最小限に抑えられます。

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

簡単な更新

NetScaler Consoleは、更新時に既存の証明書チェーンをデフォルトで保持するようになりました。これにより、新しいサーバーレベルの証明書のみをアップロードした場合でも、チェーンが損なわれず有効な状態に保たれます。

主な改善点

- 複雑さの軽減: 標準的なサーバー証明書の更新時における必須の中間アップロードを排除します。
- 安全第一: 自動チェーン保持により、SSLハンドシェイクエラーの一般的な原因である「チェーンの破損」を防ぎます。

新しいパラメータ

以下のパラメータは、単純な更新以上の要件がある場合に、明示的な制御を提供します。

パラメータ	機能
既存の証明書チェーンを上書きする	これを使用して、現在のチェーンを置き換えたり削除したりします。バンドルありの場合: 既存のチェーンを新しくアップロードされたチェーンに置き換えます。バンドルなしの場合: 現在のチェーンを削除します。
証明書チェーンを追加する	プライマリサーバー証明書ファイルに含まれていない中間証明書を手動でアップロードして追加するには、これを選択します。

中間アップロードなしでサーバー証明書を更新する方法については、「NetScaler Console証明書ストアを使用してSSL証明書を管理する」を参照してください。

カスタムSNMPトラップのサポート

NetScaler Consoleサービスは、カスタムSNMPトラップをサポートするようになりました。カスタムSNMPトラップは、**イベントメッセージ**の下で表示でき、デフォルトのSNMPアラートと区別できるようにカスタムとしてタグ付けされています。

関連トピック: イベント。

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

アップグレードジョブ: 重複するアップグレードジョブスケジュールに関する警告

アップグレードジョブのワークフローの一部として、顧客がすでに既存のアップグレードジョブがスケジュールされているNetScalerインスタンスに対してアップグレードジョブを作成しようとすると、NetScaler Consoleは警告メッセージを表示します。この警告メッセージは、同じNetScalerインスタンスで意図せずに重複するアップグレードジョブがスケジュールされるのを防ぐのに役立ちます。この機能強化により、アップグレードジョブの制御が向上し、アップグレード中の潜在的な競合が回避されます。

関連トピック: アップグレードジョブ。

ACMEベースの自動証明書更新における追加の証明書認証局とDNSプロバイダーのサポート

NetScaler Consoleの自動証明書管理環境 (ACME) 統合による自動証明書更新は、より多くの証明書認証局 (CA) とDNSプロバイダーをサポートするようになりました。サポートされているCAまたはDNSプロバイダーのいずれかを使用している場合、ACME統合を活用してシームレスな証明書管理を行うことができます。

サポートされている証明書認証局 (CA) とDNSプロバイダーの完全なリストについては、ACMEプロトコルを使用した自動証明書更新を参照してください。

ファイル整合性監視ダッシュボードにスキャンエラーが表示される

ファイル整合性監視 (FIM) ダッシュボードに、スキャンエラーの結果がメインダッシュボードビュー内に直接表示されるようになりました。エラーの詳細にアクセスするために、個々のスキャン結果や項目をクリックする必要はありません。ハッシュの不一致やスキャンエラーなどの整合性に関する問題は、ダッシュボード自体に明確でアクセスしやすい形式で表示されます。この機能強化により、トラブルシューティングプロセスが合理化され、問題を一目で迅速に特定して理解できるようになります。その結果、整合性に関する問題に効率的に対応し、時間を節約し、ワークフロー全体の透明性を向上させることができます。

関連トピック: ファイル整合性監視。

侵害の痕跡 (IoC) 検出のサポート

NetScaler Consoleの侵害の痕跡 (IoC) 検出機能は、NetScalerアプライアンスが脆弱性のために潜在的に影響を受けているかどうかを検出するように設計されています。

CVEイベントが発生した場合、最初の懸念事項の1つは、悪意のあるアクターが脆弱性を悪用することです。エクスプロイトは顧客のビジネスに壊滅的な損害をもたらすため、そのようなインシデントを直ちに検出することが重要です。過去には、NetScalerのIoCはサポートチャネルを通じて配布されていましたが、これは顧客のニーズを満たすものの、チケットの発行、サポート担当者と

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

の会話といったサポートプロセスを経る追加の労力が必要であり、場合によっては理想的ではありませんでした。NetScaler ConsoleのIoC検出機能は、現在のサポート指向のプロセスを短絡させ、顧客がNetScalerインフラストラクチャを迅速に評価するのに役立つように設計されています。

詳細については、NetScaler Consoleでの侵害の痕跡検出を参照してください。

SSLフィルターモードのサポート

NetScalerインスタンスは、特定のSSL証明書と秘密鍵のメタデータを取得できるようになりました。この「最小特権」アプローチを実装することで、インスタンスが必要なアセットのみにアクセスできるようになり、1つのインスタンスの侵害によって証明書インフラストラクチャ全体が公開されるのを防ぎます。この機能は、複数の管理者が異なる目的でNetScalerインスタンスのグループを管理する環境で特に役立ちます。

利点は次のとおりです。

- **セキュリティセグメンテーション**: NetScalerごとのレベルでメタデータアクセスを制限し、攻撃対象領域を最小限に抑え、組織のセキュリティポリシーに準拠します。
- **合理化された管理者エクスペリエンス**: 管理者に、自身のNetScalerインスタンスグループに関連するアセットのみを表示することで、マルチテナントまたは部門別展開における複雑さを軽減します。
- **最適化されたリソース利用**: 必要なSSL証明書と秘密鍵のメタデータのみを取得することで、システムメモリの肥大化を防ぎます。

フィルターモード構成は、NetScalerインスタンスとSSLファイルが特定の同期タイプを介してどのように相互作用するかを定義します。これらの設定はNetScaler Consoleを通じて管理でき、各インスタンスが必要なメタデータのみを取得するようにします。

コンポーネント	同期タイプ	説明
NetScalerインスタンス	カスタム同期	このモードのNetScalerインスタンスは、インスタンスに具体的にマッピングされた証明書とキーのメタデータのみを取得します。
NetScalerインスタンス	グローバル同期	このモードのNetScalerインスタンスは、アップロードされたすべての証明書と秘密

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

コンポーネント	同期タイプ	説明
		キーのメタデータをフェッチします。
SSLファイル	カスタムファイル	これらのファイルは、カスタム同期モードのNetScalerインスタンスに具体的にマッピングされます。
SSLファイル	グローバルファイル	これらのファイルのメタデータは、グローバル同期モードのすべてのNetScalerインスタンスによってフェッチされます。

フィルターモード設定の構成

フィルターモードを構成するには、インスタンスとファイルの同期タイプを定義します。これにより、機密性の高いメタデータの安全で最適化された配布が保証されます。

GUIを使用して構成するには：

1. **新しいファイルのアップロード（Day Zero）**: 新しいアセットを追加するには、**証明書ファイルとNetScalerインスタンス > アップロード**に移動します。次のいずれかの同期タイプを選択します。
   - **GLOBAL**: グローバル同期モードを使用することを選択し、アップロードを完了します。
   - **CUSTOM**: カスタム同期モードを使用することを選択し、マッピングする特定のインスタンスを選択してから、ファイルをアップロードします。
2. **既存ファイルの移動（Day N）**: 証明書とキーをグローバル同期モードからカスタム同期モードに移行するには、ターゲットのNetScalerインスタンスを選択し、**既存ファイルの追加**をクリックします。
3. **ドメインの選択**: インスタンスが選択されたら、関連するドメインを選択して移行をトリガーします。NetScaler Consoleは、対応する証明書と秘密キーファイルを自動的に検出し、カスタム同期モードに移行します。
4. **アセットの表示**: ランディングページに移動して、カスタム同期モードで各NetScalerインスタンスにマッピングされているすべての証明書とプライベートキーファイルを表示します。
5. **同期モードの切り替え**: インスタンスをグローバル同期モードに戻すには、ランディングページで「**Switch to Global Sync**」をクリックします。

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

修正された問題

分析

- ユーザーが「0」を含むIPアドレス（例：10.0.2.3）でホストされているサーバー上でICAセッションを起動すると、NetScaler ConsoleはIPアドレスを10.2.3と表示します。

インフラストラクチャ

- NetScaler ConsoleオンプレミスでCloud Connectの切断操作が失敗する場合があります。GUIではCloud Connectが切断されていると表示されていても、NetScaler Consoleオンプレミスインスタンスは NetScaler Consoleサービスに接続されたままになります。このため、オンプレミスインスタンスは NetScaler Consoleサービスで「稼働中」と表示されます。

- まれに、ファイル整合性監視 (FIM) のスキャン結果がエラーを報告する場合があります。

- まれに、テレメトリの再試行メカニズムが、成功した操作後に終了しないことがあり、その結果、NetScalerデバイス上でテレメトリプロセスが重複して実行されることがあります。これは、テレメトリの収集や転送に機能的な影響はありません。

- NetScaler Consoleでは、違反数グラフにはデータが反映されているにもかかわらず、アプリケーションセキュリティ違反ログの詳細がロードされない場合があります。

- Redisインスタンスが認証済みモードから未認証モードに移行し、サービスが古い認証資格情報を使い続けると、接続障害が発生します。

- パスワードで暗号化されたキーファイルを追加しようとすると、NetScaler Consoleサービスに「Invalid key file password」エラーが表示されることがあります。

- アプリケーションがユーザーグループに関連付けられており、NetScaler仮想サーバーの名前が変更されると、アプリケーションはユーザーグループから自動的に削除されます。これにより、ユーザーグループの構成に矛盾が生じます。

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

March 31, 2026

管理と監視

設定監査からファイルを除外する

特定のファイルを構成監査から除外して、変更が監視されないようにできるようになりました。システム生成ファイルや頻繁に更新されるファイル（たとえば、毎日変更されるファイル）を除外することで、監査結果のノイズを減らし、誤検出を回避できます。

設定監査ファイル差分から除外するファイル名（または相対パス）の例：

- 有効なファイル名（または相対パス）
  - `ns.conf`, `ssl/ns.cert`
- 無効なファイル名（または相対パス）
  - `/ns.txt`, `\nsconfig\ns.conf` (除外されるファイル名は相対パスである必要があります)
  - `ns.conf` (除外されるファイル名にはASCII文字のみを含める必要があります)
  - `C:/nsconfig/ns.conf` (除外されるファイル名にはドライブレターパスを使用しないでください)
  - `ssl/../../ns.conf` (除外されるファイル名には親ディレクトリトラバーサル (`..`) を含めないでください)

注:

- ファイルの差分比較は、`/nsconfig` ディレクトリ内のファイルにのみ適用されます。
- Config Audit からファイルを除外する場合、ユーザーは `/nsconfig` の下の相対パスを指定する必要があります。たとえば、`/nsconfig` の下に `ssl` フォルダーがある場合、除外は次のように指定できます: `ssl/abc.pem`
- `/nsconfig` 以外のファイルの差分は、Config Audit の差分の一部とは見なされません。

Config Audit からファイルを除外するには、次の手順を実行します。

1. **インフラストラクチャ > 構成 > 構成監査** に移動します。
2. **Settings** を選択します。
3. **NetScaler Config File Settings** で、監査から除外するファイルパスを追加します。

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

4. **Save** をクリックします。

LAS のインスタンスレベル RBAC サポート

NetScaler Console on-prem は、LAS のインスタンスレベルでロールベースのアクセス制御 (RBAC) をサポートするようになりました。以前は、管理者はすべてのデバイスのライセンスにアクセスでき、セキュリティリスクや運用上のオーバーヘッドにつながる可能性がありました。この機能強化により、管理者は特定の NetScaler インスタンスへのアクセスを制限できるようになります。その結果、管理者はアクセスを許可された特定の NetScaler インスタンスのライセンスのみを管理します。この変更により、ライセンスタスクが NetScaler Console on-prem の他の管理アクティビティと同じセキュリティ境界に従うことが保証されます。

利点の一部を以下に示します。

- **セキュリティの向上**: ライセンス操作を、管理者に割り当てられたスコープ内のデバイスのみに制限します。
- **きめ細かな運用管理**: 管理者が意図せずに不正なインスタンスのライセンスを変更できないようにします。
- **ワークフローの整合性**: ライセンス管理を確立された RBAC 構造とシームレスに統合します。

関連トピック:

- RBAC の構成方法については、「ロールベースのアクセス制御」を参照してください。
- ライセンス管理については、「ライセンス管理」を参照してください。

修正された問題

分析

HA セットアップでは、WAF または Bot ポリシーで保護されたアプリケーションが、スケジュールされた EMON ポーリング後に ADM セキュリティダッシュボードから断続的に消えることがあります。この問題は、内部データ相関の不一致が原因で発生します。

インフラストラクチャ

NetScaler FIPS アプライアンスは、組み込みエージェントを使用して Government Cloud の NetScaler Console サービスに接続できない場合があります。

タスクと推奨事項で、セキュリティアドバイザリタスクを選択した後、選択したCVEまたは影響を受けるインスタンスの**表示と修復**をクリックすると、空のページが読み込まれます。

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

LAS移行ワークフロー中に、NetScaler ConsoleサービスUIが内部エージェントによって管理されるHAペアのホスト名を表示できない場合があります。

組み込みエージェントを使用してConsoleサービスに登録されているNetScalerインスタンスのHAセットアップでは、agent_idが欠落している場合、これらのインスタンスのリリース割り当てが失敗する可能性があります。

March 23, 2026

管理と監視

CVE-2026-4368の識別と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-4368の識別と修復をサポートするようになりました。

- CVE-2026-3055の識別にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2026-4368を修復する」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- CVEの詳細については、Security Bulletinを参照してください。

CVE-2026-3055の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2026-3055の特定と修復をサポートするようになりました。

- CVE-2026-3055の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、Remediate CVE-2026-3055を参照してください。

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

注:

セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Use jobs to upgrade NetScaler instancesを参照してください。
- CVEの詳細については、Security Bulletinを参照してください。

March 09, 2026

新機能

管理と監視

- **PEM形式の秘密鍵に対するAES暗号化**

  NetScaler Consoleサービスは、証明書署名要求（CSR）を作成する際に、PEMエンコーディングアルゴリズムとしてAdvanced Encryption Standard（AES）をサポートするようになりました。CSRを生成して新しい秘密鍵を作成する際、AES256を選択してPEM形式の秘密鍵を暗号化および保護できます。これにより、既存のDESおよび3DESオプションよりも安全な代替手段が提供されます。この機能強化により、秘密鍵が最新の業界標準暗号化アルゴリズムを使用して保護されることが保証されます。

  以下に利点を示します。

  - **セキュリティの強化**: 従来のDESベースの方式と比較して、秘密鍵保護のためのより強力な暗号化を提供します。
  - **コンプライアンスへの準拠**: 組織が、AESベースの暗号化を義務付ける最新のセキュリティベストプラクティスおよび規制要件を満たすのに役立ちます。
  - **将来性への対応**: CSR生成を、業界全体で広く採用されている現代の暗号化標準に合わせます。

  CSR生成中のPEMエンコーディングアルゴリズムの設定に関する情報については、「証明書署名要求 (CSR) の作成」を参照してください。

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

その他

- **セカンダリHAノードアップグレードの柔軟なスケジュールオプション**

  Infrastructure > Upgrade Jobsでジョブを作成する際、最初のノードアップグレードが完了してから2番目のノードアップグレードが開始されるまでの遅延時間（時間単位）を指定できます。このオプションは、以下のシナリオで役立ちます。

  - 最初のノードをテストおよび検証するために追加の時間が必要な場合
  - アップグレードの進行が、固定された時刻ではなく、運用準備状況に依存する場合
  - タスクを手動で再スケジュールすることなく柔軟性が必要な場合

  以前は、固定タイムスタンプオプションの定義のみが可能でした。固定タイムスタンプオプションのみの場合、最初のノードアップグレードが遅延すると、2番目のノードのスケジュールされた時間が経過し、アップグレードが開始されませんでした。

修正された問題

アナリティクス

- RBACポリシーの設定時に、NetScaler ConsoleサービスGUIでWAF推奨オプションが表示されない場合があります。

- **Analytics**ページで、特定のユーザーに対して定義されたユーザー、ロール、グループ、およびアクセスポリシーに基づいてアクセスが許可されている特定のインスタンスのみが表示されるのではなく、すべてのインスタンスが表示される場合があります。

インフラストラクチャ

- NetScaler Consoleオンプレミスをバージョン14.1-60.54にアップグレードした後、すべてのSDXアプライアンスのテレメトリステータスに2500および3300の内部エラーが表示される場合があります。

- POCOライブラリのアップグレードにより、アップグレード後にNetScaler Consoleエージェントが継続的にクラッシュします。

- NetScaler Consoleサービスの証明書同期がHTTP 28エラーで失敗する場合があります。この問題は、Zero-Touch機能が有効になっている場合に発生し、Consoleが応答する前にリクエストが10秒でタイムアウトし、同期プロセスが中断されます。

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

その他

NetScaler Consoleサービスは、LASベースのライセンスを使用して20 MbpsでNetScaler VPXのライセンスを付与することをサポートしていません。

```
[ NSHELP-42109 ]
```

February 20, 2026

新機能

アップグレード前検証チェックの一部削除

以下のNetScaler Consoleのアップグレード前チェックが、アップグレードジョブのワークフローから削除されました。

- **ユーザーカスタマイズチェック**: 既存のユーザーカスタマイズ（起動スクリプトやcronジョブなど）が、インストール中またはインストール後にシステム動作に影響を与える可能性があるかどうかのチェック。
- **HDDエラーチェック**: ディスク関連のエラー、I/O障害、タイムアウト、ファイルシステムの問題など、インストールの安定性に影響を与える可能性のあるシステムおよびカーネルログのチェック。
- **高可用性 (HA) 構成チェック**: HAノード間の構成同期チェック。

上記のチェックは古く、リソースを大量に消費していました。これらのチェックを削除することで、アップグレードのパフォーマンスが向上し、システムオーバーヘッドが削減され、誤ったアップグレード失敗が最小限に抑えられます。一方、すべての重要な検証チェックは引き続き実施されます。

アップグレード前チェックの詳細については、「アップグレードジョブ」を参照してください。

修正された問題

インフラストラクチャ

セキュリティアドバイザリのCVE表示ページにCVEの重大度が表示されない。

NetScaler MPXおよびSDXプラットフォームのLASライセンスを構成する際、帯域幅割り当て中に小数点以下の検証エラーが発生する可能性があります。この問題は、割り当て可能なライセンスエディションの数が限られている場合に発生します。

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

February 04, 2026

- **NetScaler Consoleサービスにおけるアップグレード前チェックの分類**

  アップグレードジョブを使用したNetScalerのアップグレードにおけるNetScaler Consoleのアップグレード前チェックは、以下のカテゴリに分類されるようになりました。

  - 重大: アップグレードはブロックされます。
  - 警告: 管理者の承認があればアップグレードは許可されます。
  - 勧告: 管理者の承認があればアップグレードは許可されます。

  詳細については、「アップグレード前の検証」を参照してください。

- **技術サポートファイルの生成における必須の時間パラメータ**

  技術サポートファイルを生成する際、時間の指定が必須になりました。技術サポートファイルを生成する際には、明示的に時間参照を選択する必要があります。カスタムオプションを選択してカスタムの日時を指定するか、「今すぐ」オプションを使用できます。「今すぐ」オプションは現在のシステム時間を使用します。この機能強化により、正確な時間コンテキストが明示的に定義されるようになります。

  詳細については、「NetScalerインスタンスの技術サポートバンドルを生成する方法」を参照してください。

- **アップグレードジョブ: 選択されたインスタンスがすでにターゲットビルドにある場合、警告が表示されます**

  アップグレードジョブ中に誤ったインスタンスが選択されるのを防ぐため、すでにターゲットビルドを実行しているインスタンスを選択した場合、警告が表示されます。この機能強化により、不要なアップグレードを回避できます。インスタンスを再アップグレードする意図がある場合は、警告を無視して続行しても問題ありません。

- **インスタンスグループの可視性とマッピングの強化**

  インスタンスグループページに**インスタンスビュー**タブが導入され、インスタンスグループの可視性と管理が向上しました。**インスタンスビュー**タブは、以下の機能を提供する一元化されたビューです。

  - 管理対象のすべてのNetScalerインスタンスの統合リスト
  - 各インスタンスが関連付けられているインスタンスグループの可視性
  - どのインスタンスグループにもマッピングされていないインスタンスの明確な識別

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

- ホスト名とIPアドレスの両方を使用したインスタンス識別の改善

管理者は、マッピングされていないインスタンスをインスタンスグループにすばやく追加し、すでに割り当てられているインスタンスを特定して重複マッピングを防ぐことで、よりシンプルで効率的なインスタンスグループ管理を実現できます。

インスタンスビューを表示するには、**Infrastructure > Instances Dashboard > Instance Groups > Instances View**に移動します。

詳細については、https://docs.netscaler.com/ja-jp/netscaler-console-service/networks/instance-management/create-instance-groupsを参照してください。

- **ファイル整合性監視: スキャンから除外リストを作成する機能**

  カスタムの許可リストを作成し、特定のファイルをファイル整合性監視スキャンから除外できます。スキャンから除外するファイルを定義することで、監視を効率化し、信頼できるファイルに対する不要なアラートを減らすことができます。以前は、ファイル整合性監視スキャン中に、悪意のない特定のファイルが悪意のあるものとして誤って識別されていました。

  詳細については、https://docs.netscaler.com/ja-jp/netscaler-console-service/instance-advisory/file-integrity-monitoring%23console-detectedを参照してください。

- **バイナリ署名と検証のサポート**

  NetScaler Consoleサービスは、バイナリ署名と検証をサポートするようになりました。この機能は、NetScalerインスタンス上で不正または改ざんされたファイルの実行を検出し、防止するメカニズムを提供することで、セキュリティを強化します。NetScalerで不正なファイルを実行しようとすると、リアルタイムのSNMPトラップがNetScaler Consoleに送信され、フラグが立てられます。

  バイナリ署名と検証を使用して問題が報告されたNetScalerインスタンスのリストを表示するには、**Infrastructure > Instance Advisory > Security Advisory** に移動し、**File Integrity Monitoring** をクリックして、**Device-Reported** タブを表示します。

  詳細については、「ファイル整合性監視」を参照してください。

その他

- **オンデマンドLASエンタイトルメント同期**

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

以前は、コンソール互換のエンタイトルメントは、License Activation Service (LAS) と24時間ごとに1回だけ同期されていました。新しい「Sync Licenses」オプションを使用すると、この同期をオンデマンドで手動でトリガーでき、エンタイトルメントがすぐに最新の状態に保たれます。

LASに関する情報については、「License Activation Service」を参照してください。

修正された問題

インフラストラクチャ

- 証明書とキーの一括アップロードを実行すると、GUIは「Successfully Uploaded」ステータスを確認します。しかし、証明書はZero-Touchビューに表示されません。
- **Security Advisory Dashboard** に、定義された **Scheduled Scan Frequency** と一致しない誤った **Next Scheduled Scan** 日付が表示される場合があります。
- DNSプロバイダーが10秒のタイムアウト内に応答しない場合、ACME証明書の発行中にDNSチャレンジが失敗する可能性があります。この問題は、API応答の遅延、高いネットワーク遅延、または大幅なDNS伝播遅延が原因で発生します。
- アップグレードプロセス中に生成された一部のNetScalerファイルが、ファイル整合性監視スキャンによって誤って脆弱であるとフラグ付けされる可能性があります。
- 日本のクラウド関連URLにアクセスできるにもかかわらず、Citrix Cloud JapanのNetScaler Console ServiceでNetScaler Agentの診断ステータスが誤って「レビューが必要」と表示されます。
- NetScaler Consoleのセキュリティアドバイザリは、安全でないSSLプロトコルバージョンに関する誤ったセキュア構成の推奨事項を表示します。この推奨事項は、TLS 1.0およびTLS 1.1が、それらのプロトコルが無効になっている場合でも、非プライマリのデフォルトプロファイルで使用されていることを示しています。
- ターゲットインスタンスが、管理アクセス用にSNIPが構成されているHAペアである場合、StyleBook構成パックの操作がRBAC認証エラーで失敗する可能性があります。
- NetScaler Cloud APIは、NITRO systemfileエンドポイントへのリクエストのプロキシに失敗する可能性があります。その結果、API呼び出しが失敗する可能性があります。

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

- NetScaler ConsoleのSSL証明書有効期限切れイベントに関するメール通知が失敗する可能性があります。

- NetScaler ConsoleでAutomated Certificate Management Environment (ACME) によって発行されたすべてのリモート証明書は、証明書の数が20を超えるとNetScalerから削除されます。

ライセンス

- **License Management** の下の **LAS Licensed** テーブルに、インスタンスのホスト名が表示されない場合があります。

- プール型またはフレックス型ライセンスの場合、Console オンプレミス GUI にはエンタイトルメントブロブの更新日情報が表示されます。ただし、エンタイトルメントブロブの有効期限に関するアラートやプロアクティブな通知は送信されません。お客様は、GUI に表示されるエンタイトルメントブロブの有効期限を監視し、製品の継続的な機能を確保するために、有効期限が切れる前に更新することをお勧めします。

その他

- まれに、ゼロタッチ証明書管理の展開中に、NetScaler 上の仮想サーバーが一時的にダウンすることがあります。

- IPアドレスの代わりにFQDNを使用してインスタンスが追加された場合、NetScalerインスタンスのLASベースのライセンスへの移行が失敗します。

- プール型エンタイトルメントのみに基づくLASライセンス（UHMC/CPLを除く）を使用している場合、**Pooled Licensing** ダッシュボードの **LAS Managed Entitlements** タブにSDXデバイスが表示されない場合があります。

StyleBook

- 既存のStyleBook Configpackのリソースバインディングを編集すると失敗します。

November 11, 2025

管理と監視

CVE-2025-12101の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2025-12101の特定と修復をサポートするようになりました。

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

- CVE-2025-12101の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2025-12101の修復」を参照してください。

  注記：

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- CVEの詳細については、「セキュリティ速報」を参照してください。

November 06, 2025

修正された問題

インフラストラクチャ

再起動後、NetScaler Consoleオンプレミスセキュリティアドバイザリスキャン頻度が、24時間ではなく7日に誤って設定されます。

その他

顧客がプールライセンスのみを使用し、フレックスライセンスを持っていない場合、「**プールライセンス > スループット容量 > LAS管理対象エンタイトルメント**」の下にある「**ライセンスされたNetScalerインスタンス**」セクションにデバイスが表示されない場合があります。

October 15, 2025

管理と監視

アップグレードジョブにおけるISSU移行の完了

アップグレードジョブのワークフローは、強制的なインサービスソフトウェアアップグレード (ISSU) 移行をサポートするようになりました。「**ジョブの作成**」で「**NetScaler HAペアでのネッ**

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

トワーク停止を回避するためにISSUを有効にする」が選択されている場合、ISSUは、顧客が定義した遅延期間の後に完全な移行を自動的にトリガーします。

ISSU中、NetScalerは通常、移行を完了する前にアクティブな接続が自然に切断されるのを待ちます。しかし、長期間維持される接続が完了を遅らせたり、ブロックしたりする場合があります。この機能強化により、NetScaler Consoleは、長期間維持されるアクティブな接続を終了させることで、強制的なISSU移行をトリガーします。重要な管理セッション（CLI、GUI、コンソール）は、中断のない管理アクセスを確保するために除外されます。

利点:

- より高速で予測可能なISSUの完了。
- 長期間維持される接続によって引き起こされる運用上の遅延と障害の削減。
- アップグレードおよびロールバックワークフローにおける信頼性の向上。

サポートされるシナリオ:

- 移行が進行中で、接続が切断されるのを待っている。
- ロールバックが進行中で、接続が閉じられるのを待機しています。

修正された問題

インフラストラクチャ

証明書の有効期限通知設定が正しく構成されているにもかかわらず、SSL証明書の有効期限が近づいていることに関するメール通知がユーザーに届かない場合があります。

一部のNetScalerインスタンスは、スキャンに無関係なファイルが含まれているため、ファイル整合性監視によって誤って脆弱であるとフラグ付けされます。

Security Advisory > Scan history ページに表示されるバナーに誤った情報が含まれています。

September 17, 2025

インフラストラクチャ

ACMEプロトコルを使用した証明書の自動更新

NetScaler Consoleは、SSL/TLS証明書のライフサイクル管理を簡素化するために、ACME（Automated Certificate Management Environment）プロトコルをサポートするようになりました。

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

ACMEプロトコルのサポートには、次の利点があります。

- 有効期限が切れる前に証明書を更新することで、ダウンタイムを防止します。
- 自動追跡と更新により、手作業を削減します。
- 常に有効でCA準拠の証明書により、より強力なセキュリティを確保します。

NetScaler Consoleは、ACMEクライアントacme.shと、以下のCAベンダーとの証明書更新統合をサポートしています。

- レッツエンクリプト
- DigiCert

acme.shクライアントがサポートするすべてのDNSプロバイダーは、DNS検証のためにコンソールでもサポートされています。

次の点が、ACME通信フローの概要を説明しています。

- ACMEクライアントとして機能するNetScaler® Consoleは、新しい証明書または更新のためにACMEサーバー（CA）にリクエストを送信します。
- CAはDNS-01チャレンジを開始します。
- NetScaler Consoleは、CAから提供されたトークンを含むTXTレコードを、設定されたDNSプロバイダーに追加します。
- CAは、ドメイン所有権を確認するためにDNSプロバイダーにクエリを実行します。
- 検証が成功すると、CAは証明書を発行します。

詳細については、「ACMEプロトコルを使用した証明書の自動更新」を参照してください。

修正された問題

インフラストラクチャ

一部の無料ライセンスのお客様の場合、履歴データが削除される可能性があります。

複数のデバイスグループに関連付けられており、大規模なコマンドセットを含む構成ジョブの読み込みが遅延します。

ユーザーは次の問題に遭遇する可能性があります。

- **Console on-prem telemetry upload** をクリックしたときに、**Invalid Resource** エラーメッセージが表示される。

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

- 新しいプロファイルを作成しようとしたときに、**IP address already exists** エラーメッセージが表示される。

プラットフォーム

複数のPEを持つNetScalerが、NetScaler Consoleからスキャンされたときに、CVE-2021-22956の脆弱性があると誤ってフラグ付けされる可能性があります。

StyleBooks

設定パックに、送信元IPアドレスデータセットまたは宛先IPアドレスデータセットを使用するNetScalerアクセス制御リストが含まれている場合、設定パックの更新が失敗する可能性があります。

September 08, 2025

ライセンス

NetScalerおよびNetScaler Console ServiceでのLASの適用

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（「手動で管理されるエンタイトルメント」とも呼ばれます）は、April 15, 2026 にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026 以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（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の展開は、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: 14.1-51.80、13.1-60.29、13.1-37.247 (FIPS)
- NetScaler SVM: 14.1-51.83、13.1-60.30
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.83

  注: Console on-premのLASサポートは、リリース14.1-51.83以降です。ただし、ファイルベースのライセンスの非推奨/EOLは、Console on-premリリース14.1-51.83以降、およびConsole on-premリリース13.1-60.26以降です。

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

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場合、お客様は利用できない場合があります。

ご質問やご不明な点がございましたら、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 Console ServiceのLASサポート

NetScaler Consoleサービスは、License Activation Service (LAS) ライセンスメカニズムをサポートするようになりました。LASは、従来のファイルベースのライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品のアクティベーションのための新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

NetScaler Consoleサービスは、自動的にLicense Activation Service (LAS) が有効になりました。NetScaler FlexedおよびPooledライセンスの資格は、**Licenses > License management > License Activation Service (LAS)** に移動して表示できます。

LASのNetScalerバージョン互換性 LASを使用するには、NetScalerが以下の最小バージョン以降を実行している必要があります。

- NetScaler ADC: 14.1ビルド51.x、13.1ビルド60.x、13.1ビルド37.x (FIPS)
- NetScaler SVM: 14.1ビルド51.x、13.1ビルド60.x

注:

NetScaler Consoleサービス向けのLASは、NetScaler Flexedライセンス (CPL/UHMC) および (レガシー) NetScaler Pooledライセンスをサポートしています。Pooled vCPU、CICOなどの他のすべての形式のレガシーNetScalerライセンスは、LASではサポートされていません。 詳細については、Console ServiceのLASサポートを参照してください。

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

September 03, 2025

修正された問題

インフラストラクチャ

管理パーティション内で必要な「ns」カウンタグループがサポートされていないため、NetScaler スループットグラフは管理パーティションダッシュボードから削除されました。

August 26, 2025

管理と監視

CVE-2025-7775 の特定と修復のサポート

NetScaler Console サービスセキュリティアドバイザリは、CVE-2025-7775 の特定と修復をサポートするようになりました。

- CVE-2025-7775 の特定にはカスタムスキャンが必要です。このスキャンでは、NetScaler Console が管理対象の NetScaler インスタンスに接続し、スクリプトをプッシュします。スクリプトはインスタンス上で実行され、CVE の前提条件を確認します。前提条件が満たされている場合、NetScaler でバージョンチェックが実行されます。修復には、脆弱な NetScaler インスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2025-7775 の修復」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了 (EOL) に達した NetScaler® ビルドをサポートしていません。NetScaler がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「ジョブを使用して NetScaler インスタンスをアップグレードする」を参照してください。
- CVE の詳細については、「セキュリティ速報」を参照してください。

CVE-2025-7776 の特定と修復のサポート

NetScaler Console サービスセキュリティアドバイザリは、CVE-2025-7776 の特定と修復をサポートするようになりました。

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

- CVE-2025-7776 の特定には、バージョンと構成のスキャンを組み合わせる必要があります。修復には、脆弱な NetScaler インスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2025-7776 の修復」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了 (EOL) に達した NetScaler ビルドをサポートしていません。NetScaler がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「ジョブを使用して NetScaler インスタンスをアップグレードする」を参照してください。
- CVE の詳細については、「セキュリティ速報」を参照してください。

CVE-2025-8424の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2025-8424の特定と修復をサポートするようになりました。

- CVE-2025-8424の特定にはバージョンスキャンが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、「CVE-2025-8424の修復」を参照してください。

  注：

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。
- CVEの詳細については、「セキュリティ速報」を参照してください。

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

August 20, 2025

インフラストラクチャ

セキュリティスキャンのオプトインまたはオプトアウトのサポート

セキュリティスキャンをオプトインまたはオプトアウトすることで、セキュリティスキャン設定をカスタマイズできるようになりました。さらに、セキュリティ評価の一部として含める特定のスキャンの種類を選択できます。デフォルトでは、共通脆弱性識別子（CVE）スキャンのみが有効になっています。

セキュリティスキャン設定を構成するには：

1. **Instance advisory > Security Advisory** に移動します。
2. 右上隅の設定アイコンをクリックします。
3. **システムスキャンを構成**」で、含めるスキャンの種類を選択します。
4. **保存**」をクリックします。

システムスキャンにおけるファイル整合性監視

システムスキャンの一部としてファイル整合性監視を含めることで、セキュリティ体制を強化できるようになりました。ファイル整合性監視により、NetScalerファイルシステムに変更や追加が行われたかどうかを特定できます。

ファイル整合性監視を有効にするには：

1. **インスタンスアドバイザリ > セキュリティアドバイザリ**」に移動します。
2. 右上隅の設定アイコンをクリックします。
3. **システムスキャンを構成**」で、「**ファイル整合性監視スキャン**」を選択します。
4. **保存**」をクリックします。

修正された問題

インフラストラクチャ

インスタンスアドバイザリ > セキュリティアドバイザリ > CVE検出 > CVEビューに切り替え」ページで、一部のCVEの重大度レベルが正しく表示されない場合があります。

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

July 17, 2025

インフラストラクチャ

タイムスタンプにタイムゾーン情報が含まれる

NetScaler ConsoleサービスGUIでタイムスタンプが表示される箇所では、タイムゾーン情報も確認できるようになりました。タイムゾーンは、**System Settings**で選択されたタイムゾーンに基づいて表示されます。設定に応じて、タイムゾーンはGMT、ローカルタイムゾーン、またはUTC（ローカルの略語が利用できない場合）として表示されます。

以前は、タイムスタンプにタイムゾーン情報は表示されませんでした。この機能強化により、スケジュールされたジョブのタイムスタンプの詳細がより明確かつ正確になります。

例えば、次の図はタイムゾーンを含むスケジュールされた時刻を示しています。

修正された問題

インフラストラクチャ

Infrastructure > Instance advisory > Security Advisoryの下にあるSecure Config Recommendations機能のPDFレポート生成は、単一のカテゴリに多数の推奨事項が含まれている場合、失敗する可能性があります。

Security Advisoryダッシュボードの**Last Scan Time**フィールドに、最新のCVEスキャンのタイムスタンプが表示されません。

July 02, 2025

テレメトリ

テレメトリデータの新しい検証

NetScalerテレメトリプログラムの一環として、テレメトリデータを90日ごとに少なくとも1回アップロードする必要があります。NetScaler Consoleサービスは、アップロードされたペイロード内の最新ファイルが90日以内であることを検証するようになりました。ファイルが90日より古い場合、アップロードは拒否されます。この新しい検証チェックにより、アップロードされたテレメトリデータが最新かつ準拠していることが保証されます。

アップロードが拒否された場合:

1. オンプレミスのConsoleから新しいペイロードをダウンロードします。

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

2. 再度アップロードします。

管理対象NetScalerインスタンスからのテレメトリアナリティクスプロファイルの削除

以下のテレメトリメトリクスプロファイル構成は、テレメトリ収集に不要になりました。

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

NetScalerテレメトリプログラムの一環として、テレメトリメトリクスプロファイル構成は管理対象NetScalerインスタンスにプッシュされました。

NetScaler Console は、この構成がまだ存在する場合、NetScaler インスタンスから July 19, 2025 に自動的に削除します。または、以下のコマンドを使用していつでも手動で構成を削除できます。

```
rm analytics profile telemetry_metrics_profile
```

テレメトリメトリクスプロファイル構成の詳細については、NetScalerテレメトリプログラムを参照してください。

セキュリティ

セキュリティアドバイザリダッシュボードの機能強化

セキュリティアドバイザリダッシュボードは強化され、管理者とセキュリティ専門家がNetScalerインフラストラクチャ全体の健全性と脆弱性ステータスを即座に把握できるように設計されています。

このダッシュボードは、NetScaler展開のセキュリティ体制を包括的に鳥瞰できます。主な機能は次のとおりです。

- アクティブなセキュリティアドバイザリを表示する統合ダッシュボード。
- 影響を受けるデバイスの概要。
- 潜在的なリスクの明確な内訳。

重大な脆弱性、軽減策を含む安全な構成の推奨事項、および関連ドキュメントへのリンクをすばやく特定できます。

詳細については、Security Advisoryを参照してください。

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

修正された問題

分析

API定義を編集して変更を保存した後でも、NetScaler ConsoleサービスはAPI定義を更新できず、「更新成功」通知が誤って表示されます。

HDX™ Insight > Usersで、**Current Sessions**の下の詳細を表示するためにドリルダウンすると、NetScalerに接続されているVDAが見つからない場合、不完全なレポートとともに詳細が表示されます。

インフラストラクチャ

Upgrade Advisoryの**Instances on older build summary**セクションに表示されるインスタンスの数が正しくありません。

NetScaler ConsoleからNetScalerをアップグレードすると、システムはアップグレードステータスを電子メールのPDF添付ファイルとして送信できません。

June 25, 2025

管理と監視

CVE-2025-6543の特定と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2025-6543の特定と修復をサポートするようになりました。

- CVE-2025-6543の特定には、バージョンスキャンと構成スキャンの組み合わせが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、CVE-2025-6543を修復するを参照してください。

  注:

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、ジョブを使用してNetScalerインスタンスをアップグレードするを参照してください。
- CVEの詳細については、Security Bulletinを参照してください。

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

June 17, 2025

管理と監視

CVE-2025-5349およびCVE-2024-5777の識別と修復のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2025-5349およびCVE-2025-5777の識別と修復をサポートするようになりました。

- CVE-2025-5349の識別には、バージョンスキャンと設定スキャンの組み合わせが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。詳細については、Remediate CVE-2025-5349を参照してください。
- CVE-2025-5777の識別にはバージョンスキャンが必要であり、修復には次の2段階のプロセスが必要です。

  a. 脆弱なNetScalerインスタンスを、修正を含むリリースとビルドにアップグレードします。

  b. 構成ジョブを適用します。

  詳細については、Remediate CVE-2025-5777を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Use jobs to upgrade NetScaler instancesを参照してください。
- CVEの詳細については、Security Bulletinを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-5349およびCVE-2025-5777の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**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。

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

June 03, 2025

修正された問題

分析

セキュリティ違反、Gateway Insight、HDX Insightなどの分析データをエクスポートする場合、以前はエクスポートされたCSVレポートには5000エントリしか含まれていませんでした。このアップデートにより、制限は10,000エントリに増加しました。

インフラストラクチャ

NetScalerエージェントがプロキシサーバーを介してNetScaler Consoleサービスと通信する際に、プロキシパスワードを誤った形式で断続的に使用します。

設定 > システムイベント > 通知で複数のカテゴリを選択して通知設定を構成し、**保存**をクリックしても、変更が保存されません。

May 26, 2025

分析

VPN仮想サーバーレベルでのHDX Insightの可視性の強化

HDX Insightでは、VPN仮想サーバーレベルで、アクティブセッション、デスクトップ、起動されたアプリケーションなどの主要なメトリックを監視できるようになりました。新しいオプションである**Gateway Virtual Servers**が、**Gateway > HDX Insight**の下で利用可能になりました。

管理者として、この機能強化により、次のことが可能になります。

- **Gateway > HDX Insight > Gateway Virtual Servers**の下にあるすべての仮想サーバーのリストを表示する。
- 仮想サーバーを選択して、その仮想サーバーに特化した詳細な可視性を提供し、パフォーマンス監視を簡素化する包括的なレポートにアクセスする。

以前は、詳細なエンドユーザーエクスペリエンスレポートはNetScalerインスタンスレベルでのみ利用可能でした。

IPv6仮想サーバーのWeb Insight分析を表示するサポート

IPv6アドレスで構成された仮想サーバーのWeb Insight分析を表示できるようになりました。以前は、Web InsightはIPv6アドレスをサポートしていませんでした。管理者として、この機能強化に

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

より、Web Insightでさまざまな詳細が提供され、仮想サーバーのパフォーマンスを分析および改善できます。

詳細については、Web Insightを参照してください。

NetScaler ConsoleをGeoIP DBの集中型更新

NetScaler Consoleを使用すると、管理者はMaxMindからGeoIP DBファイルをNetScaler Console経由で直接アップロードできます。GeoIP DBファイルを管理対象のNetScalerインスタンスにすぐにプッシュするか、後で更新をスケジュールすることができます。これらのファイルは、GSLBやセキュリティポリシーで一般的に使用される正確なIP-to-ロケーションマッピングに不可欠です。

以前は、NetScalerにはNetScaler上のGeoIP DB（地理位置情報データベース）更新を管理するための集中メカニズムがありませんでした。管理者は各デバイスで手動で更新を実行する必要があり、これは時間と手間がかかり、エラーが発生しやすく、本番環境では中断を招く可能性がありました。

この機能強化により、次の利点が提供されます。

- 自動化: 更新プロセスは自動化されており、計画的なダウンタイムなしで実行されるため、運用上のオーバーヘッドが削減されます。
- 効果的なスケーラビリティ: 複数のNetScalerインスタンスにわたる更新の管理は効率的で、簡単にスケーリングできます。
- バージョンチェック: 問題が発生した場合、過去のバージョンを追跡し、古いGeoIP DBファイルをアップロードして同期できます。

詳細については、「NetScaler ConsoleをGeoIP DBの一元的な更新」を参照してください。

修正された問題

分析

- NetScalerエージェントの一部のプロセスがクラッシュし、コアファイルを生成します。その結果、ディスク容量がいっぱいになります。
- NetScaler ConsoleからMicrosoft Sentinelへの1 MBを超えるデータのエクスポートが失敗します。
- Web Insightで、**Application Metrics**の下の異常を表示するためにアプリケーションをクリックすると、**Response Time**タブのクライアントネットワーク遅延が誤った詳細を表示します。

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

May 06, 2025

修正された問題

StyleBookの定義に、空であるか定義されたインポートがないimport-stylebooksセクションが含まれている場合、StyleBookのクローン作成は以下のエラーで失敗する可能性があります。

'NoneType' オブジェクトは反復可能ではありません

StyleBookの定義に、コンポーネントからの出力を参照する式が含まれている場合、StyleBookの定義のインポートが失敗する可能性があります。

NetScaler ConsoleからのNetScalerのアップグレードは、破損したビルドイメージが原因で失敗します。イメージのアップロード中にネットワークの問題が発生すると、ビルドイメージが破損します。ファイル転送中の不一致を検出して防止するために、アップロードされたビルドイメージのチェックサム検証を有効にできます。

一部のシナリオでは、イベントステータスが変更されても通知がトリガーされません。ログは生成されますが、イベントアクションは実行されません。

April 15, 2025

ゼロタッチ証明書展開

ビルド14.1-43.x以降を実行している管理対象NetScalerインスタンスで、ゼロタッチ証明書を構成できるようになりました。ゼロタッチ証明書展開により、手動での介入を排除し、インメモリのゼロタッチ証明書ストアを構築してアプリケーション要求を処理できます。**SSL Dashboard > Zero-touch certificate management**に移動して、NetScaler Consoleにすべての証明書とキーをアップロードし、NetScalerインスタンスを選択して、**Enable**をクリックします。証明書をアップロードし、NetScalerインスタンスでゼロタッチ証明書管理を有効にすると、NetScalerは定期的に証明書リポジトリをポーリングし、必要な証明書を取得します。

以前は、SSLダッシュボードでは、各インスタンスにSSL証明書をインストールする際の手動介入を最小限に抑えることしかできませんでした。

詳細については、以下を参照してください。

- NetScalerゼロタッチ証明書管理
- NetScaler Console ゼロタッチ証明書管理

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

パブリッククラウドにおけるNetScalerインスタンスのオートスケーリングの廃止

パブリッククラウドにおけるNetScalerインスタンス構成のオートスケーリングは、NetScaler Consoleでは利用できなくなりました。

構成ジョブの改善

NetScaler Consoleは、構成ジョブに追加されたshowコマンドの出力を、電子メールとSlackを通じて送信するようになりました。

アップグレードジョブの改善

インフラストラクチャ > アップグレードジョブで、2段階のアップグレードプロセスを使用して高可用性構成のNetScalerをアップグレードするジョブを作成する際、HAフェイルオーバーを2番目のノードのアップグレード開始まで遅延させることができるようになりました。

修正された問題

インフラストラクチャ

構成ジョブでファイルアップロードオプションを使用してジョブを作成すると、次のエラーメッセージが表示されます。 `File upload not allowed. Max file size 15 MB`

構成ジョブで許可される最大ファイルサイズは2GBです。

NetScalerからの「systemfiles」NITRO呼び出しに対するサービス間DeviceAPIProxy呼び出しは、結果の取得に失敗します。

> > > で、テンプレートコマンドに変数が定義されている場合、監査テンプレートのプレビューが失敗します。

NetScaler Consoleでは、2025年3月まで、Slackの新しい通知チャネルをエクスポートのスケジュールに使用することはできません。それまでは既存のSlackチャネルをエクスポートのスケジュールに使用できますが、その後は新しいチャネルを作成する必要があります。

アプリケーションには次のスコープが必要です。

- チャンネルの読み取り
- グループの読み取り
- im:読み取り
- mpim:読み取り

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

詳細については、Slackドキュメントを参照してください。

February 19, 2025

StyleBooks

プライベートホスト型GitLab/GitHubリポジトリおよびInfoblox IPAMへのアクセスをサポート

NetScaler ConsoleサービスStyleBooksでは、プライベートホストされ、企業のイントラネット内でのみアクセス可能なGitLab/GitHubリポジトリからStyleBooksおよびConfigpacksをインポートおよび同期できるようになりました。

NetScaler ConsoleサービスIPAMでは、プライベートホストされたInfoblox DDIサーバーを外部IPAMプロバイダーとして登録できるようになりました。

以前は、公開されているGitLab/GitHubリポジトリとInfoblox DDIサーバーのみがサポートされていました。

詳しくは、「外部リポジトリからのStyleBooksのインポートと同期」および「IPアドレス管理（IPAM）の構成」を参照してください。

修正された問題

分析

無制限のVIPに準拠するため、**設定 > 分析構成**からサブスクリプションの詳細が削除されました。

February 06, 2025

分析

仮想サーバーレベルでのWebトランザクション分析の有効化

仮想サーバーレベルでWebトランザクション分析を有効にできるようになりました。これを行うには、仮想サーバーの分析を有効にする際に、新しい「詳細なWebトランザクション」オプションを選択してWebトランザクション分析を有効にする必要があります。

以前は、仮想サーバーの分析を有効にすると、Webトランザクション分析が自動的に有効になっていました。

詳しくは、「Webトランザクション分析」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

メンテナンスおよびトラブルシューティング期間中の管理対象デバイスの通知を無効にする

管理者は、メンテナンスおよびトラブルシューティング期間中、特定の管理対象デバイスの通知を一時的に無効にできます。この機能強化により、これらの期間中のデバイス固有の問題やステータス更新に関する不要なアラートや通知の受信を回避できます。

通知を無効にするには、**設定 > 管理 > インスタンス設定 > 通知無効化期間**に移動し、必要な詳細を追加します。詳細については、インスタンス設定を参照してください。

修正された問題

インフラストラクチャ

ジョブテンプレートで、**インポート**ボタンを使用して構成ジョブテンプレートをインポートする際に、次のエラーが表示されます。

```
Invalid resource
```

January 15, 2025

テレメトリ

Consoleオンプレミス テレメトリのアップロードの変更

NetScaler Consoleサービスにテレメトリファイルをアップロードするには、NetScaler Consoleオンプレミスインスタンスごとにプロファイルを作成する必要があります。複数のNetScaler Consoleオンプレミスインスタンスがグローバルに展開されている場合があります。オンプレミスインスタンスごとにプロファイルを作成することで、それらのオンプレミスインスタンスのテレメトリファイルをアップロードし、アップロード期限を個別に監視できます。

プロファイルを作成するには、**Settings > Console on-prem telemetry upload** に移動し、**Create Profile** をクリックします。

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

注:

既存のConsole on-premユーザーで、以前にテレメトリファイルをConsoleサービスにアップロードしたことがある場合は、新しいプロファイルを作成してからテレメトリファイルをアップロードする必要があります。新しいプロファイルの作成後、Console on-premの期限とConsoleサービスの期限との間に不一致が見られる場合があります。Console on-premに表示されている期日までに、NetScaler Consoleサービスにテレメトリファイルをアップロードしてください。この不一致は、新しいプロファイルを使用して1回のアップロードを完了すると解消されます。

詳細については、「Console on-prem upload」を参照してください。

分析

クライアントIPアドレスを取得するための分析設定でのカスタムヘッダーの有効化のサポート

アプリケーションの分析を有効にすると、X-Real-IP、X-Client-IP、またはその他のカスタムヘッダーなどのカスタムヘッダーを定義して、プロキシIPアドレスの代わりに実際のクライアントIPアドレスを取得できるようになります。カスタムヘッダーオプションにより、次のことが可能になります。

- さまざまなヘッダーを使用する多様なネットワークプロキシとの互換性。
- 複数のプロキシ層を持つ複雑なネットワーク環境で、実際のクライアントIPアドレスを取得する精度。
- 標準ヘッダーによって提供されるものよりも追加のセキュリティ対策。

カスタムダッシュボードでの並べ替えと検索のサポート

カスタムダッシュボード (**Overview > Custom Dashboard**) で、次の機能を使用できるようになりました。

- カスタムダッシュボードをアルファベット順に表示するための並べ替えオプション。
- 検索結果を絞り込むための検索オプション（プレーンテキストと正規表現の両方）。

インフラストラクチャ

システムイベントのメール通知におけるホスト名

NetScaler Console は、システムイベントのメール通知に、関連する NetScaler インスタンスのホスト名を含むようになりました。

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

StyleBook

GitLab 外部リポジトリからの StyleBook のインポートと同期

StyleBook は、GitLab リポジトリからの StyleBook および構成パックのインポートと同期をサポートするようになりました。以前は、この機能は GitHub リポジトリでのみ利用可能でした。

詳細については、「外部リポジトリの同期」を参照してください。

StyleBook データソースから複数の項目を選択する

データソースパラメータから複数の項目を選択できる StyleBook を作成できるようになりました。StyleBook は、パラメータタイプとしてデータ配列をサポートするようになり、ユーザーはデータソースまたはコレクション項目のリストを入力として選択できます。

詳細については、「StyleBook データソースの管理」を参照してください。

データソースコレクションのフィルターをサポート

StyleBookでは、データソースパラメータにコレクションフィルターを指定できるようになりました。設定パック操作でこのようなパラメータの入力を提供する際、ユーザーはすべての項目からではなく、フィルターされたコレクションからのみ項目を表示および選択できるようになります。

詳細については、以下を参照してください: 組み込みデータソース、カスタムデータソース

修正された問題

アナリティクス

- **設定 > 可観測性統合**で、NetScalerコマンドの失敗が発生した場合、サブスクリプションの編集または削除が失敗する可能性があります。

- **HDX Insight**および**Web Insight**では、地理位置情報レポートが定義されたIPブロックのクライアントIP位置を解決しません。

インフラストラクチャ

- NetScaler Consoleのすべてのデフォルトロールを持つユーザーがエージェント登録のアクティベーションコードを生成しようとすると、「**この操作を実行する権限がありません**」というエラーでアクションが失敗します。

- nsroot以外のユーザーがネットワーク機能 (**インフラストラクチャ > ネットワーク機能**) で特定の仮想サーバーの統計情報を表示しようとすると、エラーメッセージが表示されます。

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

StyleBooks

- NetScaler HAペアに設定パックを展開し、フェイルオーバーが発生した場合、新しいプライマリのインスタンスIDで設定パックを更新しようとすると失敗します。
- NetScalerのアクセス制御リストによって参照されるポリシーデータセットを含む設定パックを削除し、関連するStyleBookでリソースの再利用が有効になっている場合、ポリシーデータセットはNetScalerで古いままになります。
- **アプリケーション > 構成 > 設定パック**で設定パックを編集すると、追加された項目の順序は保持されません。

December 03, 2024

移行された構成間での構成エンティティの共有

構成移行ユーティリティを使用して構成を移行する際に、構成エンティティを再利用できるようになりました。後続の移行では、以前の移行によって作成されたターゲットADC上の既存の構成エンティティが正常に再利用されます。以前は、一部の構成エンティティを共有する2つの構成を移行する際に、**リソースが既に存在します**というエラーで構成の移行が失敗していました。

詳細については、以下を参照してください: StyleBookを使用した簡素化された移行

分析をポリシーベースからプロファイルベースの構成へ移行する

仮想サーバーで分析を有効にすると、分析はプロファイルベースの構成を通じて適用されるようになりました。以前は、分析はAppFlow®ポリシーを通じて構成されていました。プロファイルベースの構成には、次の利点があります。

- パフォーマンスと柔軟性の向上
- より簡単な構成と管理

分析構成に関連する機能強化は、プロファイルベースの構成でのみサポートされています。分析が有効になっている既存のすべての仮想サーバーを、プロファイルベースの構成に移行することをお勧めします。

Settings > Analytics Configuration に移動し、**Migrate Analytics** を選択します。

詳細については、「分析の移行」を参照してください。

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

修正された問題

分析

- **Web Insight** では、カスタム日付範囲が1日を超えるとデータが表示されません。

インフラストラクチャ

- NetScaler Console は、SSLダッシュボードから証明書署名要求 (CSR) を生成できません。
- AzureグループのIdentity and Access Management (IAM) で権限を更新しても、変更がNetScaler Consoleに反映されません。
- DeviceAPIProxy 呼び出しは、NetScaler からの「systemfiles」NITRO 呼び出しの結果を取得できません。
- NetScaler Consoleの強化されたGUIでは、**PINNED**メニューリストは、メニューの第一階層が展開されている場合にのみ表示されます。

StyleBook

- StyleBook構成パックを使用してリンクアグリゲーション制御プロトコル (LACP) チャネルを構成しようとすると失敗します。
- 必須パラメータが不足している場合、構成パックの強制削除は失敗します。
- StyleBook定義を更新すると、ドラフトおよびスケジュールされた構成パックが意図せず展開されます。
- StyleBook構成パック操作のRBACポリシーを作成する際、**APIProxy**権限を手動で選択する必要があります。選択されていない場合、構成パックは失敗します。

November 20, 2024

NetScaler Console GUIのユーザーエクスペリエンスの向上

NetScaler Consoleサービスは、より良いユーザーエクスペリエンスのために、改善されたグラフィカルユーザーインターフェース (GUI) を提供するようになりました。主な改善点は次のとおりです。

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

- **ホバー表示メニュー**: プライマリメニューのツリー構造が、より簡単なナビゲーションのためにホバー表示機能に置き換えられました。セカンダリメニュー項目は、ホバーすると表示され、より迅速な選択のためにサブメニューが表示されます。
- **簡素化されたメニュー階層**: メニュー階層は最大3レベルに制限され、主要オプションへのアクセスが簡素化されました。
- **更新されたサブメニューラベル**: 以前は3レベルを超えてネストされていたオプションのサブメニュー名が改訂されました。
- **折りたたみ可能なメニュー**: ペイン内のアイコンをクリックすることで、メニュー全体を折りたたんだり展開したりできるようになり、より多くの画面スペースが提供されます。
- **サイドバートグル**: パンくずリストの新しいトグルボタンを使用すると、サイドバーを非表示または表示して、ワークスペースを最適化できます。
- **ホームページの設定**: サブメニュー名の横にあるアイコンをクリックすることで、表示されているページをホームページとして設定できるようになりました。
- **お気に入りアイテムのピン留め**: お気に入りのメニュー項目を簡単にピン留めして、より迅速にアクセスできます。

詳細については、「強化されたグラフィカルユーザーインターフェイス」を参照してください。

NetScalerからSSL証明書を削除するオプション

NetScalerからSSL証明書を削除できるようになりました。以前は、**Infrastructure > SSL Dashboard**からファイルを削除しても、証明書は実行中の構成からのみ削除されていました。関連する証明書ファイルはNetScalerから削除されませんでした。

詳細については、「SSLダッシュボード」を参照してください。

修正された問題

インフラストラクチャ

- 証明書ストア（Infrastructure > SSL Dashboard > Certificate Store）を使用して証明書を更新すると、NetScaler ConsoleはNetScalerインスタンスの中間証明書を更新できません。
- アプリケーションが1000個を超えると、NetScaler Consoleは応答しなくなり、以下の操作時にCPU使用率が高くなります。
  - ユーザーグループを作成する（**Settings > Users & Roles > Groups > Add**）。
  - **Authorization Settings**タブで**Add**をクリックして特定のアプリケーションを割り当てる。

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

- 読み取り専用ユーザーがNetScaler Consoleにログインすると、次のエラーメッセージが表示されます。

  セッションが見つからないか、無効です。

StyleBooks

StyleBook設定パックを使用して最初に構成されたポリシーバインディングの順序が優先度に従って並べ替えられると、設定パックの更新が失敗します。

November 12, 2024

管理と監視

CVE-2024-8534およびCVE-2024-8535の特定と修正のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2024-8534およびCVE-2024-8535の特定と修復をサポートするようになりました。

- CVE-2024-8534の特定には、バージョンスキャンと構成スキャンの組み合わせが必要です。修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。
- CVE-2024-8535の特定にはバージョンスキャンが必要であり、修復には2段階のプロセスが必要です。

  a. 脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードします。

  b. 構成ジョブを適用します。

  詳細については、「CVE-2024-8535の修復」を参照してください。

  注:

  セキュリティアドバイザリは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

- NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。

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

- CVEの詳細については、「セキュリティ速報」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2024-8534およびCVE-2024-8535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。

October 15, 2024

テレメトリ

NetScaler Console GUI の NetScaler テレメトリページ

データ収集、テレメトリのモード、前提条件などの情報を含む NetScaler テレメトリページを GUI で表示できるようになりました。前提条件が満たされていることを確認するだけでよく、テレメトリデータアップロードのためのアクションは不要です。

必須のテレメトリデータ収集のための NetScaler テレメトリプログラムは、NetScaler Console 14.1-28.x ビルドで導入されました。

分析

Web Insight における SSL 使用状況分析の改善

Web Insight では、トラフィックが多いシナリオでの暗号、鍵強度、プロトコルなどの主要なメトリックの可視性が向上し、SSL 使用状況分析が改善されました。以前は、トラフィックが多いシナリオでのこれらの主要なメトリックの可視性は、限られた詳細しか表示されませんでした。

カスタムダッシュボードの SSL ウィジェット

カスタムダッシュボード (**概要 > カスタムダッシュボード**) で、SSL 構成に関連するメトリックを表示するダッシュボードを作成できるようになりました。カスタムダッシュボードの作成の詳細については、「インスタンスの主要なメトリックの詳細を表示するカスタムダッシュボードの作成」を参照してください。

修正された問題

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

インフラストラクチャ

- **インフラストラクチャ > SSL ダッシュボード**で、SSL 証明書チェーンのルート証明書と中間証明書が表示されません。
- 「**Infrastructure > SSL Dashboard**」では、公開されている証明書の発行者が「**推奨されません**」と誤って表示されます。
- NetScaler Consoleでは、「**<**」と「**>**」の間に含まれるイベントメッセージがメール本文に表示されません。
- セキュリティダッシュボード（**Security > Security Dashboard**）で、保護されていないアプリケーションの保護を設定または変更し、「**展開**」をクリックすると、次のエラーメッセージが表示されます。

  ```
  HTTP Error 502 while accessing the data endpoint: "Unified_appsec_profile"
  ```

October 03, 2024

ライセンス

Flexed/Pooledライセンス関連の問題のトラブルシューティング

FlexedまたはPooledライセンスダッシュボードの「**ライセンスされたNetScaler**」で、「**トラブルシューティング**」オプションを使用して、いくつかのライセンス関連の問題を表示および分析できるようになりました。可能性のあるライセンス問題には、Consoleからインスタンスへの通信や、ライセンスサーバーエージェント (LSA) の可用性などがあります。「**トラブルシューティング**」オプションは、ライセンスサーバー、LSA、プロセス、通信などの問題カテゴリとそのステータスのリストを提供します。管理者として、ライセンスの問題が見つかった場合は、これらのカテゴリを分析してトラブルシューティングできます。

詳細については、ライセンス問題のトラブルシューティングを参照してください。

StyleBook

Migration Utility構成パックにおける構成の統合と共有の強化

さまざまな移行設定パック間で設定を統合し、再利用できるようになりました。以前は、移行ユーティリティの外部で作成された設定は、複数の設定パック間で再利用できませんでした。

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

注意事項

NetScaler Consoleサービスに対して、より厳格なHTTPヘッダー検証が実装されました。APIユーザーは、正しいContent-Typeヘッダーを使用する必要があります。

修正された問題

Build Oct 03, 2024 で対処された問題。

分析

- **Security > Security Violations**の**Application Overview**で、NetScaler 14.1–21.38で報告されたWAFセキュリティ違反の詳細が、以下の操作後に空白で表示されます。

  a. WAFで報告された**Top Applications**からアプリケーションを選択して、詳細を表示します。

  b. **Violation details**の下にある**See more**をクリックします。

  c. **Timeline Details**の下にある**+**をクリックし、すべての列を選択します。

インフラストラクチャ

- MASTools HAデバイスのフェイルオーバー後、SNMPトラップが受信されません。

StyleBooks

- 'Interface'のような大文字と小文字が混在する命名のADCリソースの構成は、StyleBook configpack操作が成功しても適用されません。

September 19, 2024

インフラストラクチャ

ネットワーク機能のポーリング間隔の変更

すべてのNetScalerインスタンスに対する既存のデフォルトポーリング間隔に加えて、NetScaler Consoleは、デフォルトのポーリングサイクルよりも早く構成変更があった選択されたNetScalerインスタンスもポーリングできるようになりました。この機能強化により、デフォルトのポーリング間隔は720分に変更されました。**Infrastructure > Network Functions**で**Settings**をクリックすると、**Network Functions based on Configuration Change**の下に新しいオプション**Perform Network Functions Polling on receiving "netScalerConfigChange" event**が表示されるように

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

なりました。このオプションは、**Delay time for Network Functions**で15分の間隔でデフォルトで有効になっています。

現在、NetScalerインスタンスで構成変更イベントが発生した場合、NetScaler Consoleは、15分間隔の後、これらのインスタンスのみをポーリングします。

注記:

- デフォルトのポーリング間隔（すべてのNetScalerインスタンスをポーリングするため）を30分から1440分の間の値に変更できます。
- デフォルトの15分間隔の値（選択されたインスタンスのみをポーリングするため）を5分から60分の間の値に変更できます。
- **Perform Network Functions Polling on receiving "netScalerConfigChange" event**を無効にできます。無効にすると、NetScaler Consoleはデフォルトのポーリングサイクルに従ってすべてのNetScalerインスタンスをポーリングします。

詳細については、ポーリングの概要を参照してください。

修正された問題

Build Sep 19, 2024で対処された問題。

インフラストラクチャ

エクスポートレポート通知メールの内容がRFC 5322に準拠していません。

StyleBook

- `snmptrap_snmpuser_binding` を持つStyleBook定義からconfigpackを作成すると、「list index out of range」というエラーメッセージが表示されて失敗します。
- StyleBookを設定する際、入力概要ビューで、選択したデータソースの読み取り可能な名前の代わりにGUIDが表示されます。

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

September 03, 2024

可観測性

可観測性ツール (Splunk、New Relic、Microsoft Sentinel) でNetScaler Consoleの監査ログデータを表示する

Splunk、New Relic、またはMicrosoft SentinelとのNetScaler Consoleサービス統合のために、**設定 > 可観測性統合**で新しいサブスクリプションを作成する際、**NetScaler Console監査ログ**オプションを選択できるようになりました。サブスクリプションを設定すると、これらの可観測性ツールでNetScaler Consoleの監査ログを表示できます。

詳細については、以下を参照してください。

- Splunkとの統合
- New Relicとの統合
- Microsoft Sentinelとの統合

修正された問題

Build Sep 03, 2024で対処された問題。

分析

- **Web Insight**で、日次レポートのデータエクスポート（表形式）をスケジュールすると、レポートには毎日同じデータが表示されます。
- **Web Insight**で、カスタム日付範囲が1日を超えるとデータが表示されません。

August 27, 2024

分析

グローバル分析の構成

カスタムポリシーとグローバルポリシーを使用して、グローバル分析を構成できるようになりました。

- **カスタムポリシー** - カスタムポリシーを使用すると、特定のインサイトのみを必要とするインスタンスまたは仮想サーバーを制御できます。
- **グローバルポリシー** - グローバルポリシーを使用すると、既存の管理対象仮想サーバーおよび新規仮想サーバーで分析を構成および有効にできます。

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

最大10個のポリシーを作成できます。9個のカスタムポリシーと1個のグローバルポリシー、または10個のカスタムポリシーです。**Settings > Analytics Configuration**に移動し、**Global Analytics Summary**の下にある**Global Analytics Configuration**をクリックして、カスタムポリシーまたはグローバルポリシーを構成します。

詳細については、グローバル分析の構成を参照してください。

アプリケーション

アプリケーションをA+ SSL評価にアップグレードした場合、アップグレード後7日以内のみ元の評価に戻すことができます。

アプリケーションダッシュボード - アプリケーション（仮想サーバー）にタグを作成して適用する

アプリケーションダッシュボードで、アプリケーションにタグを作成して適用できるようになりました。これらのタグは検索機能を向上させます。タグを作成して検索バーをクリックすると、タグを使用して検索を絞り込むことができます。

詳細については、アプリケーションにタグを作成して適用するを参照してください。

StyleBook

StyleBookの外部で作成された構成を再利用し、ConfigPack間で構成を共有する

NetScalerで以前にStyleBookの外部で作成された構成を、StyleBook構成パックの一部として統合および管理できるようになりました。さらに、複数の構成パック間で構成を共有できるようになり、より柔軟で一元化された管理が可能になります。

詳細については、「設定パックの作成と編集」を参照してください。

修正された問題

Build Aug 27, 2024で対処された問題。

分析

Web Insightでは、すべての管理対象インスタンスで同じ名前を持つ仮想サーバーのデータが表示されません。

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

インフラストラクチャ

- 管理対象インスタンスが10000を超えるヘルスモニターをサービスグループにバインドするように構成されている場合、NetScaler Consoleのメモリ使用率が増加します。その結果、NetScaler Consoleにアクセスできなくなる可能性があります。

- Microsoft AzureでNetScalerエージェントまたは NetScaler VPXをプロビジョニングする際、NetScaler Console ProvisioningサービスAPIがAzureサブネットの詳細を取得できません。

July 25, 2024

修正された問題

インフラストラクチャ

「**Infrastructure > Upgrade Jobs**」で、クラシックポリシーを持つNetScalerインスタンスをアップグレードすると、アップグレード前の検証でそのインスタンスが「**Instances blocked from upgrade**」としてリストされ、アップグレードは実行されません。

回避策: インスタンスをアップグレードする前に、NSPEPIツールでサポートされている機能について、クラシックポリシーをアドバンストポリシーに変換することをお勧めします。詳細については、「クラシックポリシーを使用した構成のアップグレードに関する考慮事項」を参照してください。

テレメトリ

NetScalerテレメトリプログラムの一環として、NetScaler Consoleは以下の構成を24時間ごとにチェックしたり、NetScalerインスタンスにプッシュしたりしなくなりました。以前は、構成が欠落している場合、24時間ごとにチェックされ、NetScalerインスタンスにプッシュされていました。

```
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
```

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

July 15, 2024

インフラストラクチャ

NetScaler Console SSLダッシュボードでの3072ビット暗号化キーのサポート

証明書に3072ビットのキー強度を持つエンタープライズポリシーを構成できるようになりました。「**Infrastructure > SSL Dashboard > Settings > Enterprise Policy > Recommended key strengths**」で、3072ビットの暗号化キーを選択します。以前は、512、1024、2048、4096ビットのキー強度のみが利用可能でした。

詳細については、以下を参照してください。NetScaler Consoleサービスの場合: エンタープライズポリシーの構成NetScaler Consoleオンプレミスの場合: エンタープライズポリシーの構成

NetScaler Console GUIでNetScalerが所有するIPアドレスを表示およびエクスポートする

NetScaler Console GUIでNetScalerが所有するIPアドレス（**Infrastructure > Instances > NetScaler Owned IPs**）を表示およびエクスポートできるようになりました。

詳細については、「NetScalerが所有するIPアドレスの表示」を参照してください。

ライセンス

FlexedライセンスダッシュボードでSDXインスタンスにプロビジョニングされたVPXインスタンスの詳細を表示

Flexedライセンスダッシュボード（**NetScaler Licensing > Flexed Licensing > Dashboard**）の**Licensed NetScalers**の下で、NetScaler SDX用にチェックアウトされたVPXインスタンスの数を表示できます。インスタンス名、IPアドレス、スループット（MBPS）、エディションなど、そのSDXにプロビジョニングされたVPXインスタンスの詳細を表示するために、この数をクリックできるようになりました。

以前は、そのSDX用にチェックアウトされたVPXインスタンスの総数のみを表示できました。

ゼロキャパシティライセンスでMPX/SDXホストIDとシリアル番号の詳細を表示

NetScaler Licensing > Zero-capacity licensesで、MPXおよびSDXインスタンスの**ホストID**と**シリアル番号**の詳細を表示できるようになりました。

修正された問題

Build Jul 15, 2024 で対処された問題。

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

インフラストラクチャ

- **NetScaler Console (Infrastructure > Instances > NetScaler)**で、サイトや管理者プロファイルを変更するなど、インスタンスを変更すると、そのインスタンスに関連付けられたタグのキーと値のペアが逆になります。

- Config Jobで、HAペアのプライマリとセカンダリの両方のNetScalerでShowConfigurationテンプレートを同時に実行すると、をクリックしても、セカンダリインスタンスのファイルのみがダウンロードされます。

- ネットワークレポート (インフラストラクチャ > ネットワークレポート) にダッシュボードが存在しない場合、次のエラーメッセージが表示されます。

  「このページにアクセスする権限がありません」

  このエラーメッセージは無視しても問題なく、ダッシュボードの作成を妨げるものではありません。

- 組み込みエージェントを使用して構成されている場合、NetScaler ConsoleサービスでSNMPトラップが受信されません。

StyleBook

NetScaler Console GUIで、異なるStyleBookを使用するように構成パックを編集すると、アップグレードが期待どおりに機能しません。

July 09, 2024

CVE-2024-5491およびCVE-2024-5492の特定と修正のサポート

NetScaler Consoleサービスセキュリティアドバイザリは、CVE-2024-5491およびCVE-2024-5492の特定と修正をサポートするようになりました。

- CVE-2024-5491の特定には、バージョンと構成スキャンの組み合わせが必要です。
- CVE-2024-5492の特定には、バージョンスキャンが必要です。

脆弱なNetScalerインスタンスを、修正を含む推奨ビルド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.

注:

セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。

詳細については、「セキュリティ速報」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2024-5491およびCVE-2024-5492の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、 をクリックしてオンデマンドスキャンを開始できます。

June 18, 2024

テレメトリ

NetScalerテレメトリプログラム

既存のNetScaler Consoleのお客様は、ライセンスと機能の使用状況に関するテレメトリデータ収集を必要とするNetScalerテレメトリプログラムに準拠する必要があります。テレメトリデータは24時間ごとに自動的にアップロードされ、お客様側での操作は不要です。

- 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。
- テレメトリパラメータの詳細については、「データガバナンス」を参照してください。

June 11, 2024

分析

仮想サーバーレベルで有効化されたメトリクスコレクターとリーン期間使用状況分析

メトリクスコレクターとリーン使用状況分析が、インスタンスレベルではなく仮想サーバーレベルで有効になりました。この機能強化により、メトリクスコレクターとリーン使用状況分析は、トラフィックの多いアクティブな仮想サーバーでのみ有効になります。

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

仮想サーバーを確認し、他の仮想サーバーで**メトリクスコレクター**とリーン使用状況を有効にするには、**設定 > 分析構成**に移動し、**仮想サーバーメトリクス概要**の下にある**メトリクスを構成**をクリックします。

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。

メトリクス収集のためにNetScalerインスタンスにネットプロファイルを割り当てる

NetScaler Consoleで仮想サーバーのメトリクスコレクターを有効にすると、NetScalerからのメトリクスデータはNetScalerサブネットIPアドレス（SNIP）を介してNetScaler Consoleにエクスポートされます。一部のシナリオでは、ネットワーク内のファイアウォールによってSNIPがブロックされる場合があります。このようなシナリオでは、別のIPアドレスを使用する必要がある場合があります。ネットプロファイルの詳細については、「バックエンド通信に指定されたソースIPを使用する」を参照してください。

メトリクス収集のためにNetScalerインスタンスにネットプロファイルを割り当てることができるようになりました。メトリクスコレクターは、NetScalerカウンターデータをNetScaler Consoleにプッシュし、これはアプリケーションの問題を検出するために使用されます。**インフラストラクチャ > インスタンス > NetScaler**に移動し、インスタンスを選択し、**アクションの選択**リストから**メトリクスコレクターのネットプロファイルを構成**をクリックします。

ネットプロファイルの割り当ての詳細については、「管理対象NetScalerインスタンスにネットプロファイルを割り当てる」を参照してください。

可観測性統合 - 失敗したNetScalerサブスクリプションの詳細を表示

可観測性統合では、NetScalerからSplunkまたはPrometheusへのサブスクリプションを構成する際に、失敗したサブスクリプションの詳細なログを表示できるようになりました。管理者として、これらのログを使用して、サブスクリプション失敗の理由を分析できます。

詳細については、「失敗した構成のログを表示する」を参照してください。

可観測性統合におけるWAFおよびBotインサイトの定期エクスポートオプションの削除

NetScaler Consoleから可観測性ツール（Splunk、New Relic、Microsoft Sentinelなど）へのインサイトのエクスポートを設定する際、WAFおよびBotインサイトの定期エクスポートオプションは削除されました。WAFおよびBot違反は重要であるため、発生時にリアルタイムでインサイトをエクスポートするには、リアルタイムエクスポートオプションを使用することをお勧めします。

WAFおよびBotの定期エクスポート設定を持つ既存のサブスクリプションは、すべて自動的にリアルタイムエクスポートに変更されます。

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

インフラストラクチャ

「アプリベース」プロビジョニングのサポート

NetScaler Consoleサービスは、AWSおよびAzure向けに「アプリベース」プロビジョニングを導入しました。この機能により、クラウドデータセンターでのNetScaler展開が合理化および簡素化され、これらの環境からの効率的なアプリケーション配信が可能になります。

詳細については、AWSでのアプリベースのプロビジョニングおよびAzureでのアプリベースのプロビジョニングを参照してください。

修正された問題

Jun 11, 2024 ビルドで対処された問題。

分析

- NetScaler Console/Agentのプロセスがメモリ破損によりクラッシュする可能性があります。
- **Web Insight**では、コンテンツスイッチング仮想サーバーの背後に構成された負荷分散仮想サーバーの詳細が、日次、週次、月次レポートで表示されません。

インフラストラクチャ

- 非管理者ユーザーがNetScaler Consoleで仮想サーバーの統計情報（**Infrastructure > Network Functions**）を表示しようとすると、次のエラーメッセージが表示されます。

  「<vserver_name>へのアクセスは許可されていません」

- HAセットアップで、組み込みエージェント「mastools」をパーティションとともに使用すると、セカンダリNetScalerインスタンスのステータスがSSLダッシュボード（**Infrastructure > SSL Dashboard**）および負荷分散（**Infrastructure > Network Functions > Load Balancing**）で「不明」になります。

StyleBooks

- 構成パックを編集しても、ACLまたはポリシーベースルーティング（PBR）ルールに対して行われた追加、更新、削除などの変更は適用されません。

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

June 5, 2024

分析

NetScaler Console と Microsoft Sentinel の統合機能

Observability Integrationで、NetScaler ConsoleとMicrosoft Sentinelの統合を構成して、Microsoft Sentinelでインサイトをエクスポートおよび表示できるようになりました。統合を成功させるには、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。

- **Azure subscription** - Microsoft Sentinelを展開して使用するためのAzureサブスクリプション。
- **Log Analytics Workspace** - 収集されたデータを保存および分析するには、ワークスペースが必要です。
- **IAM ロール** - ワークスペースには、閲覧者、共同作成者などの権限レベルを設定する必要があります。
- **カスタムテーブル** - NetScaler Console データをワークスペースに保存して送信するため。

詳細については、「Microsoft Sentinel との統合」を参照してください。

プラットフォーム

OpenSSH バージョン 9.x のサポート

NetScaler の OpenSSH バージョンが 8.x から 9.x にアップグレードされました。

StyleBook

設定パックのドラフトとして保存オプション

設定パックをドラフトとして保存できるようになりました。設定をドラフトとして保存するには、次の手順に従います。

1. **アプリケーション > 構成 > 設定パック**に移動します。
2. **構成**ページで、**追加**をクリックします。
3. StyleBook を選択し、**選択**をクリックします。
4. 「**構成の作成**」ページで、「**ドラフトとして保存**」をクリックします。

保存されたドラフトは、「**保留中の構成**」の下にある「**ドラフト構成**」タブに表示されます。

詳細については、「構成パックをドラフトとして保存する」を参照してください。

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

構成パックのスケジュールオプション

新しく作成された構成パックの展開をスケジュールできるようになりました。新しい構成パックのスケジュールを作成するには、次の手順に従います。

1. **アプリケーション > 構成 > 構成パック**に移動します。
2. 「**構成**」ページで、「**追加**」をクリックします。
3. スタイルブックを選択し、「**選択**」をクリックします。
4. 「**構成の作成**」ページで、「**実行**」の下にある「**実行モード**」リストから「**後で**」を選択します。
5. スケジュールする希望の時間と日付を選択します。

展開済みの構成パックの場合、更新を公開するタイミングと構成パックを削除するタイミングをスケジュールできます。スケジュールオプションは、展開済みの構成パックを編集するときに利用できます。

詳細については、「構成パックのスケジュールを作成する」を参照してください。

修正された問題

Build Jun 5, 2024で対処された問題。

アナリティクス

- **概要**ダッシュボードの**アプリケーションヘルス**の詳細には、**App Dashboard**の**アプリケーションスコア**で利用できるものと同じ詳細が表示されません。

- NetScaler Console を介して 25000 を超える仮想サーバーが管理されている場合、App Dashboard で詳細の読み込みに時間がかかることがあります。

インフラストラクチャ

- サービスグループの状態が変更されたときに、イベントルールが予期されるアクションを生成できません。

StyleBook

- StyleBook のカスタムデータソースに、IPアドレス、整数、またはブール型のフィールドに空の値を持つコレクションデータを追加すると、操作が失敗する可能性があります。

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

- NetScaler Console GUI から構成パックを作成すると、システムは組み込みの managed-adc データソースを参照するパラメータに対して空のリストを返すことがあります。

- 構成パックを作成しようとしたり、ドライランを実行したりすると、次の両方の条件が満たされている場合に操作が失敗する可能性があります。

  - StyleBookの定義が、コンポーネントセクション内で別のStyleBookを参照しています。
  - 現在のStyleBookと参照されているStyleBookの間で、「datum」タイプのパラメータをプロパティに割り当てる場合。

May 22, 2024

分析

SSL A+評価アップグレードタスクを使用してSSL仮想サーバーを一括アップグレードする

タスクで、**SSL A+評価アップグレード**タスクを表示できるようになりました。**App Dashboard**の既存のA+ SSL評価へのアップグレードプロセスでは、一度に1つのアプリケーションしかアップグレードできません。**SSL A+評価アップグレード**タスクを使用すると、一括アップグレードを実行できます。

NetScaler Consoleは、NetScalerセキュアフロントエンドプロファイルを使用してアプリケーション仮想サーバーのSSL構成をレビューし、A+評価ではないアプリケーションを特定します。**SSL A+評価アップグレード**タスクは、A+評価ではないアプリケーションを表示します。管理者として、アプリケーションを選択し、一括アップグレードを実行してSSLコンプライアンスを達成できます。

詳細については、「実行可能なタスクと推奨事項」を参照してください。

ライセンス

Flexedライセンスレポートにおける実際の使用状況の詳細

「**フレックスライセンスレポート**」ダッシュボード（**NetScaler Licensing > Flexed Licensing > Reporting**）では、実際の帯域幅/スループット使用量を確認できるようになり、消費の詳細（ピーク使用量と平均使用量）を把握できます。以前は、ダッシュボードには割り当てとエンタイトルメントの詳細のみが表示されていました。

さらに、Flexedライセンスレポートダッシュボードでは、以下の機能強化も利用できます。

- 選択したNetScalerインスタンスの詳細を表示するためのフィルター。

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

- PDF、PNG、JPEG形式で詳細をエクスポートするオプション。
- 帯域幅はスループット容量に名称変更されました。

詳細については、「Flexed license reporting」を参照してください。

StyleBooks

StyleBooksでNetScalerポリシー式を作成する

StyleBooks GUIでは、リストから項目を選択することでNetScalerポリシー式を構築できるようになり、より迅速かつ正確に式を作成できるようになりました。パラメータでポリシー式エディタを使用できるようにするには、StyleBooksのパラメータ定義で`is_policy_expression` GUI属性を指定します。

詳細については、「Policy expressions in StyleBooks」を参照してください。

修正された問題

Build May 22, 2024 で対処された問題。

インフラストラクチャ

Config Jobで、HAペアのプライマリとセカンダリの両方のNetScalerで**ShowConfiguration**テンプレートを同時に実行すると、**Download Result Files**をクリックしても、セカンダリインスタンスのファイルのみがダウンロードされます。

StyleBooks

NetScaler Consoleから管理アクセスにサブネットIPアドレス (SNIP) を使用するNetScalerインスタンスを削除し、その後そのインスタンスを再追加すると、インスタンス削除前に作成された設定パックに対する操作が失敗する可能性があります。

April 23, 2024

分析

カスタムNetScalerインスタンスの定期的なデータエクスポートのサポート

NetScaler ConsoleからSplunkまたはNew Relicへのデータエクスポートのサブスクリプションを作成する際、**定期エクスポート** (日次または時間単位) を選択し、カスタムインスタンスに適用で

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

きるようになりました。以前は、カスタムインスタンスへの定期的なインサイトデータのエクスポートはサポートされていませんでした。

インフラストラクチャ

ディスク使用率に関する追加のイベントアラート

NetScaler Consoleでは、ディスク使用率アラームの追加のしきい値を設定できるようになりました。このしきい値を使用すると、上限しきい値に達する前にアラートを受信する下限レベルを設定できます。下限レベルのしきい値を設定するには、**設定 > SNMP > 編集** に移動し、**下限レベルのしきい値を構成** を有効にします。

詳細については、「システムアラームの設定と表示」を参照してください。

修正された問題

Build April 23, 2024 で対処された問題。

インフラストラクチャ

- NetScaler Consoleレポートを**インフラストラクチャ > インスタンス > NetScaler**でスナップショットとしてエクスポートしようとすると、ページが応答しなくなります。

- NetScaler Consoleでエージェントを介して10を超えるNetScalerインスタンスが管理されている場合、エージェントインベントリサブシステムが失敗します。その結果、NetScaler Consoleは最新のNetScaler構成データをフェッチしません。

ライセンス

- Flexed Licenseダッシュボードに表示されるインスタンスの数が正しくありません。

セキュリティ

- **セキュリティ > セキュリティ違反 > すべての違反 > 違反の詳細**で**今すぐエクスポート**または**エクスポートをスケジュール**オプションを使用して違反レコードを表形式でエクスポートする場合、**エクスポートするレコード数**で選択されたレコード数に関係なく、現在のページビューに表示されているレコードのみがレポートに含まれます。

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

April 10, 2024

分析

可観測性統合 - NetScalerメトリクスと監査ログのSplunkへのエクスポート設定のサポート

設定 > 可観測性統合で、NetScalerメトリクスと監査ログのSplunkへのエクスポートを設定できるようになりました。

詳細については、「NetScalerメトリクスと監査ログのSplunkへのエクスポートを設定する」を参照してください。

インフラストラクチャ

ホスト名によるNetScaler GUIへのアクセス

「**Infrastructure > Instances > NetScaler**」を介してNetScalerに接続すると、ホスト名をクリックすることで、ホスト名を介してNetScaler GUIへの接続が確立されるようになりました。以前は、ホスト名またはIPアドレスのいずれかをクリックすると、NSIPを介してNetScaler GUIへの接続が開始されていました。

アップグレード中の高可用性ノード間の不一致の表示

NetScalerの高可用性展開をアップグレードする際に、プライマリノードとセカンダリノード間の構成の不一致を表示できるようになりました。不一致を確認し、アップグレードを続行するか停止するかを決定できます。この機能を使用するには、「**Infrastructure > Upgrade Jobs**」に移動し、「**Pre-upgrade validation**」タブで不一致を表示します。

詳細については、「アップグレードジョブ」を参照してください。

修正された問題

Build April 10, 2024で対処された問題。

インフラストラクチャ

- syslogメッセージに上付き文字などの特殊文字が含まれている場合、「**Infrastructure > Events > Syslog Messages**」ページが空白で表示されます。

- SSL証明書に証明書チェーンがある場合、「**Infrastructure > SSL Dashboard > Usage**」に表示される使用済みおよび未使用の証明書の数が正しくありません。

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

ライセンス

- エージェントの再起動後、プールライセンスまたはフレックスライセンスに必要なポート27000および7279が利用できなくなる場合があります。このような場合、プールライセンスまたはフレックスライセンスを使用しているNetScalerインスタンスは猶予期間に入る可能性があります。

セキュリティ

- **セキュリティ > WAF推奨** に移動すると、次のエラーメッセージが表示されることがあります。

  「HTTPエラー500 () データエンドポイント「apps」へのアクセス中に発生」

March 26, 2024

修正された問題

Build March 26, 2024 で対処された問題。

インフラストラクチャ

- アップグレードジョブの作成または更新中に、**インフラストラクチャ > アップグレードジョブ > ジョブの作成 > インスタンスの選択 > インスタンスの追加** でインスタンスを選択しようとすると、**インスタンスの追加** ページにワークフローに適用されない **パーティション** タブが表示されます。パーティションを選択すると、ページが応答しなくなり、それ以上進むことができません。

- **設定 > 通知 > Slack > Slack通知の作成** でSlack通知を作成し、**添付ファイル付き通知** を選択すると、通知が表示されず、次のエラーメッセージが表示されます。

  `Invalid token`

StyleBooks

- **> > >** で オプションが選択されているときに、デバイスAPIプロキシ操作を実行しようとすると、操作は失敗します。

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

March 12, 2024

ライセンス

NetScaler ConsoleサービスでNetScalerエージェントをLSAとして手動で選択するサポート

NetScalerプールライセンスまたはNetScalerフレックスライセンスのライセンスサーバーエージェント (LSA) として、NetScalerエージェントを手動で選択できるようになりました。

LSAがダウンしている場合、NetScaler Consoleサービスは次のLSAを自動選択する前に24時間待機します。管理者は、この機能を使用して、その間に新しいLSAを手動で選択できます。ただし、管理者は、選択される新しいLSAのステータスが**UP**であり、その診断ステータスが**OK**であることを確認する必要があります。

詳細については、フレックスまたはプールライセンスのNetScalerエージェントの動作を参照してください。

修正された問題

Build March 12, 2024 で対処された問題。

分析

- Gateway仮想サーバーで**Gateway Insight**を有効にすると、**Settings > Analytics Configuration > All Virtual Servers**の**Analytics Status**列に**Disabled**と表示されます。

- **Gateway > Gateway Insight**では、**Authentication**タブに認証失敗のユーザー詳細が表示されません。

インフラストラクチャ

- ユーザー定義ポリシーが作成され、そのポリシーにユーザーが追加されると、特定のリソースに対するGET APIリクエストで権限の問題が発生し、次のエラーが表示されます。

  「必要な権限が付与されていないため、承認されていません」

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

February 28, 2024

インフラストラクチャ

VIPライセンスとNetScaler Console Serviceストレージの更新

- **NetScaler Consoleサービスでの無制限のVIP**: NetScaler Consoleサービスリリース14.1-21.x以降、ライセンスされたVIPの概念は削除されました。NetScaler Consoleサービスでは、無制限のVIPが利用可能になりました。VIPライセンスSKUはまもなく販売終了（EOS）および更新終了（EOR）となるため、NetScaler Console仮想サーバーライセンスを購入する必要はなくなります。
- **NetScaler Consoleサービスストレージ**:
  - NetScaler ConsoleサービスストレージSKUはまもなく販売終了（EOS）および更新終了（EOR）となります。
  - NetScaler Consoleサービスのデフォルトのストレージエンタイトルメントは5GBになりました。
  - 過去に購入されたNetScaler Consoleサービスストレージライセンスは、期間が終了するまで有効です。
  - 過去に購入されたNetScaler Console VIPライセンスで、NetScaler Consoleサービスストレージの比例的なエンタイトルメントが付与されていたものは、期間が終了するまで有効です。
  - より高いNetScaler Consoleストレージエンタイトルメントが付与される他のライセンスパッケージを購入した場合、デフォルトの5GBは、そのエンタイトルメントに合わせて変更されます。

分析およびメトリクスコレクターの更新

- 14.1 21.xビルド以降の無制限VIPサポートにより、既存および新規のすべての仮想サーバーが自動的にライセンス付与されるようになりました。仮想サーバーを明示的にライセンス付与することなく、分析を有効にできます。
- 14.1 21.xビルド以降、NetScaler Consoleに追加された新しいNetScalerインスタンスでは、すべてのNetScalerライセンスタイプでメトリクスコレクターがデフォルトで無効になりました。既存の管理対象インスタンスのメトリクスコレクター構成は変更されません。

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

分析

アクションポリシー - アプリケーション使用状況の通知を構成する

アクションポリシー（**Settings > Actions > Action Policies**）で、アプリケーション使用状況のアクションポリシーを構成し、**Requests per second**、**Throughput**、**Data Volume**オプションを選択できるようになりました。これらのオプションを使用すると、1秒あたりのリクエストの平均、1秒あたりのリクエストの異常、スループットの平均、スループットの異常、総データ量、およびデータ量の異常に関する通知を構成して受信できます。詳細については、「アプリケーションイベント通知を受信するためのアクションポリシーの構成」を参照してください。

可観測性統合

SplunkおよびNew Relicとの統合のための構成ワークフローが、ユーザーエクスペリエンス向上のために強化され、**Settings > Observability Integration**で利用できるようになりました。以前は、SplunkおよびNew Relicとの統合のための構成ワークフローは**Settings > Ecosystem Integration**で利用可能でした。

詳細については、「可観測性統合」を参照してください。

可観測性統合 - NetScalerメトリクスをPrometheusにエクスポートする設定のサポート

設定 > 可観測性統合で、デフォルトスキーマを選択することで、NetScalerメトリクスをPrometheusにエクスポートするように設定できるようになりました。

詳細については、Prometheus統合および可観測性統合を参照してください。

Gateway Insight - レポートのエクスポートの改善

Gateway > Gateway Insightで、各メトリクス（EPA、認証、承認失敗、SSO、アプリケーション起動）の下にあるすべてのテーブルの設定アイコンを使用して、選択したオプションのみを含むレポートをエクスポートできるようになりました。以前は、エクスポートされたレポートには、選択されたオプションに関係なくすべての情報が表示されていました。

StyleBook

デフォルトStyleBookの更新

NetScalerバージョン10.5に基づくデフォルトStyleBookは、今後のリリースで非推奨になります。NetScalerバージョン13.0に基づく新しいデフォルトStyleBookのセットが、**アプリケーション > 構成 > StyleBook > デフォルトStyleBook**で利用可能になりました。

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

StyleBookをクローンするオプション

NetScaler Consoleでは、管理者がStyleBookとその依存関係の複製を作成できるようになりました。管理者は、`parameters`や`components`の更新など、追加のカスタマイズのためにこのバンドルを使用できます。

この機能を使用するには、**アプリケーション > 構成 > StyleBook**に移動し、デフォルトまたはカスタムのStyleBookを選択して、**クローン**をクリックします。

詳細については、「StyleBook のクローン作成」を参照してください。

修正された問題

Build Feb 28, 2024 で対処された問題。

インフラストラクチャ

- NetScaler Console から NetScaler Console サービスへの移行が失敗し、特定の Azure Active Directory グループが NetScaler Console サービスで利用できません。この問題は、NetScaler Console で作成された Azure Active Directory グループ名にスペースが含まれているために発生します。

- 複数の Azure Active Directory グループに属しているユーザーは、NetScaler Console にアクセスできません。

- **Web Insight** および **Security Violations** では、GUI のスケジュールエクスポートワークフローがユーザーエクスペリエンス向上のために強化されました。

- **インフラストラクチャ > ネットワークレポート**では、表形式のエクスポートレポートに、サービス、サービスグループ、仮想サーバー、インターフェイス名などの詳細が含まれていません。

- フレキシブルライセンスダッシュボードには、プレミアム帯域幅ライセンスプールから少なくとも 1 つの NetScaler がチェックアウトされた後にのみ、NetScaler の詳細が表示されます。

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

February 06, 2024

アナリティクス

アプリダッシュボード - NetScaler管理者パーティションからのアプリケーションメトリック詳細表示のサポート

アプリダッシュボードで、NetScaler管理者パーティションから作成されたアプリケーションのメトリック詳細を表示できるようになりました。以前は、管理者パーティションからのアプリケーションはメトリックなしでしか表示できませんでした。

インフラストラクチャ

Citrix Cloud™でのNetScaler ADMのブランド変更

14.1 16.xビルド以降、NetScaler ADMサービスはNetScaler Consoleサービスにブランド変更されました。引き続き、Application Delivery Managementは以下の場所でNetScaler Consoleにブランド変更されます。

- Citrix Cloudホームページの**マイサービス**の下にあるタイル。
- **Citrix Cloudメニュー > マイサービス**のサービス名。
- **Citrix Cloudメニュー > IDおよびアクセス管理 > 管理者 > 管理者/グループの追加**から、**アクセス設定 > カスタムアクセス**の管理者追加ワークフローにおける製品名。

アップグレードジョブでデフォルトの検証スクリプトを実行する

NetScaler Consoleには、アップグレードジョブワークフローにデフォルトの検証スクリプトのオプションが含まれるようになりました。これらのデフォルトスクリプトは、アップグレードジョブの前後に実行され、差分レポートを生成します。カスタムのデフォルトスクリプトを実行するオプションも引き続き利用できます。

詳細については、「NetScalerインスタンスのアップグレード」を参照してください。

NetScaler Consoleサイトのレーダーオブジェクト展開を自動化

NetScalerは、NetScaler Consoleサイトへのレーダーオブジェクト展開の自動化をサポートしており、NetScalerインスタンスでの手動展開の必要性を排除します。

この機能強化は、NetScalerインスタンスを編集する場合にのみ利用可能で、サイトタイプが**データセンター**（タイプ**プライベート**を含む）または**ブランチ**の場合にのみ適用されます。

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

リアルユーザー測定リストから**NetScalerに展開**を選択すると、**NetScalerインスタンス**リストが自動的に入力され、レーダーオブジェクト (r20.gif) を展開する特定のインスタンスを選択できます。

詳細については、「レーダーオブジェクト展開の自動化」を参照してください。

修正された問題

Build Feb 06, 2024で対処された問題。

分析

- **XML SQL**攻撃は、セキュリティダッシュボード（**セキュリティ > セキュリティダッシュボード**）とセキュリティ違反ダッシュボード（**セキュリティ > セキュリティ違反**）の両方で報告されません。

ライセンス

- フレックスライセンスダッシュボードは、プレミアム帯域幅ライセンスプールから少なくとも1つのNetScalerがチェックアウトされた後にのみ、NetScalerの詳細を表示します。

管理と監視

- 構成ジョブが作成されると、**Infrastructure > Configuration > Jobs** のステータスは **Completed** と表示されますが、**Details > Execution Summary** には 0% 完了と表示されます。

- NetScaler HA の 2 段階アップグレードジョブのステータスは、NetScaler HA アップグレードが完了しているにもかかわらず、「Scheduled」と表示されます。プライマリノードは完了と表示されますが (**Status Stage 1: Completed)**、セカンダリノードはスケジュール済みと表示されます (**Stage 2: Scheduled**)。

- **Infrastructure > Configuration > Audit Templates > Add** で名前に特殊文字を含む構成監査テンプレートが作成されると、テンプレートは正常に生成されます。ただし、ポーリング中に **Configuration Audit** ダッシュボードでそのテンプレートの差分レポートが生成されません。

  この問題は、- (ダッシュ) および '_' (アンダースコア) 以外の特殊文字が使用された場合に発生します。

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

January 24, 2024

分析

タスクでアップグレードアドバイザリの詳細を表示

Tasks で、**Upgrade Advisory** の実行可能なタスクを表示できるようになりました。現在の利用状況に基づいて、NetScaler インスタンスが 90 日以内に End-of-Life (EOL) または End-of-Maintenance (EOM) に達しているか、達しようとしている場合、**Upgrade Advisory** タスクはそれらのインスタンスの詳細を表示します。**Take Action** をクリックして、それらのインスタンスを推奨ビルドにアップグレードできます。

インフラストラクチャ

読み取り専用ユーザーの権限強化

以下の機能に対する読み取り専用権限を持つユーザーは、NetScaler インスタンスをポーリングできるようになりました。

- SSL証明書 (**インフラストラクチャ > SSLダッシュボード > 今すぐポーリング**)
- ネットワーク機能 (**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**)
- 構成監査 (**インフラストラクチャ > 構成 > 構成監査 > 今すぐポーリング**)

修正された問題

Build Jan 24, 2024で対処された問題。

- NetScaler SDXの組み込みエージェント登録は成功メッセージを表示しますが、SDXインスタンスは**インフラストラクチャ > インスタンスダッシュボード**に表示されません。

- **インフラストラクチャ > ネットワーク機能 > 負荷分散**で、**サーバー**タブにはサーバーの数が表示されますが、非デフォルトユーザーのテーブルエントリは表示されません。

January 16, 2024

CVE-2023-6548およびCVE-2023-6549の特定と修復のサポート

NetScaler Console service Security Advisoryは、CVE-2023-6548およびCVE-2023-6549の特定と修復をサポートするようになりました。

- CVE-2023-6548の特定にはバージョンスキャンが必要です。

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

- CVE-2023-6549の特定には、バージョンと構成スキャンの組み合わせが必要です。

修正には、脆弱なNetScalerインスタンスを、修正を含む推奨ビルドにアップグレードする必要があります。

注:

セキュリティアドバイザリは、サポート終了 (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

NetScaler 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。

詳細については、「セキュリティ速報」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2023-6548およびCVE-2023-6549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。

January 09, 2024

分析

カスタムダッシュボードを他のユーザーと共有するサポート

管理者として、カスタムダッシュボードを他のユーザーと共有できるようになりました。**概要 > カスタムダッシュボード**で、ダッシュボードを選択し、**共有**をクリックします。ユーザー名を入力し、**招待**をクリックしてダッシュボードを共有します。割り当てられたユーザーは、ダッシュボードを読み取り専用モードで表示できます。

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

インフラストラクチャ

NetScaler ConsoleサイトでITMレーダーを構成する

ITMレーダーは、ネットワーク監視機能を強化します。データセンター、仮想マシン、またはクラウドプロバイダーに展開されたサイトは、パフォーマンスメトリックに関する洞察を提供するレーダーオブジェクト (r20.gif) をホストできるようになりました。ITMレーダーオブジェクトは、貴重なエンドユーザーアプリケーション統計を積極的に収集し、より効果的なネットワーク監視と情報に基づいたトラフィック管理の決定のために、堅牢なITMレーダーテレメトリをサイトに提供します。

詳細については、「ITMレーダーの構成」を参照してください。

SplunkおよびNew Relicでゲートウェイインサイトデータを表示

NetScaler ConsoleサービスとSplunkおよびNew Relicの統合のために、**Settings > Ecosystem Integration** で新しいサブスクリプションを作成する際に、**Gateway Insights** オプションを選択できるようになりました。**Gateway Insights** オプションでサブスクリプションを構成すると、SplunkおよびNew Relicでゲートウェイインサイトデータを表示できます。

詳細については、「Splunkとの統合」および「New Relicとの統合」を参照してください。

SSLデータをSplunkおよびNew Relicに即座にエクスポート

管理者がSplunkおよびNew Relicで **SSL Certificate Insight** を選択してサブスクリプションを作成すると、SSLデータはすぐにSplunkおよびNew Relicにエクスポートされるようになりました。以前は、管理者はデータを初めてエクスポートするために **Poll Now** (**Infrastructure > SSL Dashboard**) をクリックする必要がありました。

タスクでアップグレードアドバイザリの詳細を表示

Tasks で、**Upgrade Advisory** の実行可能なタスクを表示できるようになりました。現在の利用状況に基づいて、NetScalerインスタンスが90日以内にEnd-of-Life (EOL) またはEnd-of-Maintenance (EOM) に達しているか、または達しようとしている場合、Upgrade Advisoryタスクはそれらのインスタンスの詳細を表示します。**Take Action** をクリックして、それらのインスタンスを推奨ビルドにアップグレードできます。

アクションポリシー - リクエスト、帯域幅、応答時間の通知を構成

Action Policies (**Settings > Actions > Action Policies**) で、Application Performanceでアクションポリシーを構成する際に、**Requests**、**Bandwidth**、および **Response Time** オプションを選択できるようになりました。これらのオプションを使用すると、合計リクエスト、合計帯域幅、平

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

均応答時間、および応答時間の異常に関する通知を構成および受信できます。詳細については、「アプリケーションイベント通知を受信するためのアクションポリシーの構成」を参照してください。

さらに、これらのメトリックについて、**Web Insight** のグラフ傾向からアクションポリシーを設定できるようになりました。管理者として、任意のアプリケーションでこれらのメトリックに異常なトラフィックパターンや急激なスパイクを検出した場合、この機能強化により、グラフ上の特定のポイントに配置した後、**Create Action Policy** をクリックして相対アクションポリシーを作成できます。

修正された問題

Jan 09, 2024ビルドで対処された問題。

ライセンス

- Flexed または Pooled ライセンスが適用された後、**Analytics Configuration** ページ (**Settings > Analytics Configuration**) が正しい詳細で更新されません。
- **NetScaler Licensing > Flexed Licensing > Dashboard** の Flexed ライセンスダッシュボードが空白で表示されます。
- **NetScaler Licensing > License Management** で、電子メール通知によるしきい値超過の構成が期待どおりに機能しません。

既知の問題

NetScaler Application Delivery Management (NetScaler Console) には、以下の既知の問題があります。

ライセンス

- この問題は、SDXが、あらゆる種類のNetScalerローカルライセンス（固定容量サブスクリプションまたは永続ライセンス）のファイルベースライセンスから、LASベースのライセンスを持つあらゆる種類のライセンスに移行済みまたは移行中の場合で、レガシーなファイルベースライセンスがSVMから削除されていない場合に影響します。

  影響: LASへの移行後もローカルのレガシーなファイルベースライセンスがSVM上に残っている場合、そのファイルベースライセンスの有効期限切れにより、そのライセンスファイルの有効期限日にSDX（SVMおよびSDX上のVPX）のライセンスが解除されます。

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

回避策: LASへの移行が正常に完了した後、SVM上のローカルファイルベースライセンスを削除します。ファイルベースライセンスはSVMフォルダー /mpsconfig/license にあり、シェルプロンプトを使用してこのフォルダーから削除する必要があります。

管理と監視

- IOCスキャンを開始したときと、IoCスキャン結果の両方で、管理パーティションが表示されます。IOCスキャンはNetScalerアプライアンス全体をカバーするため、これらのエントリは無視できます。

- ファイル整合性監視スキャンで脆弱性が見つからない場合、NetScaler® Console CVEアドバイザリは誤った全体的な重大度を表示する場合があります。正しい重大度は、詳細なCVEビューに表示されます。

- **Infrastructure > SSL Dashboard > Manage Certificate Store** で **NetScaler証明書のインポート** をクリックすると、NetScaler ConsoleはPFX形式のNetScaler証明書をインポートできません。

インフラストラクチャ

- NetScaler Consoleで、インスタンスがシステムグループに対して承認され、新しいパーティションがインスタンスに追加されると、システムグループの承認設定が新しいパーティションに自動的に割り当てられます。

- NetScaler BLX™インスタンスに証明書をインストールしようとすると、インストールが失敗し、**Infrastructure > SSL Dashboard > SSL Audit Logs**ページに次のエラーメッセージが表示されます。

  `SCP: Authentication by password fails on _<ip-address>_.`

- **Infrastructure > Events > Rules > Create rule > Select Failure Objects**で一部のエンティティを選択してイベントルールを作成すると、選択したすべてのエンティティが表示されません。この問題は、仮想サーバー、サービス、またはサービスグループの数が多い場合に発生します。

  回避策: この問題については、NetScalerサポートチームにお問い合わせください。

- **Configuration Jobs**で使用されるSSHまたはSCP操作が、次のエラーメッセージで失敗する可能性があります。

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

SSH sshセッションの確立に失敗しました: -5

回避策:

a. SSHクライアントを使用してNetScaler Consoleにログオンします。

b. 次のコマンドの出力を確認します。

```
ls -l /etc/sshd_config
```

c. `/etc/sshd_config` で、次を追加するように更新します。

```
HostKey /nsconfig/ssh/ssh_host_ecdsa_key
```

d. 変更を適用します:

```
ps -aux | grep /usr/sbin/sshd | grep -v grep | tr -s ' ' | cut -d ' ' -f 2 | xargs kill -9
```

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

データコンプライアンス

PCI DSS コンプライアンス

決済カード業界 (PCI) データセキュリティ基準 (DSS) は、クレジットカード業界のセキュリティ標準であり、クレジットカードデータを保存、処理、または送信する際に必要となる、人、プロセス、テクノロジーに対するセキュリティレベルを定義しています。PCI DSSは、加盟店、処理業者、サービスプロバイダー、およびクレジットカードデータを保存、処理、または送信するその他すべての事業体に適用されます。PCI DSS準拠証明書 (AOC) は、最終的に、特定のセキュリティレベルが必要であり、それが存在することを事業体が証明するものです。

PCI DSSコンプライアンスロゴ(/en-us/netscaler-console-service/media/pci-compliance-logo.png)

NetScaler® Application Delivery Managementサービス PCI DSSコンプライアンス

NetScaler Application Delivery Management (ADM) サービスは、お客様向けのPCI DSSコンプライアンス管理ドメインに対する評価により、PCI DSSコンプライアンスを正常に達成しました。NetScaler Consoleサービスは、お客様のPCIデータを保存、処理、または送信しません。NetScaler Consoleサービスは、当社のサービスと管理を評価するために、毎年、認定セキュリティ評価機関 (QSA) によるPCI DSS評価も受けます。

Citrixは顧客のPCI DSSコンプライアンスをサポートしますが、NetScaler製品およびサービスを使用するだけでは、それ自体でPCI DSSコンプライアンスを達成することはできません。顧客は、PCI DSSコンプライアンス要件を達成および維持するために、適切なコンプライアンスプログラム、内部プロセス、および管理策が導入されていることを確認する責任があります。

オフラインレポートをダウンロードするには、NetScaler Console Service PCI Attestation of Compliance (AOC)をクリックしてください。

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

NetScaler® テレメトリプログラム

NetScaler テレメトリプログラムは、顧客がメンテナンスおよびサポートのライセンス義務を遵守するために必要なライセンスおよび機能の使用状況データのアップロードを可能にする、必須のデータ収集プログラムです。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 の展開および機能の使用状況テレメトリデータを収集します。NetScaler Console の構成および機能の使用状況データも、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。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当社の製品およびサービスの強化をサポートするために、NetScaler インスタンスを NetScaler Console に追加することを強くお勧めします。詳細はこちら。NetScaler テレメトリプログラムは、ビルド 14.1-28.x 以降で自動的に有効になります。

前提条件

以下を確認してください。

- エージェントが最新バージョンで実行されていること。デフォルトでは、エージェントは自動的にアップグレードされます。一部のシナリオでは、エージェントが古いバージョンで実行されている場合があり、エージェントを手動でアップグレードする必要があります。エージェントを手動でアップグレードする方法の詳細については、エージェントの手動アップグレードを参照してください。
- NetScaler エージェントがポート 22 で NetScaler と通信できること。
- NetScaler Gateway テレメトリデータを受信するために、ネットワークでポート 5140 が許可されていること。(VPN 仮想サーバー構成を持つ NetScaler インスタンスにのみ適用されます)。

注：

- テレメトリのアップロードは、24 時間ごとに自動的に行われます。
- 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するために、2024 年 6 月 18 日にリリースされた NetScaler テレメトリプログラムの一部として、以下の構成が NetScaler Console を介して NetScaler インスタンスにプッシュされました。

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

```
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
```

- NetScaler テレメトリプログラムの一部としてプッシュされたテレメトリメトリックプロファイルを、次のコマンドを使用して削除する必要があります。

```
rm analytics profile telemetry_metrics_profile
```

- 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
```

- Gateway テレメトリのために、`/nsconfig/.telemetry.conf` ファイルが次のコマンドで更新されます。NetScaler Console は、このコマンドを毎時間チェックし、このコマンドが見つからない場合は追加します。このコマンドは、VPN 仮想サーバー構成を持つ NetScaler インスタンスにのみプッシュされます。

```
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、テレメトリを介し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、論理的な資産照合の目的のみに使用されます。

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

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

カテゴリ	説明	使用目的
ライセンス、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のため、およびサービスを管理、測定、改善するため。
NetScaler Console の展開と機能使用状況のテレメトリ	Console の展開と機能の使用状況に関する情報。	サービスを管理、測定、改善するため。

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。

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

データガバナンス

NetScaler ConsoleサービスはCitrix Cloudサービスの一部であり、サインアップ、オンボーディング、認証、管理、ライセンス供与のためのプラットフォームとしてCitrix Cloudを使用します。Citrixは、NetScaler Consoleサービスの一部として、Citrix Cloudでデータを収集および保存します。このドキュメントでは、収集されるデータと、データ収集、保存、送信の方法について説明します。

Citrixにおけるデータ保護の慣行の詳細については、「Citrix Cloud Services Data Protection Overview」を参照してください。

この情報は、セキュリティ担当者、コンプライアンス担当者、情報監査担当者、ネットワークインフラストラクチャおよび運用管理者、事業部門の責任者を対象としています。

NetScaler®テレメトリプログラム

NetScalerテレメトリプログラムは、NetScaler Consoleサービスで**14.1-28.x**ビルドから有効になっています。このプログラムにより、必要なデータが自動的にアップロードされます。収集される必要なテレメトリの詳細については、「Data Governance for NetScaler Telemetry」を参照してください。

データの収集、保存、送信方法?

NetScaler Consoleサービスは、管理対象インスタンスとエージェントからデータを収集します。これらのインスタンスはお客様のオンプレミスに展開され、エージェント（お客様のオンプレミスに展開）から、TLS 1.2プロトコルを使用して暗号化されたSSLチャネルを介して、安全にクラウドにデータが送信されます。

データは、データベース層でのマルチテナントデータ分離を備えたリレーショナルデータベースに保存され、お客様が選択したPoint of Presence (POP) に応じて、米国、EMEA（フランクフルト）、APJ（シドニー）のAWSクラウドでホストされているElastic File System (EFS) のファイルとして保存されます。すべてのPoPはAWS Commercialリージョンでホストされています。

パスワード、SNMPコミュニティ文字列、SSL証明書、およびNetScaler構成バックアップは、テナントごとに一意のAES 256キーを使用して暗号化され、データベースに安全に保存されます。Citrix Cloudが使用する商用リージョンと、各リージョン内でのNetScaler Consoleサービスの存在の詳細については、「Geographical Considerations」を参照してください。

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

データカテゴリ

データ処理の慣行については、データは次のように分類されます。

- **顧客コンテンツ** - ストレージのためにお客様のアカウントにアップロードされたデータ、または特定のサービスを実行するためにNetScalerがアクセスを許可されているお客様のコンピューティング環境内のデータ。
- **ログ** - サービスに関する記録を含みますが、これらに限定されません。
  - パフォーマンス、安定性、使用状況、セキュリティ、サポートに関するデータと情報
  - デバイス、システムに関する技術情報

顧客コンテンツ

NetScaler Console Service は、さまざまなソースから情報を収集します。

- NetScaler
- ネットスケーラー ゲートウェイ
- NetScaler Web App Firewall (WAF) およびボット管理

NetScaler Console Service は、ログに記載されている情報に加えて、管理者のセッションおよびアクティビティの詳細に関する情報も収集します。

ログ

ログは、ソフトウェア更新のプロビジョニング、ライセンス認証、サポート、分析、およびCitrix User Agreementsに準拠したその他の目的を促進するために使用されます。

収集されるメタデータおよびテレメトリログには、次のものが含まれます。

- NetScaler Service エージェントハイパーバイザー、パブリッククラウドプラットフォーム、またはその両方（エージェントハイパーバイザーとパブリッククラウドプラットフォーム）
- エージェントの地理的位置
- NetScaler のバージョン
- NetScaler の製品タイプ
- ライセンス情報（Express およびサブスクリプション）
- NetScaler Console管理者がクラウドサービスを利用すること（これにより、管理者ユーザーエクスペリエンスが向上します）。

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

詳細な顧客コンテンツとログ

- **イベント管理（ログイン > インフラストラクチャ > イベント）**
  - NetScalerネットワークの状態とパフォーマンスに関するアラートを提供するSNMPトラップ。
  - NetScalerネットワークの状態情報を経由するWebトランザクションのSyslog。
  - イベントのSMS/Slack通知をトリガーするためのSMSサーバー、Slack、およびPagerDutyプロファイルの詳細。
  - メール設定用のSMTPサーバーの詳細。
  - ServiceNowでチケットを作成するためのServiceNowプロファイルの詳細。
- **SSL証明書管理（ログイン > インフラストラクチャ > SSLダッシュボード）**
  - NetScalerインスタンスによって最適化されたWebアプリのSSL証明書、SSLキー、SSL CSR、CA発行者、および署名アルゴリズム。
- **構成監査（ログイン > インフラストラクチャ > 構成 > 構成監査）**
  - NetScalerインスタンスに関連するNetScaler構成監査変更のデータ追跡。これには、Webアプリサーバーの IPアドレスとNetScalerのIPアドレスの詳細が含まれます。
- **構成ジョブ（ログイン > インフラストラクチャ > 構成 > 構成ジョブ）**
  - NetScaler構成の詳細、インスタンスIPアドレス、およびWebアプリサーバーのIPアドレスの詳細。
- **StyleBooks（ログイン > アプリケーション > 構成 > StyleBooks）**
  - NetScaler構成がテンプレートとして保存され、Webアプリサーバーの IPアドレス詳細が含まれます。
- **インスタンス管理 (ログイン > インフラストラクチャ > インスタンス)**
  - NetScalerインスタンスのIPアドレス、NetScalerインスタンスタイプ、NetScaler構成バックアップ、NetScalerの重大なイベント、およびNetScalerインスタンスが展開されているデータセンターの地理的位置（構成されている場合）。
- **インフラストラクチャ分析 (ログイン > インフラストラクチャ > インフラストラクチャ分析)**
  - NetScalerインスタンスのIPアドレス、NetScalerインスタンスタイプ、NetScalerの重大なイベント、関連付けられているアプリの数、およびNetScalerインスタンスが展開されているデータセンターの地理的位置（構成されている場合）。

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

- **アプリケーション (ログイン > アプリケーション)**
  - アプリケーションダッシュボード: アプリケーションURL、リクエストメソッド、レスポンスコード、合計バイト数、Webアプリサーバーの詳細、仮想サーバーIPアドレス、クライアントの詳細、ブラウザ、クライアントOS、クライアントデバイス、SSLプロトコル、SSL暗号強度、SSLキー強度、NetScalerインスタンスIPアドレス、サーバーフラップのタイムスタンプ、およびレスポンスコンテンツタイプ。
- **分析 (AppFlow/ Logstream)**
  - **Web Insights (ログイン > アプリケーション)**: 仮想サーバーIPアドレス、クライアント、URL、ブラウザ、オペレーティングシステム、リクエストメソッド、レスポンスステータス、ドメイン、WebアプリサーバーIPアドレス、SSL証明書、ネゴシエートされたSSL暗号、SSLキー強度、SSLプロトコル、およびSSL障害フロントエンド。
  - **HDX Insight (ログイン > Gateway)**: ICAユーザーの詳細、ICAアプリケーションの詳細、VDAサーバーの詳細、HDX Insightのデスクトップの詳細、アプリクライアントの地理的位置の詳細、HDXアクティブセッションの詳細、HDX用VPNライセンス、クライアントNetScaler IPアドレス、クライアントタイプ、およびバージョン。
  - **Gateway Insight (ログイン > Gateway)**: ユーザーの詳細、アプリケーションの詳細、ブラウザ、オペレーティングシステム、セッションモード、Gatewayライセンス、AAAサーバーの詳細、およびGatewayで構成されたAAAポリシー。
  - **セキュリティ違反 (ログイン > セキュリティ)**: クライアントIP、URL、セキュリティ違反(WAFおよびBot)、攻撃の地理的位置、攻撃タイムスタンプ、トランザクションID、WAF、およびNetScalerセキュリティ構成ステータス。
  - **API分析 (ログイン > セキュリティ > API Gateway)**: APIインスタンス、APIエンドポイント、合計帯域幅、APIパフォーマンス情報、合計リクエスト、応答時間、エラーに関する情報。各APIインスタンスをさらにドリルダウンして、個々のAPIエンドポイントとパフォーマンスを可視化する機能。認証の成功、失敗に関連するセキュリティ。レート制限、SSL暗号、プロトコル情報、およびSSLエラー。
- **セキュリティアドバイザリ (ログイン > インフラストラクチャ > インスタンスアドバイザリ > セキュリティアドバイザリ)**
  - **バージョンスキャン**: このスキャンでは、NetScaler ConsoleがNetScalerインスタンスのバージョンと、修正が利用可能なバージョンおよびビルドを比較する必要があります。このバージョン比較により、NetScaler Consoleのセキュリティアドバイザリは、NetScalerがCVEに対して脆弱であるかどうかを特定できます。このスキャンの根底にあるロジックは、NetScalerリリースおよびビルドxx.yyでCVEが修正された場合、xx.yyビルドよりも低

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

いビルドのすべてのNetScalerインスタンスが脆弱であると見なされるというものです。バージョンスキャンは現在、セキュリティアドバイザリでサポートされています。

- **構成スキャン**：このスキャンでは、NetScaler ConsoleがNetScaler構成ファイルとCVEスキャンに固有のパターンを照合する必要があります。特定の構成パターンがNetScaler ns.confファイルに存在する場合、そのインスタンスはそのCVEに対して脆弱であると見なされます。このスキャンは通常、バージョン スキャンと組み合わせて使用されます。

  構成スキャンは現在、セキュリティアドバイザリでサポートされています。

- **カスタムスキャン**：このスキャンでは、NetScaler Consoleサービスが管理対象のNetScalerインスタンスに接続し、スクリプトをプッシュして実行する必要があります。スクリプトの出力は、NetScalerがCVEに対して脆弱であるかどうかをNetScaler Consoleが特定するのに役立ちます。例としては、特定のシェルコマンド出力、特定のCLIコマンド出力、特定のログ、特定のディレクトリまたはファイルの存在または内容などがあります。構成スキャンで対応できない場合、セキュリティアドバイザリは複数の構成パターンの一致にもカスタムスキャンを使用します。カスタムスキャンを必要とするCVEの場合、スケジュールされたスキャンまたはオンデマンドスキャンが実行されるたびにスクリプトが実行されます。そのCVEに関するセキュリティアドバイザリドキュメントで、収集されるデータと特定のカスタムスキャンのオプションについて詳しく学習してください。

セキュリティ

Citrix Services Security Exhibitでは、アクセスと認証、システム開発と保守、セキュリティプログラム管理、資産管理、暗号化、運用管理、人事セキュリティ、物理セキュリティ、事業継続性、インシデント管理など、Citrix Cloud Servicesに適用されるセキュリティ制御について詳しく説明しています。

Citrix Cloud製品のセキュリティは、暗号化およびキー管理ポリシーによって制御されます。Citrixが製品開発ライフサイクル全体でセキュリティをどのように採用しているかの詳細については、Security Development Processesホワイトペーパーを参照してください。

NetScaler Console Serviceのデータ保持ポリシー

NetScaler Console内の統計測定値、ダッシュボード、レポート、アラート、イベント、ログなどのデータ、およびログイン詳細は、お客様がサービスを購読している期間保持されます。その後、ユーザーアカウントはExpressアカウントに変換され、ユーザーは2つの仮想サーバーのみを管理できます。

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

Expressアカウントの容量は500 MBまたは1日分の分析/レポートデータであり、いずれかの制限に最初に達した方が適用されます。Expressアカウントが使用されない場合、またはお客様が30日以上アカウントにログインしない場合、アカウントおよび関連するすべての顧客コンテンツは自動的に削除されます。

Citrix Cloud Servicesアカウントのデータ保持と削除の詳細については、Citrix Cloud Services Data Protection Overviewを参照してください。

注

NetScaler Consoleのすべての分析データは、最大30日間保持されます。

サードパーティサービス

NetScaler Console Serviceは、お客様が選択したPoint of Presence (POP) に応じて、米国、EMEA (フランクフルト)、APJ (シドニー) リージョンのAmazon Web Service (AWS) データセンター内でホストされます。

現在、NetScaler Console Serviceは、さまざまなサードパーティテクノロジーのサービスとAPIを使用しています。

- 製品機能に使用されるサービス:
  - AWS EFS、AWS RDS、AWS エラスティックキャッシュ、AWS ALB、AWS Route 53、AWS EKS、AWS シークレットマネージャー、AWS ECR リポジトリ、および AWS MSK。
- NetScaler Console の監視と運用に使用されるサードパーティサービスおよびツールは次のとおりです。
  - オンコールローテーションのための PagerDuty
  - Splunk を使用したログ分析
  - ログ集約のための Fluentd
  - コミュニケーションとアラートのための Slack
  - AWS クラウドウォッチ、SQS
  - AWS のストレージ領域としての S3 –コアファイルとメトリックの保存用
  - 監視のための Prometheus および Grafana (Honeycomb 展開の場合)

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

参照

- 収集されたデータへのアクセス方法の詳細については、「Citrix Services Security Exhibit」を参照してください。
- 収集されたデータの保持期間の詳細については、「Citrix Cloud Services Data Protection Overview」を参照してください。
- Citrix Cloud 技術セキュリティ概要。
- Citrix Cloud 技術的および組織的なデータセキュリティ対策。

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

IoC情報の利用条件

IoC情報（以下に定義）を使用することにより、お客様は以下の利用条件を認識し、同意するものとします。

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

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

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

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

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

はじめに

このドキュメントでは、NetScaler Console のオンボーディングと初回セットアップを開始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、NetScaler Gateway、Citrix Secure Web Gateway など）を管理するネットワーク管理者およびアプリケーション管理者を対象としています。NetScaler Console を使用して管理するデバイスの種類に関係なく、このドキュメントの手順に従ってください。

オンボーディングを開始する前に、ブラウザ要件、エージェントインストールの要件、およびポート要件を確認してください。

ステップ1：Citrix Cloud™ にサインアップする

NetScaler Console の使用を開始するには、まず Citrix Cloud 企業アカウントを作成するか、社内の他のユーザーが作成した既存のアカウントに参加する必要があります。詳細なプロセスと手順については、Citrix Cloud へのサインアップを参照してください。

ステップ2：Express アカウントで NetScaler Console を管理する

Citrix Cloudにログオンしたら、次の操作を行います。

注:

- 日本の場合、`citrix.citrixcloud.jp`にログオンする必要があります。
- Government Cloud の場合、`citrix.cloud.us`にログオンする必要があります。

1. **Available Services** セクションに移動します。
2. **NetScaler® Console** タイルで、**Manage** をクリックします。

   NetScaler Console タイルが **My Services** セクションに移動します。
3. ビジネスニーズに合ったリージョンを選択します。

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

重要

- 後でリージョンを変更することはできません。
- Citrix Cloud Japan (`citrix.citrixcloud.jp`) または Citrix Cloud Government (`citrix.cloud.us`) からログインする場合、この手順は適用されません。適用されるエンドポイント URL へのアクセスが許可されていることを確認する必要があります。詳細については、「システム要件」を参照してください。

4. ご自身に適用される役割とユースケースを選択してください。

初期化がバックグラウンドで完了するまで時間がかかる場合がありますが、その間ブラウザからログオフできます。

注:

Citrix は、NetScaler Console リソースを管理するために Express アカウントを割り当てます。NetScaler Console Express アカウントが 45 日間非アクティブのままの場合、そのアカウントは削除されます。詳細については、「Express アカウントを使用して NetScaler Console を管理する」を参照してください。

Citrix Cloud アカウントに再度ログインすると、**NetScaler Console GUI** 画面が表示されます。**Get Started** をクリックして、サービスを初めてセットアップします。

ステップ 3: NetScaler 展開タイプを選択する

NetScaler インスタンスを展開または検出するには、次の手順を実行します。

1. 次のいずれかの環境を選択します。
   - **オンプレミス**
   - **AWS**
   - **マイクロソフト アジュール**
   - **グーグル クラウド プラットフォーム**
2. データセンターまたはクラウド内の NetScaler Console と管理対象インスタンス間の通信を有効にするには、エージェントをインストールします。

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

「**エージェントタイプの選択**」ステップでは、選択した環境に応じてエージェントのインストールオプションが異なります。

- **外部VMエージェント**
  - **オンプレミス** - **オンプレミス**を選択し、次に**ハイパーバイザー上**を選択した場合、Citrix Hypervisor™ VMware ESXi、Microsoft Hyper-V、Linux KVM Serverなどの任意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。
  - AWS、Microsoft Azure、Google Cloud Platformなどのパブリッククラウドのいずれかを選択した場合、選択したクラウドに**外部エージェント**をインストールできます。
- **マイクロサービスとして** - エージェントをKubernetesアプリケーションとして展開します。
- **組み込みエージェント** - NetScaler内にエージェントを展開します。

3. **次へ**をクリックします

エージェントをインストールする手順は、オプションごとに異なります。以下のリンクは、エージェントをインストールするための特定の手順を示しています。

- ハイパーバイザー
- 外部エージェント
- マイクロサービスとして
- 組み込みエージェント

ハイパーバイザーにエージェントをインストールする

ハイパーバイザーにエージェントをセットアップするには、次の手順を実行します。

1. ハイパーバイザーを選択し、**イメージのダウンロード**をクリックして、エージェントイメージをローカルシステムにダウンロードします。

   サービスURLとアクティベーションコードが生成され、GUIに表示されます。
2. サービスURLとアクティベーションコードをコピーします。
3. ハイパーバイザーにエージェントをインストールする際に、コピーしたサービスURLとアクティベーションコードを指定します。

   エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。オンプレミスハイパーバイザーにエージェントをインストールす

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

る方法の詳細については、「オンプレミスにエージェントをインストールする」を参照してください。

4. エージェントのインストールが正常に完了したら、**エージェントのセットアップ**ページに戻り、**エージェントの登録**をクリックします。

次のステップ: インスタンスの追加。

注

初期設定中にエージェントを追加したくない場合は、**スキップ**をクリックしてNetScaler Consoleが提供する機能を確認してください。エージェントとインスタンスは後で追加できます。後でエージェントを追加するには、**設定 > エージェントのセットアップ**に移動します。後で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。

パブリッククラウドに外部VMエージェントをインストールする

エージェントのセットアップページからエージェントイメージをダウンロードする必要はありません。エージェントイメージは、それぞれのクラウドマーケットプレイスで入手できます。

1. エージェントのインストール時に使用するサービスURLとアクティベーションコードをコピーして保存します。

   新しいアクティベーションコードが必要な場合は、**新しいアクティベーションコードを作成**をクリックし、エージェントのインストール時に使用するコードをコピーして保存します。

   - Microsoft Azureクラウドにエージェントをインストールする方法の詳細については、「Microsoft Azure Cloudにエージェントをインストールする」を参照してください。
   - AWSにエージェントをインストールする方法の詳細については、「AWSにエージェントをインストールする」を参照してください。
   - Google Cloudにエージェントをインストールする方法の詳細については、「GCPにエージェントをインストールする」を参照してください。

2. エージェントのインストールが成功したら、**Set Up Agent** ページに戻り、**Register Agent** をクリックします。

次のステップ: インスタンスの追加。

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

マイクロサービスとしてエージェントをインストールする

Kubernetesクラスターにマイクロサービスとしてエージェントを展開し、NetScaler Consoleで**サービスグラフ**を表示できます。

サービスグラフの開始方法の詳細については、サービスグラフの設定を参照してください。

1. 次のパラメータを指定します。
    a. **アプリケーション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。
    b. **エージェントパスワード** – CPXがこのパスワードを使用してエージェント経由でCPXをNetScaler Consoleにオンボードするためのパスワードを指定します。
    c. **パスワードの確認** – 確認のために同じパスワードを指定します。
    d. **Submit** をクリックします。
2. **Submit** をクリックすると、YAMLまたはHelm Chartをダウンロードできます。
3. **Close** をクリックします。

    詳細については、Kubernetesクラスターにエージェントをインストールするを参照してください。

組み込みエージェントを使用する

環境内のNetScalerインスタンスには、組み込みエージェントが含まれています。組み込みエージェントを起動し、それを使用してインスタンスとNetScaler Console間の通信を確立できます。

1. 生成された**サービスURL**と**アクティベーションコード**をコピーします。NetScalerインスタンスで組み込みエージェントを起動する際に使用するために保存してください。

    NetScalerインスタンスで組み込みエージェントを起動する方法の詳細については、「NetScalerインスタンスで組み込みエージェントを起動する」を参照してください。
2. 組み込みエージェントが起動したら、**エージェントのセットアップ**ページに戻り、**インスタンスの登録**をクリックします。

次のステップ: インスタンスの追加。

インスタンスの追加

インスタンスとは、NetScaler Consoleから検出、管理、監視したいネットワーク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、インスタンスをサービスに追加する必要があります。

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

エージェントのインストールと登録が正常に完了すると、エージェントは**エージェントのセットアップ**ページに表示されます。エージェントのステータスが隣の緑色の点で示されるUP状態になったら、**次へ**をクリックしてサービスにインスタンスの追加を開始します。

1. **インスタンスの追加**ページで、登録済みエージェントに接続されているNetScalerインスタンスを表示します。インスタンスが**Up**ステータスであることを確認し、**次へ**をクリックします。
2. **完了**をクリックして初期設定を完了し、展開の管理を開始します。

注

初期設定中にインスタンスを追加したくない場合は、**完了**をクリックして設定を完了し、後でインスタンスを追加できます。後でNetScaler Consoleにインスタンスを追加する方法については、「インスタンスの追加」を参照してください。

NetScaler Console GUIダッシュボードを使用してNetScalerインスタンスをオンボードする

NetScaler Consoleを初めてセットアップする際に、**はじめに**ワークフローでNetScalerインスタンスのオンボーディングをスキップした場合でも、NetScaler Console GUIダッシュボードからインスタンスをオンボードできます。NetScalerインスタンスがまだ追加されていない場合、GUIはインスタンスの追加を促します。

左側のナビゲーションバーのモジュールをクリックすると、右側にそのモジュールの機能と利点の表形式のプレビューが表示されます。これらの機能と利点は、NetScaler Consoleを使用してNetScalerインスタンスをより適切に管理するのに役立ちます。

「**NetScalerインスタンスの追加**」をクリックして、インスタンスをオンボードします。「**開始**」ワークフローが再起動します。このドキュメントに記載されているステップ3: NetScaler展開タイプの選択以降の手順に従って、インスタンスをオンボードします。 NetScalerインスタンスがすでにオンボードされている場合、NetScaler Consoleにログオンすると、左側にナビゲーションバーがあるNetScaler Consoleのランディングページのみが表示されます。

エージェントのアクション

NetScaler Consoleを設定した後、エージェントにさまざまなアクションを適用できます。「**インフラストラクチャ > インスタンス > エージェント**」に移動します。

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

「**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**: 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。
- **エージェントのパスワードを変更**: インフラストラクチャのセキュリティを確保するために、エージェントのデフォルトパスワードを変更します。
- **テクニカルサポートファイルを生成**: 選択した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。

エージェントの診断を表示し、エンドポイント検証のアラートを受信する

NetScaler Consoleは、エージェントに対して定期的な（1時間ごとの）診断チェックを実行し、次の情報を提供します。

- **エンドポイントの到達可能性** – すべてのエンドポイントに到達可能かどうかを確認します。エージェントは、NetScaler ConsoleとNetScalerインスタンス間の通信にさまざまなエンドポイントを使用します。詳細については、「ソフトウェア要件」を参照してください。
- **ヘルスチェックプローブ** – 最新のヘルスチェックのタイムスタンプを提供します。
- **エージェントプロキシ** – エージェントプロキシが存在するかどうかを確認します。

エージェントのエンドポイント到達可能性ステータスが変更された場合（「**OK**」から「**要確認**」へ）、スーパー管理者は問題の詳細を含むメール通知を受け取ります。「**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、新しく追加された「**診断ステータス**」オプションを表示し、「**要確認**」または「**OK**」などのステータスを確認します。

クリックして、エージェントの診断情報を表示します。

- **カテゴリ**。問題のカテゴリを提供します。
- **ステータス**。**要確認**や**OK**など、問題のステータスを提供します。
- **推奨事項**。問題のトラブルシューティングに必要な推奨事項を提供します。

トラブルシューティングを行い、エンドポイントの到達可能性ステータスが**要確認**から**OK**に変わると、スーパー管理者には問題が解決されたことを知らせるメール通知が届きます。

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

メール通知

次の例は、エンドポイントの到達可能性ステータスが**OK**から**要確認**に変わった後のメール通知です。

次の例は、エンドポイントの到達可能性ステータスが**要確認**から**OK**に変わった後のメール通知です。

インスタンスを管理するように組み込みエージェントを構成する

NetScaler MPX、VPX、Gateway インスタンス (バージョン `12.1.48.13` 以降を実行) および NetScaler SDX インスタンス (バージョン 13.0 61.x 以降および 12.1 58.x 以降を実行) で、組み込みエージェントを利用できます。データセンターまたはパブリッククラウドに専用エージェントをインストールする代わりに、NetScaler インスタンスでこのエージェントを起動できます。組み込みエージェントは、インスタンスとNetScaler Console間の通信を可能にします。

注:

組み込みエージェントは、以下のNetScalerインスタンスタイプでのみ利用可能です。

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

組み込みエージェントは、小規模なNetScalerスタンドアロンまたはHAペア展開に最適です。複数のNetScalerインスタンスがある場合は、展開に専用エージェントを使用してください。このエージェントは、組み込みエージェントよりも優れたデータ集約機能を提供します。詳細については、「オンプレミスにエージェントをインストールする」を参照してください。

NetScaler Consoleの組み込みエージェントは、インスタンス管理、監視、およびプールまたはフレックスライセンスをサポートしています。ただし、組み込みエージェントでは以下の機能はサポートされていません。

- アプリケーションダッシュボード
- ウェブ インサイト

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

- SSL インサイト
- HDX™ インサイト
- ゲートウェイ インサイト
- セキュリティインサイト
- 高度な分析
- プールまたはフレックスライセンス (ファイルベースライセンス)

組み込みエージェントから外部エージェントに移行できます。詳細については、「組み込みエージェントから外部エージェントへの移行」を参照してください。

前提条件

NetScalerインスタンスで組み込みエージェントを構成する前に、以下を確認してください。

- NetScaler (MPX、VPX、またはGateway) インスタンスはバージョン `12.1.48.13` 以降で実行されています。SDXインスタンスはバージョン `13.0.61.x` 以降で実行されています。
- NetScalerインスタンスにDNSネームサーバーが追加されています。

  詳細については、「ネームサーバーの追加」を参照してください。
- Citrix Cloudアカウントをお持ちであること。詳細については、「Citrix Cloudへのサインアップ」を参照してください。

注:

ポートおよびその他のシステム要件に関するすべての情報については、「システム要件」を参照してください。

組み込みエージェントの構成

NetScaler組み込みエージェントを構成するには、次のタスクを実行します。

1. 「はじめに」の指示に従って、 オプションを選択します。
2. 「**サービスURL**」と「**アクティベーションコード**」をコピーします。

   エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。MPXまたはGatewayのお客様は、手順7をスキップしてください。

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

3. SSHクライアントを使用して組み込みエージェントを起動します。Gatewayユーザーはこの手順をスキップする必要があります。

   a. NetScalerインスタンスにログオンします。詳細については、「NetScalerへのアクセス」を参照してください。

   b. `/var/mastools/scripts`ディレクトリに移動し、次のコマンドを入力します。

   SDXインスタンスの場合

	NETSCALERプロファイルでの登録	NETSCALERプロファイルなしでの登録
前提条件	登録する前に、NetScalerプロファイルを作成します。詳細については、「NetScalerプロファイルの作成方法」を参照してください。	
このコマンドを実行します	`./mastools_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile`	`./mastools_init.sh <user_name> <service-url> <activation-code> -sdx`
ユーザー資格情報	`<device_profile_name>`に`nsroot`を入力します。または、nsrootと同じアクセス権限を持つユーザー名を使用することもできます。	`<user_name>`に`nsroot`を入力します。または、nsroot と同じアクセス権限を持つユーザー名を使用することもできます。

注：

NetScaler Console は、その SDX で実行されているすべての VPX インスタンスを検出し、VPX インスタンスを個別に登録する必要はありません。

SDX アプライアンスで実行されていない VPX インスタンス、および MPX および Gateway インスタンスの場合：

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

NetScaler イメージのバージョンが 13.0 61.x または 12.1 57.x より低い場合は、コマンド `cat /var/mastools/version.txt` を入力して `mastools` のバージョンを確認する必要があります。出力が `0.0-0.0` の場合、初回です。

ソフトウェアのバージョンに応じて、次のいずれかのコマンドを入力します。

注：

NetScaler プロファイルに登録する前に、プロファイルを作成する必要があります。詳細については、「NetScaler プロファイルの作成方法」を参照してください。

NETSCALER イメージバージョン	MASTOOLS_VERSION は `0.0-0.0` ですか？	プロファイルを使用した登録コマンド	プロファイルを使用しない登録コマンド
13.0 61.xx および 12.1 57.xx より低い	はい	`./mastools_init.sh <device_profile_name> <service_url> "MAS;<activation_code>" -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> "MAS;<activation_code>"`
13.0 61.xx および 12.1 57.xx より低い	いいえ	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`
13.0 61.x および 12.1 57.xx より高い	該当なし	`./mastools_init.sh <device_profile_name> <service_url>`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

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

NETSCALER イメージバージョン	MASTOOLS_VERSION は 0.0-0.0 ですか？	プロファイルを使用した登録コマンド	プロファイルを使用しない登録コマンド
		`<activation_code> -profile`	

注:

- `<device_profile_name>` または `<user_name>` に、`nsroot` と入力します。または、nsroot と同じアクセス権限を持つユーザー名を使用することもできます。
- HAペアでは、プライマリノードで登録を完了します。セカンダリノードで登録コマンドを実行すると、次のメッセージが表示されます: **プライマリノードで登録コマンドを実行してください。**

4. NetScaler Consoleページに戻り、**インスタンスの登録**をクリックします。
5. **インスタンスの追加**で、組み込みエージェントを起動したインスタンスを表示します。インスタンスが**稼働中**ステータスであることを確認し、**次へ**をクリックします。
6. **完了**をクリックします。

組み込みエージェントの構成が成功すると、NetScaler Consoleの機能にアクセスできます。たとえば、次のとおりです。

- **仮想サーバーと分析** – 仮想サーバーにライセンスを適用して、NetScalerインスタンスを管理します。詳細については、「サブスクリプションの管理」を参照してください。
- **アプリケーションダッシュボード** – すべてのアプリケーションを包括的に表示します。詳細については、「アプリケーション管理とダッシュボード」を参照してください。
- **インフラストラクチャ分析** – この機能は、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。詳細については、「インフラストラクチャ分析」を参照してください。

NetScaler®組み込みエージェントを介したライセンスサーバーの構成

注:

NetScaler組み込みエージェントにはLSAロールを割り当てることはできません。

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

あるサイトでライセンスサーバーエージェント (LSA) が構成されており、他のサイトから同じLSAを使用したい場合は、NetScaler組み込みエージェントを使用できます。組み込みエージェントを使用している間は、NetScalerインスタンスで次のコマンドを使用してライセンスサーバーを構成する必要があります。

```
add licenseserver 127.0.0.1 -port 27000
```

この構成では、NetScalerはConsoleサービスを介してライセンスサーバーエージェント (LSA) に到達できます。

注:

組み込みエージェントは、**インフラストラクチャ > インスタンス > エージェント > アクティベーションコードの生成**ページに移動して構成することもできます。URLとアクティベーションコードをNetScalerインスタンスにコピーして貼り付け、そのインスタンスを検出します。

組み込みエージェントが起動したら、**インフラストラクチャ > インスタンス > NetScaler**に移動します。このページには、組み込みエージェントを使用して検出された管理対象インスタンスの詳細が表示されます。

トラブルシューティング

登録が失敗した場合、または登録は成功したが組み込みエージェントがNetScaler Console GUIに表示されない場合は、ログを確認できます。

- 登録に失敗した場合は、`/var/mastools/logs/mastools_reg.py.log`でログを確認してください。
- 登録が成功しても、ビルトインエージェントがNetScaler Console GUIに表示されない場合は、以下を確認してください。
  - `/var/mastools/logs/mastools_upgrade.log`の**Mastools_upgrade**ログ
  - `/var/log/mastoolsd.log`の**バイナリログ**。

オンプレミスにNetScalerエージェントをインストールする

エージェントは、NetScaler Consoleと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。

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

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。詳細については、「エージェントのインストール要件」および「プールされたライセンス用の軽量エージェント」を参照してください。

注

ポートおよびその他の要件に関するすべての情報については、「サポートされているポート」を参照してください。

NetScalerエージェントをインストールするには:

1. はじめにで説明されているように、エージェントイメージをダウンロードします。
2. エージェント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。
3. **Console**タブから、次の例に示すように、初期ネットワーク構成オプションを設定します。

   注

   NetScalerエージェントへのインターネットアクセスを許可するようにDNSを設定していることを確認してください。

4. 初期ネットワーク構成が完了したら、構成設定を保存します。プロンプトが表示されたら、デフォルトの (`nsrecover/nsroot`) 資格情報を使用してログオンします。

   エージェントで設定済みのネットワーク設定を変更する場合は、`networkconfig`コマンドを入力し、CLIのプロンプトに従います。

5. サービスURLを入力するプロンプトが表示されない場合は、NetScalerエージェントで/mpsに移動し、次のいずれかのスクリプトを実行します。

   ```
   deployment_type.py
   ```

   ```
   register_agent_cloud.py
   ```

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

6. エージェントイメージをダウンロードしたときに保存した**サービスURL**と**アクティベーションコード**を入力します。エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。

7. エージェントの登録が成功すると、エージェントが再起動してインストールプロセスを完了します。

エージェントが再起動したら、NetScaler Console GUIにアクセスし、**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。エージェントが構成されたら、パスワードを変更する必要があります。

1. **インフラストラクチャ > インスタンス > エージェント**に移動します
2. エージェントを選択し、**アクションの選択**リストから**パスワードの変更**をクリックします。

3. 現在のパスワード (`nsroot`) を入力し、次に新しいパスワードを指定し、**OK**をクリックしてパスワードを変更します。

   パスワードは次の条件を満たす必要があります。

   - 6文字以上であること
   - 1つ以上の特殊文字を含むこと
   - 1つ以上の大文字を含むこと
   - 1つ以上の小文字を含むこと
   - 1つ以上の数字を含むこと

注:

NetScalerエージェントをオンプレミスで構成した後、NetScalerインスタンスにライセンスを適用する前に、最大10分間待つことをお勧めします。

Microsoft AzureクラウドにNetScalerエージェントをインストールする

エージェントは、NetScaler Consoleと、エンタープライズデータセンターまたはクラウド上の管理対象インスタンスとの間の仲介役として機能します。

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

Microsoft AzureクラウドにNetScalerエージェントをインストールするには、仮想ネットワークにエージェントのインスタンスを作成する必要があります。Azure MarketplaceからNetScalerエージェントイメージを取得し、Azure Resource Managerポータルを使用してエージェントを作成します。

NetScalerエージェントインスタンスの作成を開始する前に、インスタンスが配置される必要なサブネットを持つ仮想ネットワークを作成していることを確認してください。VMプロビジョニング中に仮想ネットワークを作成できますが、異なるサブネットを作成する柔軟性はありません。詳細については、*Azure documentation*を参照してください。

仮想マシンがインターネットリソースにアクセスできるように、DNSサーバーとVPN接続を構成します。

前提条件

以下があることを確認してください。

- Microsoft Azureユーザーアカウント
- Microsoft Azure Resource Managerへのアクセス

注

- NetScalerエージェント仮想マシンをプロビジョニングする前に、リソースグループ、ネットワークセキュリティグループ、仮想ネットワーク、およびその他のエンティティを作成して、プロビジョニング中にネットワーク情報が利用できるようにすることをお勧めします。
- NetScalerエージェントがNetScaler ConsoleおよびNetScalerインスタンスと通信できるように、推奨されるポートが開いていることを確認してください。NetScalerエージェントのポート要件に関する詳細については、ポートを参照してください。

Microsoft Azure CloudにNetScalerエージェントをインストールするには：

1. Microsoft Azureの資格情報を使用して、Azureポータル（https://portal.azure.com）にログオンします。
2. **+リソースの作成**をクリックします。
3. 検索バーに`NetScaler agent`と入力し、**NetScaler agent**を選択します。

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

Azure ネットワークペイン(/en-us/netscaler-console-service/media/adm-service-azure-agent-search.png)

4. **作成**をクリックします。

   リソースマネージャーの作成(/en-us/netscaler-console-service/media/ma-service-azureagent3.png)

5. **仮想マシンの作成**ペインで、仮想マシンを作成するために各セクションで必要な値を指定します。

   基本:

   このタブで、**プロジェクトの詳細**、**インスタンスの詳細**、および**管理者アカウント**を指定します。

   仮想マシンの作成(/en-us/netscaler-console-service/media/create-vm-basic.png)

   - **リソースグループ** – ドロップダウンリストから作成したリソースグループを選択します。

     注

     この時点でリソースグループを作成することもできますが、Azure Resource Manager の**リソースグループ**からリソースグループを作成し、ドロップダウンリストからそのグループを選択することをお勧めします。

   - **仮想マシン名** – NetScaler agent インスタンスの名前を指定します。
   - **リージョン** - エージェントをデプロイするリージョンを選択します。
   - **可用性オプション** – リストから可用性セットを選択します。
   - **イメージ** - このフィールドには、すでに選択されているエージェントイメージが表示されます。別のエージェントイメージに変更する場合は、リストから必要なイメージを選択します。
   - **サイズ** - NetScalerエージェントをデプロイするための仮想ディスクのタイプとサイズを指定します。

     サポートされている仮想ディスクタイプ（**HDD**または**SSD**）をリストから選択します。

     サポートされている仮想ディスクのサイズに関する詳細については、「エージェントのインストール要件」および「プールライセンス用の軽量エージェント」を参照してください。

   - **認証タイプ** – パスワードを選択します。

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

- **ユーザー名とパスワード** – 作成したリソースグループ内のリソー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。

  重要

  - エージェントには独自のユーザー名とパスワードを指定することをお勧めします。`nsrecover`または`nsroot`はエージェントユーザー用に予約されているため、ユーザー名として使用しないでください。
  - プロビジョニング中に、`nsroot`または`nsrecover`ではないユーザー名を設定します。ただし、プロビジョニング後の最初のログインでは、ユーザー名として`nsrecover`を使用する必要があります。

ディスク:

このタブで、「**ディスクオプション**」と「**データディスク**」を指定します。

- **OSディスクタイプ** - 仮想ディスクタイプ（HDDまたはSSD）を選択します。

ネットワーク:

必要なネットワークの詳細を指定します。

- **仮想ネットワーク** – 仮想ネットワークを選択します。
- **サブネット** – サブネットアドレスを設定します。
- **パブリックIPアドレス** - オプションで、IPアドレスを選択します。
- **ネットワークセキュリティグループ** – オプションで、作成したセキュリティグループを選択します。
- **受信ポートの選択** - パブリック受信ポートを許可する場合は、セキュリティグループで受信および送信ルールが構成されていることを確認してください。次に、リストから受信ポートを選択します。詳細については、「前提条件」を参照してください。

注

エージェントがインターネットにアクセスできることを確認してください。

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

管理:

Azure Security Center、**監視**、および**ID**を指定します。

詳細設定:

オプションで、**拡張機能**、**カスタムデータ**、および**近接配置グループ**を指定します。

注

カスタムデータで、はじめにで指示されているように、NetScaler Consoleの**エージェントのセットアップ**ページからコピーした**サービスURL**と**アクティベーションコード**を指定します。詳細を次の形式で入力します。

```
registeragent -serviceurl &lt;apigatewayurl> -activationcode
&lt;activationcodevalue>
```

エージェントはこの情報を使用して、起動時にNetScaler Consoleに自動登録します。
この自動登録スクリプトを指定する場合は、手順7と8をスキップしてください。

タグ:

NetScalerエージェントタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、エージェントを簡単に整理および識別できます。タグはAzureとNetScaler Consoleの両方に適用されます。

タグの指定(/en-us/netscaler-console-service/media/create-vm-tags.png)

構成設定が検証され、**確認と作成**タブに検証結果が表示されます。

- 検証に失敗した場合、このタブに失敗の理由が表示されます。該当するセクションに戻り、必要に応じて変更を加えてください。
- 検証に合格したら、**作成**をクリックします。エージェントの展開プロセスが開始されます。

  VMの概要(/en-us/netscaler-console-service/media/review-create-vm.png)

  展開プロセスには約10〜15分かかる場合があります。展開が正常に完了すると、Microsoft AzureアカウントでNetScalerエージェント仮想マシンを表示できます。

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

VMの展開(/en-us/netscaler-console-service/media/deploy-vm.png)

6. エージェントが起動して実行されたら、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ます。仮想マシンの作成時に指定したユーザー名とパスワードを使用します。
7. シェルプロンプトでコマンド「**deployment_type.py**」を入力して、展開スクリプトを実行します。
8. はじめにで指示されているように、NetScaler Consoleの**エージェントのセットアップ**ページからコピーして保存した**サービスURL**と**アクティベーションコード**を入力します。エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。

   エージェントの登録(/en-us/netscaler-console-service/media/adm-service-deployment.png)

エージェントの登録が成功すると、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 Consoleにアクセスし、**Set Up Agent**ページにある**Discovered Agents**の下で、エージェントのステータスを確認します。

Amazon Web Services (AWS) に NetScaler エージェントをインストールする

NetScaler エージェントは、NetScaler Console と、データセンターまたはクラウド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。

前提条件

Amazon GUI を使用して、Amazon Web Services (AWS) Virtual Private Cloud (VPC) 内で NetScaler エージェント AMI を起動するには、以下が必要です。

- AWS アカウント
- AWS 仮想プライベートクラウド (VPC)
- IAM アカウント
- エージェントが NetScaler Console サービスに接続するためのサービス URL とアクティベーションコード。NetScaler Console サービス GUI で、**Infrastructure > Instances > Agents** に移動し、**Generate Activation Code** をクリックして、サービス URL とアクティベーションコードを生成します。

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

注

- NetScaler エージェント仮想マシンをプロビジョニングする前に、Citrix はセキュリティグループ、仮想プライベートネットワーク、キーペア、サブネット、およびその他のエンティティを作成することをお勧めします。これにより、プロビジョニング中にネットワーク情報が利用可能になります。
- NetScaler エージェントが NetScaler Console および NetScaler インスタンスと通信できるように、推奨されるポートが開いていることを確認してください。NetScaler エージェントのポート要件の詳細については、「ポート」を参照してください。

AWS に NetScaler エージェントをインストールするには:

1. AWS 認証情報を使用して、AWS Marketplace にログオンします。
2. 検索フィールドに「**NetScaler agent**」と入力して NetScaler エージェント AMI を検索し、**Go** をクリックします。
3. 検索結果ページで、利用可能なリストから **NetScaler Console External agent AMI** をクリックします。
4. **NetScaler Console External Agent AMI**ページで、**Continue to Subscribe**をクリックします。

5. サブスクリプションが正常に完了したら、**Continue to Configuration**をクリックします。

6. **Configure this software**ページで、次の操作を行います。
   a. **Fulfillment option**リストからAMIを選択します。
   b. **Software Version**リストから最新のNetScalerエージェントバージョンを選択します。
   c. **Region**リストからお使いのリージョンを選択します。
   d. **Continue to Launch**をクリックします

7. **Launch this software**ページには、NetScalerエージェントを登録するための2つのオプションがあります。
   a. **Webサイトから起動**
   b. **EC2で起動**

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

Webサイトから起動

ウェブサイトから起動するには、以下を選択します。

1. **EC2インスタンスタイプ**リストからEC2インスタンスタイプ
2. **VPC設定**リストからVPC。ソフトウェア用のVPCを作成するには、**EC2でVPCを作成**をクリックします。
3. **サブネット設定**リストからサブネット。VPCを選択した後、サブネットを作成するには、**EC2でサブネットを作成**をクリックします。
4. **セキュリティグループ設定**リストからファイアウォール用のセキュリティグループ。セキュリティグループを作成するには、**販売者設定に基づいて新規作成**をクリックします。
5. **キーペア設定**リストからアクセスセキュリティを確保するためのキーペア。ソフトウェア用のキーペアを作成するには、**EC2でキーペアを作成**をクリックします。
6. **起動**をクリックします

7. ウェブサイトからの起動が成功しました。

   注

   デプロイプロセスには約10〜15分かかる場合があります。デプロイが正常に完了すると、AWSアカウントでNetScalerエージェント仮想マシンを表示できます。
8. エージェントがデプロイされたら、NetScalerエージェントに名前を割り当てます。
9. エージェントが稼働状態になったら、NetScalerエージェントにElastic IPアドレスを割り当てます。

   注

   Elastic IPアドレスは、NetScalerエージェントがNetScaler Consoleと通信できるようにします。ただし、NAT Gatewayを設定してインターネットにトラフィックをルーティングしている場合は、Elastic IPアドレスは必要ない場合があります。
10. 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ます。

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

注

NetScalerエージェントには、次のいずれかの方法でログオンできます。

- `nsrecover` をユーザー名として使用し、AWSインスタンスIDをパスワードとして使用します。
- `nsroot` をユーザー名として使用し、有効なキーペアをパスワードとして使用します。

11. 次のコマンドを入力して展開画面を呼び出します: **deployment_type.py**
12. Getting Started で指示されているように、NetScaler Consoleの **エージェントのセットアップ** ページからコピーして保存した **Service-URL** と **アクティベーションコード** を入力します。エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。

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

エージェントが再起動したら、NetScaler Consoleにアクセスし、**エージェントのセットアップ** ページの **検出されたエージェント** の下で、エージェントのステータスを確認します。

EC2で起動

EC2で起動するには、**アクションの選択** リストから **EC2経由で起動** を選択し、次に **起動** をクリックします。

1. **インスタンスタイプの選択** ページで、インスタンスを選択し、**次へ: インスタンスの詳細を設定** をクリックします。

2. 「**インスタンスの詳細設定**」ページで、必要なパラメータを指定します。

   「**高度な詳細**」セクションで、「**ユーザーデータ**」フィールドに認証の詳細またはスクリプトを指定することで、ゼロタッチエージェントを有効にできます。

   - **認証の詳細** - Getting Startedで指示されているように、NetScaler Consoleの「**エージェントのセットアップ**」ページからコピーした「**サービスURL**」と「**アクティベーションコード**」を指定します。詳細を次の形式で入力します。

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

```
registeragent -serviceurl <apigatewayurl> -activationcode
<activationcodevalue>
```

エージェントは、この情報を使用して起動時にNetScaler Consoleに自動登録します。

- **スクリプト** - エージェントの自動登録スクリプトをユーザーデータとして指定します。以下はスクリプトの例です。

```
#!/var/python/bin/python2.7

import os

import requests

import json

import time

import re

import logging

import logging.handlers

import boto3



'''

Overview of the Script:

The script helps to register a NetScaler agent with NetScaler
Console. Pass it in userdata to make NetScaler agent in AWS to
autoregister on bootup. The workflow is as follows

1)  Fetch the NetScaler Console API credentials (ID and secret) from
AWS secret store (NOTE: you have to assign IAM role to the NetScaler
agent that will give permission to fetch secrets from AWS secret
store)

2)  Login to NetScaler Console with credentials fetched in step 1
```

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

```
3)  Call NetScaler Console to fetch credentials (serviceURL and
token) for agent registration

4)  Calls registration by using the credentials fetched in step 3

'''



'''

These are the placeholders which you need to replace according to
your setup configurations

aws_secret_id: Id of the AWS secret where you have stored NetScaler
Console Credentials

The secrets value should be in the following json format

{ "adm_user_id_key": "YOUR_ID", " adm_user_secret_key":
"YOUR_SECRET"}

'''



aws_secret_id = "<AWS_secret_id>"

adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"



'''

Set up a specific logger with your desired output level and log file
name

'''

log_file_name_local = os.path.basename(__file__)

LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
```

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

```
LOG_MAX_BYTE = 50*1024*1024

LOG_BACKUP_COUNT = 20



logger = logging.getLogger(__name__)

logger.setLevel(logging.DEBUG)

logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME,
maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)

logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%
(funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
datefmt="%Y-%m-%d %H:%M:%S")

logger_handler.setFormatter(logger_fortmater)

logger.addHandler(logger_handler)



class APIHandlerException(Exception):

    def __init__(self, error_code, message):

        self.error_code = error_code

        self.message = message



    def __str__(self):

        return self.message + ". Error code '" +
str(self.error_code) + "'"



def parse_response(response, url, print_response=True):

    if not response.ok:
```

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

```
        if "reboot" in url:

            logger.debug('No response for url: reboot')

            resp = {"errorcode": "500", "message": "Error while
reading response."}

            return resp



        if print_response:

            logger.debug('Response text for %s is %s' % (url,
response.text))



        response = json.loads(response.text)

        logger.debug("ErrorCode - " + str(response['errorcode']) +
". Message -" + str(response['message']))

        raise APIHandlerException(response['errorcode'],
str(response['message']))

    elif response.text:

        if print_response:

            logger.debug('Response text for %s is %s' % (url,
response.text))



        result = json.loads(response.text)

        if 'errorcode' in result and result['errorcode'] > 0:

            raise APIHandlerException(result['errorcode'],
str(result['message']))

        return result
```

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

```
def _request(method, url, data=None, headers=None, retry=3,
print_response=True):

    try:

        response = requests.request(method, url, data=data,
headers=headers)

        result = parse_response(response, url,
print_response=print_response)

        return result

    except [requests.exceptions.ConnectionError,
requests.exceptions.ConnectTimeout]:

        if retry > 0:

            return _request(method, url, data, headers, retry-1,
print_response=print_response)

        else:

            raise APIHandlerException(503, 'ConnectionError')

    except requests.exceptions.RequestException as e:

        logger.debug(str(e))

        raise APIHandlerException(500, str(e))

    except APIHandlerException as e:

        logger.debug("URL: %s, Error: %s, Message: %s" % (url,
e.error_code, e.message))

        raise e

    except Exception as e:

        raise APIHandlerException(500, str(e))
```

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

```
try:
    '''Get the AWS Region'''
    client = boto3.client('s3')
    my_region = client.meta.region_name
    logger.debug("The rgion is %s" % (my_region))

    '''Creating a Boto cleint session'''
    session = boto3.session.Session()
    client = session.client(
        service_name='secretsmanager',
        region_name=my_region
    )

    '''Getting the values stored in the secret with id:
<aws_secret_id>'''
    get_id_value_response = client.get_secret_value(
        SecretId = aws_secret_id
    )
    adm_user_id = json.loads(get_id_value_response["SecretString"])
["adm_user_id_key"]
    adm_user_secret =
json.loads(get_id_value_response["SecretString"])
["adm_user_secret_key"]
```

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

```
except Exception as e:

    logger.debug("Fetching of NetScaler Console credentials from AWS
secret failed with error: %s" % (str(e)))

    raise e



'''

Initializing common NetScaler Console API handlers

'''

mas_common_headers = {

    'Content-Type': "application/json",

    'Accept-type': "application/json",

    'Connection': "keep-alive",

    'isCloud': "true"

}



'''

API to login to the NetScaler Console and fetch the Session ID and
Tenant ID

'''

url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
login"

payload = 'object={"login":{"ID":"' + adm_user_id + '","Secret":"' +
adm_user_secret + '"}}'
```

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

```
try:

    response = _request("POST", url, data=payload,
headers=mas_common_headers)

    sessionid = response["login"][0]["sessionid"]

    tenant_id = response["login"][0]["tenant_name"]

except Exception as e:

    logger.debug("Login call to the NetScaler Console failed with
error: %s" % (str(e)))

    raise e



'''

API to fetch the service URL and Token to be used for registering
the agent with the NetScaler Console

'''

mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)

url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id

logger.debug("Fetching Service URL and Token.")

try:

    response = _request("GET", url, data=None,
headers=mas_common_headers)

    service_name  = response["trust_preauthtoken"][0]
["service_name"]

    token = response["trust_preauthtoken"][0]["token"]

    api_gateway_url = response["trust_preauthtoken"][0]
```

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

```
["api_gateway_url"]

except Exception as e:

    logger.debug("Fetching of the Service URL Passed with error. %s"
% (str(e)))

    raise e



'''

Running the register agent command using the values we retrieved
earlier

'''

try:

    registeragent_command = "registeragent -serviceurl
"+api_gateway_url+" -activationcode "+service_name+"\;"+token

    file_run_command = "/var/python/bin/python2.7 /mps/
register_agent_cloud.py "+registeragent_command

    logger.debug("Executing registeragent command: %s" %
(file_run_command))

    os.system(file_run_command)

except Exception as e:

    logger.debug("Agent Registeration failed with error: %s" %
(str(e)))

        raise e
```

このスクリプトは、AWS Secrets Managerから認証の詳細を取得し、`deployment.py`スクリプトを実行してエージェントをNetScaler Consoleに登録します。

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

> **注**
>
> パブリックIPアドレスを自動割り当てできますが、Elastic IPアドレスを割り当てることもできます。NAT Gatewayが設定されていない場合は、Elastic IPアドレスの割り当てが必要です。

このステップでElastic IPアドレスが設定されていない場合でも、EC2コンソールで設定できます。新しいElastic IPアドレスを作成し、インスタンスIDまたはENI-IDを使用してNetScalerエージェントに関連付けることができます。
「**ストレージの追加**」をクリックします。

3. 「**ストレージの追加**」ページで、インスタンスのストレージデバイス設定を構成し、「**次へ: タグの追加**」をクリックします。

4. 「**タグの追加**」ページで、インスタンスのタグを定義し、「**次へ: セキュリティグループの設定**」をクリックします。

5. 「**セキュリティグループの設定**」ページで、インスタンスへの特定のトラフィックを許可するルールを追加し、「**確認と起動**」をクリックします。

   確認と起動(/en-us/netscaler-console-service/media/agent-aws-7.jpg)

6. 「**インスタンス起動の確認**」ページで、インスタンス設定を確認し、「**起動**」をクリックします。
7. 「**既存のキーペアを選択するか、新しいキーペアを作成する**」ダイアログボックスで、キーペアを作成します。既存のキーペアから選択することもできます。

   承認に同意し、「**インスタンスの起動**」をクリックします。

   インスタンスの起動(/en-us/netscaler-console-service/media/agent-aws-8.jpg)

デプロイプロセスには約10〜15分かかる場合があります。デプロイが正常に完了すると、AWSアカウントでNetScalerエージェント仮想マシンを表示できます。

GCPにNetScalerエージェントをインストールする

NetScalerエージェントは、NetScaler Consoleと、データセンターまたはクラウド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。Google Cloud Platform (GCP) にエージェントを展開して、NetScaler Consoleを介したGoogleクラウド仮想ネットワーク内に展開されたNetScaler

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

インスタンスの安全なリモート管理を容易にすることができます。詳細については、Google Cloud Platform Marketplaceを参照してください。

前提条件

GCPにNetScalerエージェントをインストールするには、GCPアカウントが必要です。

GCPにNetScalerエージェントをインストールする

GCPにNetScalerエージェントをインストールするには、次の手順に従います。

1. 資格情報を使用してGCPコンソール (console.cloud.google.com) にログオンし、マーケットプレイスに移動します。
2. 検索フィールドに「**NetScaler agent**」と入力します。
3. 結果フィールドから**NetScaler agent**をクリックし、次に**Launch**をクリックします。

4. **新しいNetScalerエージェントの展開**ページでは、ほとんどのオプションがデフォルトで設定されています。必要に応じてデフォルト設定を変更し、**Deploy**をクリックします。

5. エージェントが展開されたら、インスタンスリンクをクリックし、**VMインスタンスの詳細ページ**で詳細を確認します。

6. エージェントの外部IPアドレスを使用してSSHクライアントを介してエージェントにログオンします。次のコマンドを使用します。

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

   パスワード: インスタンスID

   VMインスタンスの詳細ページで、外部IPアドレスとインスタンスIDを確認できます。

7. 展開画面を呼び出すには、次のコマンドを入力します: **deployment_type.py**
8. 開始するで指示されているように、NetScaler Consoleの**エージェントのセットアップ**ページからコピーして保存した**サービスURL**と**アクティベーションコード**を入力します。エージェントは、サービスを見つけるためにサービスURLを使用し、サービスに登録するためにアクティベーションコードを使用します。

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

エージェントの登録が成功すると、エージェントはインストールプロセスを完了するために再起動します。

エージェントが再起動した後、NetScaler Consoleにアクセスし、**エージェントのセットアップ**ページの**検出されたエージェント**の下で、エージェントのステータスを確認します。

YAMLを使用してKubernetesクラスターにNetScalerエージェントをインストールする

注

マイクロサービスとしてエージェントをインストールする手順は、入門セクションで利用できます。

Kubernetesマスターノードで:

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 Console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。

注:

YAMLを使用してKubernetesクラスターで構成されたNetScalerエージェントは、自動エージェントアップグレード（常時最新アップグレード）をサポートします。

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

OpenShiftコンソールを使用してNetScalerエージェントオペレーターをインストールする

注:

OpenShiftエージェントは、NetScaler Consoleサービスでのみサポートされています。

オペレーターは、Kubernetesアプリケーションを効果的、自動的、かつスケーラブルな方法でデプロイおよび管理できるオープンソースツールキットです。管理者として、**NetScaler® ADM Agent Operator**を使用してOpenShiftクラスターにエージェントをデプロイできます。

注:

OpenShiftクラスターで構成されたエージェントは、デフォルトでは自動的にアップグレードされません。

前提条件

デプロイする前に、以下を確認してください。

- ポッドの権限を制御するための特権セキュリティコンテキスト制約があることを確認してください。エージェントの場合、サービスアカウントに特権セキュリティコンテキスト制約を取得するには、次のコマンドを実行します。

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- エージェントログインシークレットを作成するには、次のコマンドを実行します。

  ```
  kubectl create secret generic admlogin --from-literal=username=nsroot --from-literal=password=<adm-agent-password> -n <namespace>
  ```

  注:

  - `<adm-agent-password>` はパスワードの例です。エージェントのパスワードを設定する必要があり、NetScaler CPX はこれらの資格情報を使用してエージェントに登録します。
  - インスタンスの作成時に、エージェントYAMLの `loginSecret` に **admlogin** を指定します。

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

NetScaler CPX™とエージェントを異なる名前空間にデプロイする場合は、以下を確認してください。

- NetScaler CPXがデプロイされている名前空間に`citrix-cpx=enabled`でラベルを付けます。
- エージェントオペレーターをインストールする際に、`helper.required`をtrueまたはfalseに設定します。

  注:

  デフォルトでは、`helper.required`は**false**に設定されています。このパラメーターがfalseに設定されている場合、NetScaler CPXとエージェントが異なる名前空間にある場合は、すべての名前空間に**admlogin**シークレットを作成する必要があります。

- エージェントのYAMLで必要となる`accessSecret`があります。これらの資格情報は、エージェントがNetScaler Consoleサービスに接続するために必要です。

```
kubectl create secret generic <secretname> --from-literal=accessid=<ID> --from-literal=accesssecret=<Secret> -n namespace
```

注:

インスタンス作成時に、エージェントYAMLのaccessSecretにシークレット名を入力します。

NetScaler Consoleにアクセスするためのアクセスidとシークレットは、以下の手順で取得できます。

a. Citrix Cloud™管理コンソールにログオンします。

b. Citrix Cloudメニューから、**Identity and Access Management**を選択します。

c. **API Access**タブから、安全なクライアント名を入力し、**Create Client**をクリックします。

d. IDとシークレットが生成されます。**ダウンロード**をクリックして、CSVファイルを保存します。

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

エージェントオペレーターをインストールする

1. OpenShiftクラスターコンソールにログオンします。
2. **オペレーター > OperatorHub**に移動します。
3. 検索バーにエージェント名を入力し、**NetScaler ADM Agent Operator**を選択して、**インストール**をクリックします。

4. **オペレーターのインストール**ページには、2つのオプションがあります。

   - **クラスター上のすべての名前空間 (デフォルト)** - エージェントオペレーターがクラスターで利用可能なすべての名前空間をサブスクライブできるようにし、クラスター上の任意の名前空間からエージェントオペレーターのインスタンスを起動できるようにします。
   - **クラスター上の特定の名前空間** - エージェントオペレーターがクラスター上の選択された名前空間をサブスクライブできるようにし、選択された名前空間からのみエージェントオペレーターのインスタンスを起動できるようにします。

     この例では、エージェントオペレーターは**Default**という名前空間に割り当てられています。**更新承認**の下で**自動**を選択し、**インストール**をクリックします。

     エージェントオペレーターが正常にサブスクライブされるまで待ちます。

5. **ワークロード > Pods** に移動し、`netscaler-adm-agent-operator-controller` Pod が起動して 稼働中であることを確認します。
6. Pod が起動して実行されたら、**インスタンスの作成** をクリックします。

7. パラメータを更新するには、**YAML ビュー** を選択し、**作成** をクリックします。

   注:

   OpenShift クラスターごとにエージェントのインスタンスは 1 つのみであることを確認してください。

8. **ワークロード > Pod** に移動し、エージェント Pod が起動して実行されていることを確認します。

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

エージェントインスタンスを削除する

クラスターからエージェントのインスタンスを削除するには、**オペレーター > インストール済みオペレーター** に移動します。**NetScaler ADM Agent Operator** タブでインスタンスを選択し、リストから **AdmAgent の削除** を選択します。

エージェントオペレーターをアンインストールする

クラスターからエージェントオペレーター Pod をアンインストールする場合は、**オペレーター > インストール済みオペレーター** に移動し、リストから **オペレーターのアンインストール** を選択します。

Helmチャートを使用してコンテナベースのエージェントをインストールする

NetScaler CPXをNetScaler Consoleに接続して管理および監視するために、コンテナベースのエージェントを展開できます。コンテナベースのエージェントを展開するには、このドキュメントに記載されている手順に従ってください。

注:

コンテナベースのエージェントは、デフォルトでは自動的にアップグレードされません (常時アップグレード)。

ヘルプとサポートの利用方法

Citrix Cloud™ユーザーとして、インフラストラクチャが円滑に機能していることを確認するために、ヘルプが必要になる場合があります。このトピックでは、さまざまなヘルプとサポートのオプション、およびそれらにアクセスする方法について詳しく説明します。

Citrix Cloudアカウントの作成

Citrix Cloudアカウントのサインアップ時にエラーが発生した場合は、Citrixカスタマーサービスにお問い合わせください。

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

アカウントにサインインする

Citrix Cloudアカウントへのサインインで問題が発生した場合は、次の点を確認してください。

- アカウント登録時に提供したメールアドレスとパスワードでサインインしていることを確認してください。
- 次の場合、Citrix Cloudはサインインする前にパスワードのリセットを自動的に促します。
  - しばらくCitrix Cloudにサインインしていない場合
  - パスワードがCitrix Cloudの要件を満たしていない場合
- 詳細については、この記事のパスワードの変更を参照してください。
- 会社がCitrixアカウントの代わりに会社の資格情報を使用してCitrix Cloudにサインインすることを許可している場合は、 をクリックし、会社のサインインURLを入力します。その後、会社の資格情報を入力して、会社のCitrix Cloudアカウントにアクセスできます。会社のサインインURLがわからない場合は、会社の管理者に問い合わせてサポートを受けてください。

パスワードの変更

Citrix Cloudアカウントのパスワードを忘れた場合は、 をクリックし、アカウントのメールアドレスを入力します。パスワードをリセットするためのメールが届きます。パスワードリセットメールが届かない場合、またはさらにサポートが必要な場合は、Citrixカスタマーサービスにお問い合わせください。

アカウントのパスワードを安全に保つために、Citrix Cloud はサインインしようとしたときにパスワードのリセットを求める場合があります。このプロンプトは次の場合に表示されます。

- パスワードが Citrix Cloud の複雑さの要件を満たしていません。パスワードは 8 文字以上で、以下を含む必要があります。
  - 少なくとも 1 つの数字
  - 少なくとも 1 つの大文字
  - 少なくとも 1 つの記号: `! @ # $ % \^ * ? + = -`
- パスワードに辞書に載っている単語が含まれています。
- パスワードが、侵害されたパスワードの既知のデータベースにリストされています。
- 過去 6 か月間 Citrix Cloud にサインインしていません。

プロンプトが表示されたら、**パスワードのリセット**を選択して、アカウントの新しい強力なパスワードを作成します。

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

Citrix Cloud サポートフォーラム

Citrix Cloud サポートフォーラム では、ヘルプの入手、フィードバックや改善提案の提供、他のユーザーとの会話の閲覧、または独自のトピックの開始ができます。

NetScaler® のサポートスタッフはこれらのフォーラムを追跡しており、お客様の質問に答える準備ができています。他の Citrix Cloud コミュニティメンバーもヘルプを提供したり、ディスカッションに参加したりする場合があります。

フォーラムのトピックを読むためにログインする必要はありません。ただし、トピックを投稿したり返信したりするにはログインする必要があります。ログインするには、既存の Citrix アカウントの資格情報を使用するか、Citrix Cloud アカウントを作成したときに提供したメールアドレスとパスワードを使用します。Citrix アカウントを作成するには、アカウントの作成またはリクエストにアクセスしてください。

サポート記事とドキュメント

NetScaler は、Citrix Cloud を最大限に活用し、NetScaler 製品で発生する可能性のある多くの問題を解決するのに役立つ、豊富な製品およびサポートコンテンツを提供しています。

Citrix Cloudリソースセンター

Citrix Cloudリソースセンターは、Citrix Cloudサービスの利用開始、機能の詳細学習、問題解決に役立ついくつかのリソースを提供します。表示されるリソースは、現在作業しているCitrix Cloudの機能またはサービスに適用されます。たとえば、Virtual Apps and Desktopsサービス管理コンソールを使用している場合、リソースセンターには次のリソースが表示されます。

Citrix Cloudコンソールの右下にある青いコンパスアイコンをクリックすると、いつでもリソースセンターにアクセスできます。

- **開始する**: 現在作業しているサービスに特化した主要タスクの簡単なガイド付きウォークスルーを提供します。また、サービスの機能について詳しく学び、エンドユーザーが成功できるようにするためのトレーニングおよびオンボーディングリソースへのリンクも提供されます。
- **お知らせ**: 新しくリリースされた機能の通知と、重要なCitrixコミュニケーションへのリンクを提供します。機能通知をクリックすると、その機能の簡単なガイド付きウォークスルーが表示されます。
- **記事を検索**: 一般的なタスクに関する製品ドキュメントとナレッジセンターの記事のリストを提供し、Citrix Cloudを離れることなく、より多くの記事を見つけるのに役立ちます。作業中のサービスに基づいて記事を絞り込んだリストを表示するには、**How do I...** ボックスに検索ク

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

エリを入力します。通常、サポート記事がリストの最初に表示され、その後に製品ドキュメント記事が続きます。

シトリックス テックゾーン

Citrix Tech Zoneには、Citrix Cloudおよびその他のNetScaler製品について詳しく学ぶのに役立つ豊富な情報が含まれています。ここでは、Citrixテクノロジーの設計、構築、展開に関する洞察を提供するリファレンスアーキテクチャ、図、ビデオ、技術文書を見つけることができます。

テクニカルサポート

技術的なヘルプが必要な問題が発生した場合は、画面の右上にある**Feedback and Support**アイコンをクリックし、**Open a Ticket**を選択します。

Go to My Supportをクリックし、次に**My Support**をクリックして、My Supportポータルからチケットを開きます。My Supportポータルを使用して、既存のチケットを追跡したり、現在の製品エンタイトルメントを表示したりすることもできます。

サービス稼働状況ダッシュボード

Citrix Cloudサービス稼働状況ダッシュボードは、各地域におけるCitrix Cloudプラットフォームとサービスのリアルタイムの可用性の概要を提供します。Citrix Cloudで問題が発生した場合は、サービス稼働状況ダッシュボードを確認して、Citrix Cloudまたは特定のサービスが正常に動作していることを確認してください。

サービス稼働状況ダッシュボード(/en-us/netscaler-console-service/media/service-health-dashboard.png)

ダッシュボードを使用して、次の条件について詳しく確認できます。

- 地理的地域別にグループ化された、すべてのCitrix Cloudサービスの現在の可用性ステータス
- 過去7日間（デフォルト）またはそれ以前の7日間ごとの各サービスのサービス稼働状況履歴
- 特定のサービスのメンテナンス期間

デフォルトでは、サービス稼働状況はリストとして表示されますが、カレンダービューで表示することもできます。**次へ**または**前へ**を選択して、7日間ごとのサービス稼働状況履歴をスクロールします。影響を受けるサービスのみを表示するようにリストをフィルタリングすることもできます。

サービス履歴ビュー(/en-us/netscaler-console-service/media/service-health-history-view.png)

影響を受けるサービスのサービス稼働状況インシデントに関する詳細情報を表示するには：

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

- リストビューから、サービスインジケーターの横にあるアイコンをクリックして、サービス稼働状況インシデントに関する詳細情報を表示します。
- カレンダービューから、サービスエントリをクリックして、サービス稼働状況インシデントのステータスを表示します。

サービス稼働状況のサブスクリプション

サービス稼働状況の通知を受け取るには、ダッシュボードの右上にある**購読**をクリックし、使用したい通知方法を選択します。

購読リンクが強調表示されたサービス稼働状況ダッシュボード(/en-us/netscaler-console-service/media/service-health-subscribe-link.png)

すべてのサービスの通知を購読することも、選択したサービスのみの通知を購読することもできます。デフォルトでは、サービス稼働状況インシデントに関するすべての通知を受け取ります。インシデント中の通知の頻度を制限するには、最初と最後の通知のみを受け取るように選択できます。

サービス稼働状況の購読オプション(/en-us/netscaler-console-service/media/service-health-subscribe-customizations.png)

購読方法に応じて、購読確認メッセージ（電話通知を購読する場合など）または各通知メッセージ（メール通知を購読する場合など）に、購読解除および設定変更のリンクが含まれています。

電話によるサービスヘルス購読確認(/en-us/netscaler-console-service/media/service-health-subscribe-confirm-phone.jpg)

購読オプションが強調表示されたサービスヘルス通知メール(/en-us/netscaler-console-service/media/service-health-subscribe-edit-email.png)

購読を解除するか、購読設定を変更するには：

1. 既存の通知を見つけ、購読解除または通知設定変更のリンクを選択します。
2. 購読を解除する場合は、**Unsubscribe** を選択し、キャンセルしたい通知方法を選択します。すべての通知方法から購読解除するには、**Remove all subscriptions** を選択します。
3. 設定を変更する場合は、通知方法を選択し、サービスと最小インシデント通知に適切な変更を加え、**Save** を選択します。

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

強化されたグラフィカルユーザーインターフェース

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

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

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

ホバーで表示されるメニュー

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

サブメニューのホバー表示(/en-us/netscaler-console-service/media/hover-and-display-submenu.png)

効率化されたメニュー階層

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

- **インフラストラクチャ > 構成**

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

- **NetScaler® ライセンス > プールライセンス**
- **ゲートウェイ > HDX™ Insight**

更新されたサブメニューラベル

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

インフラストラクチャ > 構成

構成ノードの変更(/en-us/netscaler-console-service/media/configuration-node-changes.png)

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

NetScalerライセンス > プールライセンス

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

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

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

ゲートウェイ > HDX Insight

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

設定

設定の下には、サブメニューのラベルまたは名前の変更以外に、他の変更はありません。

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

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

折りたたみ可能なメニュー

アイコンをクリックして、メニュー全体を折りたたんだり展開したりできます。

展開されたメニュー

ペインのアイコン「**>>**」をクリックして、メニュー全体を展開します。

折りたたまれたメニュー

ペインの「**Collapse <<**」をクリックして、メニュー全体を折りたたみます。

サイドバーの切り替え

サイドバーの表示/非表示を切り替えることで、画面スペースを最適化できます。パンくずリストの切り替えボタンをクリックして、サイドバーを非表示または表示します。

サイドバーを表示

サイドバーを非表示にする

このオプションは、サイドバーを非表示にすることで画面スペースを最適化します。

ホーム画面として設定

NetScaler Console GUIには、ページとして表示されるサブメニュー名の横にアイコンがあります。ホーム画面アイコンを使用すると、ランディングページを設定できます。このアイコンは、その特定のページにいる場合にのみ表示されます。ページをホーム画面から削除するには、アイコンをもう一度クリックするだけです。

お気に入りの項目をピン留めする

ピン留め機能を使用すると、お気に入りの項目にすばやくアクセスできます。メニューまたはサブメニューをピン留めするには、その上にカーソルを合わせ、名前の横に表示されるピンアイコンをクリックします。

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

ピン留めされたメニューはサイドバーの**PINNED**の下に表示され、簡単にアクセスできます。

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

Console Advisory 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

ハイブリッドマルチクラウド (HMC) インフラストラクチャが成長するにつれて、NetScaler インスタンスの管理、監視、分析、トラブルシューティングの課題は多岐にわたります。完全なインフラストラクチャとそこで実行されているすべてのアプリケーションを可視化する一元化されたコントローラが、今必要とされています。

今日の状況では、インスタンスを中央コントローラにオンボーディングすることは、迅速、簡単、かつロータッチな方法で行う必要があります。このニーズを念頭に置いて、NetScaler Console は新しいオンボーディングワークフローを開始し、HMC 展開を完全に可視化するためのより迅速な方法を提供します。

概要: NetScaler Console オンボーディングワークフローのコンポーネント

このワークフローの構成要素は、NetScaler サービス接続と Call Home という 2 つの ADC 側コンポーネントです。

- **Console Advisory Connect**: NetScaler の新機能で、NetScaler インスタンスを NetScaler Console にシームレスにオンボーディングするのに役立ちます。この機能により、NetScaler インスタンスは NetScaler Console に自動的に接続し、システム、使用状況、テレメトリデータを NetScaler Console に送信できます。このデータに基づいて、NetScaler Console は NetScaler インフラストラクチャに関する洞察と推奨事項を提供します。これには、パフォーマンスの問題、高いリソース使用率、および重大なエラーの迅速な特定などが含まれます。

  Console Advisory Connect は、以下の NetScaler バージョンで利用できます。

  - NetScaler MPX および VPX イメージバージョン 12.1 57.18 以降、および 13.0 61.48 以降。詳細については、「NetScaler アプライアンス向け NetScaler Console 接続の概要」を参照してください。
  - NetScaler SDX バージョンイメージ 12.1 58.14 以降、および 13.0 61.48 以降。詳細については、「NetScaler SDX アプライアンス向け NetScaler Console 接続の概要」を参照してください。

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

- **Call Home**: ADC の既存機能で、インスタンスを定期的に監視し、データを Citrix テクニカルサポートサーバーに自動的にアップロードします。詳細については、「Call Home」を参照してください。Call Home によって収集されたデータは、この新しいワークフローを有効にするために NetScaler Console にもルーティングされます。

インターネット接続または Call Home を持つすべての NetScaler インスタンス、または NetScaler Console 接続が有効になっているインスタンスは、NetScaler Console に接続されます。NetScaler Console は、Call Home ルート、NetScaler Console 接続ルート、またはその両方を通じて、これらの NetScaler インスタンスから関連するメトリックの収集を開始します。詳細については、「MPX および VPX インスタンスのデータガバナンス」および「SDX インスタンスのデータガバナンス」を参照してください。

このデータを使用して、NetScaler Console は顧客ごと (一意の組織 ID) に NetScaler インスタンスのインベントリを作成し、NetScaler インスタンスの統合リストを表示します。NetScaler Console はこのデータを使用して、NetScaler および Gateway インスタンスに関する洞察も作成します。これにより、HMC 展開に関する意味のある洞察が得られ、問題が特定され、問題を軽減するためのアクションが推奨されます。問題を軽減する前に、NetScaler インスタンスを NetScaler Console にオンボーディングする必要があります。

オンボーディングする NetScaler および Gateway インスタンスを選択 をチェックし、NetScaler Console にオンボーディングする NetScaler インスタンスを選択できます。開始すると、オンボーディングプロセスに誘導されます。

自動オンボーディングプロセスでは Console Advisory Connect を使用するため、エクスペリエンスが自動化され、シームレスで高速になります。Console Advisory Connect と自動オンボーディングをサポートしないバージョンの NetScaler インスタンスの場合、NetScaler Console はスクリプトベースのオンボーディングを提供します。これは半自動化されたプロセスです。

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

注

- 自動およびスクリプトベースのオンボーディングでは組み込みエージェントを使用します。ただし、このワークフローでは、オンボーディングに外部エージェントを使用する柔軟性も提供されます。NetScaler Consoleでプールライセンスまたは完全なアナリティクススイートを使用したい場合は、外部エージェントベースのオンボーディングを使用できます。あるいは、プールライセンスと完全なアナリティクススイートの両方を使用したい場合も同様です。組み込みエージェントは管理と監視のみをサポートします。
- Console Advisory Connectによって収集されたメトリックは、NetScaler Consoleサービスエンドポイントに直接送信されます。NetScalerがNetScaler Console上の管理/検出されたNetScalerであり、そのADCに外部エージェントが構成されている場合でも、メトリックはNetScalerからNetScaler Consoleサービスエンドポイントに直接送信され、外部エージェントを経由してルーティングされることはありません。

オンボーディングのクイックツアー

オンボーディングの最初の接点は、製品から送信されるメールです。オンボーディングの概要を以下に示します。

1. A **NetScaler製品から送信されるメール**：NetScaler Consoleから、NetScalerインフラストラクチャの主要なインサイトを示すメールが届き、NetScaler Consoleの使用開始を促されます。メール内の**ADMサービスにオンボード**をクリックします。**Citrix Cloud**ページが表示されます。
2. In the **Citrix Cloud™**ログインページで：
   - 既存のCitrix Cloudのお客様の場合は、**Citrix.com**、**My Citrix**、または**Citrix Cloud**の資格情報を使用してCitrix Cloudにサインインします。
   - 既存のCitrix Cloudのお客様でない場合は、Citrix Cloudにサインアップしてください。詳細については、「Citrix Cloudへのサインアップ」を参照してください。

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

注

- 複数の組織IDに属しており、そのうちの1つの組織IDがCitrix Cloudにある場合は、既存の資格情報を使用してサインインします。その後、新しい組織IDのオンボーディングワークフローを完了します。
- Console Advisory Connectベースのロータッチオンボーディングワークフローの一部として受信するメール通知を有効または無効にできます。詳細については、「メール設定」を参照してください。

3. **NetScaler Consoleウェルカムページ**：NetScaler Consoleとその利点の概要が表示されます。
4. **NetScalerおよびGatewayインスタンスに関するインサイト**：セキュリティアドバイザリ（現在のNetScaler CVEに関するアドバイス）、アップグレードアドバイザリ（EOM/EOLタイムラインに基づくアドバイス）、主要なメトリック、トレンドなど、NetScalerインフラストラクチャ全体の詳細なインサイトが得られます。また、NetScalerのパフォーマンスと健全性に影響を与える問題を強調し、その問題を軽減する方法を推奨します。
5. **オンボードするNetScalerおよびGatewayインスタンスを選択**：NetScalerインベントリの統合ビューが表示されます。NetScaler ConsoleにオンボードするNetScalerインスタンスを選択できます。
6. **NetScalerインスタンスをNetScaler Consoleにオンボード**：オンボーディング用に選択されたNetScalerインスタンスに基づいて、NetScaler Consoleがオンボーディングプロセスをガイドします。デフォルトでは、自動オンボーディング用に組み込みエージェントが選択されています。
7. **NetScaler Console GUIダッシュボード**：オンボーディングが完了すると、NetScaler Consoleインスタンスのダッシュボードに誘導されます。

これらのオンボーディング方法の詳細については、「NetScaler Console Connectを使用したNetScalerインスタンスのオンボーディング」を参照してください。

Console Advisory Connect を使用して NetScaler インスタンスをオンボードする

このドキュメントでは、NetScaler Console の使用を開始するのに役立つ段階的なガイドを提供します。開始する前に、NetScaler Console が新しいオンボーディングワークフローをどのように開始するかをお読みください。これにより、ハイブリッドマルチクラウド (HMC) 展開の完全な可視性をより迅速に得ることができます。「NetScaler インスタンスの NetScaler Console connect を使用したロータッチオンボーディング」を参照してください。

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

ステップ 1: 開始する

NetScaler Console から、NetScaler インフラストラクチャの主要なインサイトを示し、NetScaler Console の使用を開始するよう招待するメールが届きます。

オンボーディングメール(/en-us/netscaler-console-service/media/onboarding-email.png)

1. メールで、 をクリックします。**Citrix Cloud™** ページが表示されます。
2. **Citrix Cloud** ログインページで:
   - 既存の Citrix Cloud のお客様である場合は、**Citrix.com**、**My Citrix**、または **Citrix Cloud** の資格情報を使用して Citrix Cloud にサインインします。
   - 既存の Citrix Cloud のお客様でない場合は、Citrix Cloud にサインアップします。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。

   注

   - 複数の Org ID に属しており、そのうちの 1 つの Org ID が Citrix Cloud にある場合は、既存の資格情報を使用してサインインします。その後、新しい Org ID のオンボーディングワークフローを完了します。
   - Consolve Advisory Connect ベースのロータッチオンボーディングワークフローの一部として受信するメール通知を有効または無効にできます。詳細については、「メール設定」を参照してください。
3. NetScaler Console のランディングページで、なぜそこにいるのか、そして NetScaler Console を使用する利点を読んでください。

   アセットインサイトの表示(/en-us/netscaler-console-service/media/view-asset-insights.png)

注

メール内のセキュリティアドバイザリのインサイトは、NetScalerビルドバージョンスキャンのみに基づいています。NetScalerインスタンスをNetScaler Consoleにオンボーディングすると、より決定的で網羅的なセキュリティアドバイザリのインサイトを確認できます。

1. **次へ**をクリックします。**NetScalerおよびGatewayインスタンスに関するインサイト**ページが開きます。

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

次のいくつかの手順は、NetScaler Consoleが提供できるもののプレビューを提供し、NetScalerインスタンスをNetScaler Consoleにシームレスにオンボーディングするのに役立つガイド付きワークフローとして機能します。

ステップ2：NetScalerおよびGatewayインスタンスに関するインサイト

このインサイトページは、Call HomeまたはNetScaler Console接続、あるいはその両方を通じて収集されたデータを使用して、NetScalerインスタンスに関するインサイトを提供します。このページでは、セキュリティアドバイザリ（現在のNetScaler CVEに関するアドバイス）、アップグレードアドバイザリ（EOM/EOLのタイムラインに基づくアドバイス）、主要なメトリック、トレンドなど、NetScalerインフラストラクチャ全体に関するインサイトを提供し、NetScalerのパフォーマンスと健全性に影響を与える問題を強調し、問題を軽減する方法を推奨します。これらのインサイトと推奨事項は、NetScaler Consoleが提供する豊富なメリットと付加価値のほんの一部にすぎません。さらに多くのメリット、詳細なインサイト、および推奨されるアクションを実行できるようにするには、NetScalerインスタンスをNetScaler Consoleにオンボーディングする必要があります。

インサイトと推奨事項は、次のタイプに分類されます。

- **セキュリティアドバイザリ**: NetScalerインスタンスをオンボーディングして、NetScalerインスタンスのCVE影響の詳細を取得し、推奨される修復または軽減策を実行します。
- **アップグレードアドバイザリ**: NetScalerインスタンスをNetScaler Consoleにオンボーディングし、EOM/EOLに達した、または達しつつある、あるいは古いリリース/ビルドを使用しているNetScalerインスタンスをアップグレードします。
- **最近のイベント**: NetScalerインスタンスをNetScaler Consoleにオンボーディングして、200以上のイベントを定期的に監視し、メール、PagerDuty、Slack、ServiceNow経由で通知を受け取るためのルールを作成し、適切なアクションを実行します。
- **リソース使用率 - トレンドと異常**: NetScalerインスタンスをNetScaler Consoleにオンボーディングして、NetScalerインスタンスの健全性、パフォーマンスの問題、およびそれらの問題を軽減するための推奨事項の包括的なビューを取得します。NetScalerインスタンスの予測CPUおよびメモリ使用量も評価できます。
- **NetScaler展開ガイダンス**: NetScalerインスタンスをNetScaler Consoleにオンボーディングし、NetScaler Consoleの構成ジョブを使用してHAペアとして構成します。

1. **セキュリティアドバイザリ**: NetScaler Consoleセキュリティアドバイザリは、NetScalerインスタンスを危険にさらす脆弱性について警告し、軽減策と修復策を推奨します。

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

注:

オンボーディングメールとガイド付きワークフローのセキュリティアドバイザリのインサイトは、NetScalerビルドバージョンスキャンのみに基づいています。NetScalerインスタンスをNetScaler Consoleにオンボーディングすると、決定的で網羅的なセキュリティアドバイザリのインサイトを確認できます。**例**: CVEが脆弱性評価のためにバージョンと構成の両方のスキャンを必要とする場合、オンボーディングメールとガイド付きワークフローはバージョンスキャンに基づいた結果を表示します。そのため、誤検知が発生する可能性があります。影響のより決定的で正確な評価を知るには、NetScalerをNetScaler Consoleにオンボーディングしてください。オンボーディング後、NetScaler Consoleセキュリティアドバイザリは、バージョンと構成のスキャンに基づいた、脆弱なNetScaler評価である影響評価を表示します。

CVE ID、脆弱性の種類、および影響を受けるNetScalerインスタンスを確認できます。CVE IDリンクをクリックすると、セキュリティ速報記事に移動します。

- この推奨事項は、NetScalerインスタンスをNetScaler Consoleにオンボーディングして、NetScalerインスタンスへのCVEの影響に関する詳細情報を取得し、推奨される軽減策または修復策を実行するように案内します。影響を受けるNetScalerインスタンスをクリックすると、影響を受けたインスタンスのIPアドレスが表示されます。

2. **アップグレードアドバイザリ**: このアドバイザリを使用して、EOM/EOLに近づいている、または古いビルドを使用しているNetScalerインスタンスを確認します。

   これらのインサイトに基づいて、NetScaler Consoleは、EOM/EOL前にタイムリーなアップグレードを計画するか、最新の機能と修正の恩恵を受けることを推奨します。

   アップグレードを実行するには、NetScalerインスタンスをNetScaler Consoleにオンボーディングする必要があります。

3. **最近のイベント**: NetScalerインスタンスで発生した重大なエラーの詳細と、エラーが発生したNetScalerインスタンスのリストを取得します。

4. **リソース使用率 - 傾向と異常**: CPU、メモリ、HTTPスループット、SSLスループットの高いリソース使用率に関するインサイトを見つけます。各インサイトについて、NetScaler Consoleは推奨されるアクションを提案します。これらのインサイトと推奨事項をより詳細に把握するに

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

は、NetScalerインスタンスをNetScaler Consoleにオンボーディングする必要があります。オンボーディング後の利点は次のとおりです。

- CPU: NetScaler Consoleで今後24時間のCPU使用率を予測します。
- メモリ: NetScaler Consoleで今後24時間のメモリ使用率を予測します。
- SSLスループット: NetScaler ConsoleでインテリジェントなApp AnalyticsによるSSLリアルタイム最適化を表示します。
- HTTPスループット: Infrastructure Analyticsを使用してNetScalerのスループット容量の問題をトラブルシューティングします。

- **キーメトリック**: CPU、メモリ、HTTPスループット、SSLスループットに関連する主要なメトリックの詳細を取得し、メトリックの異常な傾向を明らかにします。

5. **展開ガイダンス**: スタンドアロンのNetScalerとして展開されているNetScalerインスタンスを可視化します。NetScaler Consoleは、より優れた回復性のためにこれらのNetScalerインスタンスをHAペアとして構成することを推奨します。これには、NetScalerインスタンスをNetScaler Consoleにオンボードし、メンテナンスジョブを使用してインスタンスをHAペアとして構成する必要があります。

ステップ3：オンボードするNetScalerおよびGatewayインスタンスを選択する

このページには、環境内のすべてのNetScalerおよびGatewayインスタンスが表示されます。NetScaler Consoleにオンボードする NetScalerおよびGatewayインスタンスを表示して選択し、**次へ**をクリックします。

1. NetScaler Consoleにオンボードする NetScalerインスタンスを表示して選択します。

   デバイス情報、NetScaler構成、利用可能なNetScaler機能、ライセンス情報など、いずれかのインスタンスの詳細が必要な場合は、NetScalerインスタンスの下にあるインスタンスのIPアドレスをクリックします。

   インスタンスがリストにない場合は、右上の**リストにNetScalerが見つかりませんか**を使用します。

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

3つの方法で続行できます。**NetScalerをリストに追加**の下に示されている手順に従うか、**NetScalerを検索**オプションを使用します。これら2つの手順で解決しない場合は、ワークフローをスキップしてNetScalerインスタンスをオンボーディングする従来の方法に進む**従来の方法を使用**オプションをクリックします。

NetScalerを検索オプションの場合、必須フィールド（シリアルID、NetScalerインスタンスIPアドレス、ライセンスシリアル番号、フルフィルメントID）に詳細を入力して検索します。

ステップ4：NetScalerインスタンスをNetScaler Consoleにオンボードする

組み込みエージェント（デフォルトオプション）または外部エージェントを使用してインスタンスをオンボードできます。

組み込みエージェントを使用してNetScalerインスタンスをオンボードする

自動およびスクリプトベースのオンボーディングでは、デフォルトで設定されている組み込みエージェントを使用します。

自動オンボーディング：以下のNetScalerバージョンでのみサポートされています。

- NetScaler MPXおよびVPXイメージバージョン12.1 57.18以降、および13.0 61.48以降
- SDXバージョンイメージ13.0 61.48以降、および12.1 58.14以降

別のNetScalerインスタンスを選択するには、 をクリックします。

選択されたNetScalerインスタンスの合計のうち、一部のインスタンスは自動オンボーディングの対象となる場合があります（最小バージョン基準に基づく）。自動オンボーディングの対象となるインスタンスを確認できます。

オンボーディングのテスト実行を実行して、NetScalerインスタンスがオンボードの準備ができていることを確認できます。 をクリックしてテスト実行を開始します。詳細については、「NetScalerインスタンスのオンボーディング準備状況をテストする」を参照してください。

テスト実行なしでオンボードする場合は、NetScalerのユーザー名とパスワードを入力します。資格情報はNetScalerユーザー管理者資格情報である必要があり、NetScaler Consoleはこれらの資格情報を使用してNetScalerをオンボードします。 をクリックして、NetScalerインスタンスをNetScaler Consoleにオンボードします。

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

注

NetScalerの資格情報を指定してデバイスプロファイルを作成すると、ADM GUIは各NetScalerインスタンスのユーザー名とパスワードを再度要求することはありません。ただし、**デバイスプロファイル**ドロップダウンからプロファイルを選択して、NetScalerインスタンスを認証できます。

自動オンボーディングには2〜5分かかる場合があります。

注:

NetScalerインスタンスをNetScaler Consoleに自動オンボーディングしたくない場合は、自動オンボーディングを無効にして、スクリプトベースのオプションを使用してオンボーディングできます。

スクリプトベースのオンボーディング: 自動オンボーディングが完了した後、スクリプトベースのオンボーディングを使用して残りのインスタンスをオンボーディングできます。次のいずれかのオプションを使用します。

- **オプション1**: スクリプトをダウンロードし、tarファイルを展開して、UIに表示されているコマンドを使用して、いずれかのNetScalerインスタンスで実行します。このスクリプトを実行するNetScalerインスタンスが、他のすべての選択されたNetScalerインスタンスへのネットワーク接続を持っていることを確認してください。
- **オプション2**: 各NetScalerインスタンスのCLIコンソールにログインし、UIに表示されているコマンドを実行します。詳細については、ドキュメント「NetScaler組み込みエージェントを構成してインスタンスを管理する」のステップ7を参照してください。各NetScalerインスタンスに対して新しい一意のアクティベーションコードを生成するようにしてください。

すべてのインスタンスをオンボーディングしたら、**NetScaler Consoleに移動**をクリックして、NetScaler Consoleインスタンス管理UIダッシュボードに移動し、さまざまな機能を探索します。

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

注

NetScaler Consoleの新規顧客でNetScaler Consoleライセンスがない場合、Citrixサービスアカウントはデフォルトでexpressアカウントになります。NetScaler Consoleアカウントの資格の詳細については、「Expressアカウントを使用してNetScaler Consoleリソースを管理する」を参照してください。

外部エージェントを使用してNetScalerインスタンスをオンボーディングする

NetScaler Consoleでプールライセンスまたは完全な分析スイート、あるいはその両方を使用したい場合は、外部エージェントベースのオンボーディングを使用できます。

☐
以下の手順を完了します。

1. デバイスプロファイルを選択します。

   注

   セキュリティ上の理由から、オンボーディングにデフォルトのNetScaler資格情報 (nsroot/nsroot) を使用することはできません。

2. 外部エージェントを選択し、**新しいエージェントのセットアップ**をクリックします。
3. 次のいずれかの環境を選択します。

   - アマゾン ウェブ サービス
   - マイクロソフト アジュール
   - グーグル クラウド プラットフォーム
   - オンプレミス

オンプレミスハイパーバイザーにエージェントをインストールする

オンプレミスを選択した場合、エージェントを次のハイパーバイザーにインストールできます: Citrix Hypervisor™、VMware ESXi、Microsoft Hyper-V、Linux KVM Server。

☐

1. **ハイパーバイザー上 (オンプレミス)** を選択し、**次へ**をクリックします。

   ☐

2. ハイパーバイザーの種類を選択し、イメージをダウンロードします。例: VMware ESXi。

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

イメージをダウンロード(/en-us/netscaler-console-service/media/adc-external-agent-onboard-3.png)

3. サービスURLとアクティベーションコードを使用してエージェントを設定します。

   エージェントを設定(/en-us/netscaler-console-service/media/adc-external-agent-onboard-4.png)

   エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。オンプレミスハイパーバイザーにエージェントをインストールする方法の詳細については、「オンプレミスにNetScalerエージェントをインストールする」を参照してください。

4. 「**Register Agent**」をクリックします。完了したら、「**Done**」をクリックしてNetScalerオンボーディングNetScaler Consoleページに戻ります。

   オンボーディングを完了(/en-us/netscaler-console-service/media/adc-external-agent-onboard-5.png)

5. 「**Start onboarding**」をクリックします。すべてのインスタンスをオンボーディングしたら、「**View instance dashboard**」をクリックしてNetScaler Consoleインスタンス管理UIダッシュボードに移動し、さまざまな機能を探索します。

   インスタンスダッシュボードを表示(/en-us/netscaler-console-service/media/adc-external-agent-onboard-6.png)

パブリッククラウドにエージェントをインストールする

エージェントは、次のいずれかのクラウド環境にインストールできます。

- アマゾン ウェブ サービス
- マイクロソフト アジュール
- グーグル クラウド プラットフォーム

詳細については、次のドキュメントを参照してください。

- Microsoft Azure クラウドにエージェントをインストールする
- AWS にエージェントをインストールする
- GCP にエージェントをインストールする

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

NetScalerインスタンスのオンボーディング準備状況をテストする

NetScalerインスタンスをNetScaler Consoleにオンボーディングする際、インスタンスがオンボーディングの準備ができているかどうかをテストできます。テスト実行ステータスは、インスタンスが準備できているか、またはレビューが必要かを示します。

オンボーディング準備状況のテスト(/en-us/netscaler-console-service/media/built-in-agent-test-dry-run.png)

テストをクリックして、診断ドライランを開始します。「**自動オンボーディングのテスト**」ページには、問題カテゴリ、ステータス、および推奨事項が表示されます。

エージェントのドライラン診断の詳細(/en-us/netscaler-console-service/media/test-auto-onboarding-message.png)

詳細については、「NetScaler Console GUIでNetScaler診断情報を表示する」を参照してください。

NetScalerのテスト実行ステータスが「**レビューが必要**」の場合：

- デバイスプロファイルでNetScalerのログイン資格情報を確認します。
- 次のようなエンドポイントに到達できません：
  - `adm.cloud.com`
  - `agent.adm.cloud.com`
  - `trust.citrixnetworkapi.net`
  - `download.citrixnetworkapi.net`

オンボーディング準備状況のテストを実行する際に問題が発生した場合は、推奨事項について「トラブルシューティング」を参照してください。

メール設定

NetScaler Consoleサービスでは、Advisory Console Connectベースのロータッチオンボーディングワークフローを使用してNetScalerインスタンスをオンボーディングできます。このワークフローの一環として、お客様はNetScaler Consoleサービスから製品が開始するメールを受信します。Advisory Console Connectベースのロータッチオンボーディングワークフローの一環として受信するメール通知を有効または無効にできます。メール通知は、以下の方法で設定および管理できます。

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

- **すべての管理者にメールを有効にする** - 組織内のすべての管理者にメールを有効にできます。デフォルトでは、組織内のすべての管理者にメールが有効になっています。
- **選択した管理者にメールを有効/無効にする** - 組織内の特定の管理者のみがメールを受信し、他の管理者は受信しないようにメール設定をカスタマイズできます。
- **すべての管理者にメールを無効にする** - 組織内のすべての管理者のメールを無効にして停止できます。

メール設定の構成

Console Advisory Connectベースのロータッチオンボーディングワークフローの一環として受信するメールを、メール設定で有効または無効にできます。**メール設定**を構成するには：

1. 製品が開始するメールで、**ADMサービスにオンボード**をクリックします。**Citrix Cloud™**ページが表示されます。
2. **Citrix Cloud**ログインページで：
   - 既存のCitrix Cloudのお客様である場合は、Citrix.com、My Citrix、またはCitrix Cloudの資格情報を使用してCitrix Cloudにサインインします。
   - 既存のCitrix Cloudのお客様でない場合は、Citrix Cloudにサインアップします。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。

     注：

     複数の組織IDに属しており、そのうちの1つの組織IDがCitrix Cloudにある場合は、既存の資格情報を使用してサインインします。

   NetScaler Consoleランディングページが表示され、NetScaler Consoleの概要とその利点が提供されます。
3. NetScaler Consoleランディングページで、**次へ**をクリックします。

   「**NetScalerおよびGatewayインスタンスに関するインサイト**」ページが表示され、推奨事項とともにNetScalerインフラストラクチャ全体のインサイトを得ることができます。
4. 「**NetScalerおよびGatewayインスタンスに関するインサイト**」ページで、「**次へ**」をクリックします。

   「**オンボーディングするNetScalerおよびGatewayインスタンスの選択**」ページが表示され、オンボーディングするNetScalerインスタンスのリストと、「**メール設定**」などの追加オプションを確認できます。

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

5. 「**メール設定**」をクリックします。「**メール設定**」ペインが表示されます。

   これで、メール設定を構成してメールを有効または無効にできます。

注:

NetScalerインスタンスを1つだけオンボーディングした場合、これらのメールは受信されません。

NetScaler Console GUIをすでに使用していて、メール設定を構成したい場合は、次の手順を実行します。

1. NetScaler Console GUIで、**インフラストラクチャ > インスタンス**に移動し、**NetScaler**をクリックします。「**NetScaler**」ページが表示されます。
2. 「**NetScaler**」ページで、「**アセットインベントリ**」をクリックします。

   「**オンボーディングするNetScalerおよびGatewayインスタンスの選択**」ページが表示され、オンボーディングされたNetScalerインスタンスのリストと、「**メール設定**」などの追加オプションが表示されます。
3. 「**メール設定**」をクリックします。「**メール設定**」ペインが表示されます。

   これで、メール設定を構成してメールを有効または無効にできます。

すべての管理者にメールを有効にする

デフォルトでは、組織内のすべての管理者に対してメールが有効になっています。

Console Advisory Connectベースのワークフローの一部としてメール通知を有効にする、または購読するには：

1. **メール設定**ペインで、すべての管理者に対して**メールを有効にする**を選択します。

   管理者メールを有効にする(/en-us/netscaler-console-service/media/enable-settings.png)
2. **保存**をクリックし、**閉じる**をクリックします。

   組織内のすべての管理者が購読され、Console Advisory Connectベースのワークフローの一部としてメール通知を受け取るようになります。

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

組織内の特定の管理者に対してメールを有効/無効にする

組織内の特定の管理者のみがメールを受信するようにメール設定をカスタマイズできます。メールが有効になっている管理者のリストが左側に、メールが無効になっている管理者のリストが右側に表示されます。

組織内の特定の管理者に対してメールを無効にするには：

1. **有効**リストで管理者のメールアドレスを見つけます。
2. 追加ボタン（**+**）をクリックします。

   選択した管理者を無効にする(/en-us/netscaler-console-service/media/disable-selected-admins.png)

   管理者のメールアドレスが**無効**リストに追加されていることを確認します。
3. **保存**をクリックし、**閉じる**をクリックします。

   管理者は、Console Advisory Connectベースのワークフローの一環として、メール通知を受け取らないように登録解除されました。

   注:

   複数の管理者のメールを無効にする場合は、**有効**なメールリストでそれらのメールIDをすべて選択し、追加ボタン (**+**) をクリックして、メールIDを**無効**なリストに追加します。**保存**をクリックし、**閉じる**をクリックします。

組織内の特定の管理者またはすべての管理者に対して以前にメールを無効にしていた場合でも、すべての管理者に対してメールを有効にすることができます。組織内の特定の管理者に対してメールを有効にするには、次の手順を実行します。

1. **無効**なリストで管理者のメールアドレスを見つけます。
2. 削除ボタン (-) をクリックします。管理者のメールアドレスが**無効**なリストから削除されます。

3. **保存**をクリックし、**閉じる**をクリックします。

   管理者はオンボーディング関連のメールを受信するようになります。管理者はメール通知を受信するように登録されました。

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

注:

複数の管理者のメールを有効にする場合は、**無効**なメールリストでそれらのメールIDをすべて選択し、削除ボタン (-) をクリックして、メールIDを**有効**なリストに追加します。**保存**をクリックし、**閉じる**をクリックします。

すべての管理者のメールを無効にする

組織に属するすべての管理者に対してメールを無効にする、または停止する場合は、このオプションを選択できます。

メールの受信を無効にする、または登録解除するには、次の手順を実行します。

1. **メール設定**ペインで、**すべての管理者のメールを無効にする**を選択します。

2. 「**保存**」と「**閉じる**」をクリックします。

   組織内のすべての管理者は購読解除され、メール通知を受信しなくなります。

診断ツールまたはNetScaler Console GUIを使用して問題をトラブルシューティングする

注

診断ツールは、Console Advisory Connectベースのロータッチオンボーディングを使用してオンボーディングされた、またはオンボーディングされる予定のNetScalerインスタンスにのみ適用されます。

詳細については、NetScaler Console 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。
NetScalerインスタンスをNetScaler Consoleにオンボーディングする際、NetScalerインスタンスのオンボーディングが正常に完了しないいくつかの問題が発生する可能性があります。管理者として、オンボーディング失敗の原因を知る必要があります。以下の状況で、診断ツールを使用して診断チェックを実行できます。

- 自動オンボーディングまたはスクリプトベースのオンボーディング中に問題が発生した場合
- NetScalerインスタンスがオンボーディングの準備ができているかを確認したい場合

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

- NetScaler Console GUIで「ダウン」ステータスを表示している、すでにオンボーディングされているNetScalerインスタンスの問題を分析したい場合

NetScalerインスタンスでConsole Advisory Connectが有効になっている場合、診断の詳細は自動的にCitrixに送信され、NetScaler Console GUIで詳細を表示できます。Console Advisory Connectが有効になっていない場合は、診断ツールを手動で使用できます。

診断ツールを手動で使用する

診断ツールは、`mastools`アップグレード（13.1-2.x以降）の一部として利用可能で、`/var/mastools/scripts`でアクセスできます。NetScalerインスタンスで`cat /var/mastools/version.txt`コマンドを実行することで、`mastools`のバージョンを確認できます。

診断ツールを実行するには：

1. SSHクライアントを使用して、NetScalerインスタンスにログオンします。
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. `cd /var/mastools/scripts`と入力します。
4. `sh mastools_diag`と入力します。

ツールが起動し、以下の診断チェックの結果が表示されます:

- **エヌエスシーエルアイ**
- **DNS設定**
- **インターネット接続**
- **インスタンスからADMへの接続**
- **ユーザー権限**

トラブルシューティング後も問題が解決しない場合は、サポートに連絡できます。サポートに連絡する際は、診断ツール実行後に表示される構成情報を提供する必要があります。

以下は、問題のないNetScalerインスタンスの診断結果の例です:

- **1** – 診断チェックの種類を表示します
- **2** – 診断チェックの結果を緑または赤で表示します。緑は結果が成功したことを示し、赤は結果が成功しなかったことを示します。
- **3** – 診断ツールを実行するたびに、NetScaler Consoleの構成情報が黄色で表示されます。NetScalerサポートに連絡する場合は、この情報を提供する必要があります。

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

診断ツールを使用してNetScalerインスタンスのオンボーディング準備状況を検証する

NetScalerインスタンスをNetScaler Consoleにオンボーディングする前に、NetScalerインスタンスで診断ツールを実行して、その準備状況を確認できます。NetScalerインスタンスに問題がなく、オンボーディングの準備ができていれば、ツールは「**device not claimed on ADM**」というメッセージを表示します。

NetScaler Console で要求されていないデバイス(/en-us/netscaler-console-service/media/device-not-claimed.png)

NetScaler Console GUI で NetScaler 診断情報を表示する

Infrastructure > Instances > NetScaler に移動し、**Asset Inventory** をクリックすると、新しく追加された**オンボーディング準備状況**オプションが表示されます。このオプションは、**要確認**または**OK**などの NetScaler インスタンスのオンボーディング準備状況を提供します。

- **要確認**。NetScaler インスタンスには修正が必要な問題があります。
- **OK**。NetScaler インスタンスはオンボーディングの準備ができています。

> **注:**
>
> **オンボーディング準備状況**が空白の場合、NetScaler インスタンスが診断サポートを備えた最新のイメージで実行されていないことを意味します。

NetScaler インスタンスに問題がある場合、**要確認**オプションが表示され、クリックして詳細を表示できます。

自動診断メッセージ(/en-us/netscaler-console-service/media/auto-diagnostic-info.png)

要確認をクリックすると、**NetScaler 診断の詳細**ページに問題の詳細が表示されます。

自動診断の問題の詳細(/en-us/netscaler-console-service/media/auto-diagnostic-issue.png)

- **カテゴリ**。問題のカテゴリを提供します。
- **ステータス**。**要確認**、**OK**、または**該当なし**などの問題のステータスを提供します。
- **推奨事項**。問題のトラブルシューティングに必要な推奨事項を提供します。

問題を修正すると、オンボーディング準備状況のステータスが**OK**に変更されます。

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

トラブルシューティング

以下は、NetScalerインスタンスに関するいくつかの問題と、そのトラブルシューティング手順です。

無効なユーザー名またはパスワード

回避策: 管理者プロファイルで指定されたユーザー名とパスワードが正しいことを確認してください。NetScalerインスタンスのパスワードを変更した場合は、インスタンスの管理者プロファイルを変更する必要があります。詳細については、「管理者プロファイルの変更」を参照してください。

DNS構成エラー

回避策: DNSが構成されているか、DNS IPアドレスが有効であることを確認してください。詳細については、「DNS構成」を参照してください。

インターネット接続なし

回避策: ファイアウォール設定がインターネットアクセスをブロックしていないこと、および必要なプロキシが構成されていることを確認してください。

NetScaler Consoleエンドポイントへの接続なし

回避策: ファイアウォール設定を確認し、以下のNetScaler Consoleエンドポイントがファイアウォールでブロックされていないことを確認してください。

```
ADM_GRP_EP = "adm.cloud.com"



ADM_AGENT_EP = "agent.adm.cloud.com"



ADM_TRUST_EP = "trust.citrixnetworkapi.net"



ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
```

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

診断チェックで問題が見つからず、接続の問題が依然として解決しない場合は、NetScaler Consoleの構成情報（黄色で表示）をメモし、NetScalerサポートに連絡してください。

NetScalerインスタンスがオンボーディングの準備ができていることを確認するためにテスト実行を行うと、以下の問題が発生する可能性があります。

組み込みエージェントのドライランタイムアウト

ドライランの結果が5分以内に取得されない場合、タイムアウトメッセージが表示されます。

タイムアウト(/en-us/netscaler-console-service/media/onboarding-timeout.png)

推奨事項: NetScalerインスタンスが診断サポートを備えた最新のイメージで実行されているかどうかを確認することをお勧めします。また、アセット選択テーブルでは、「オンボーディング準備状況」列が空白で表示されます。

デバイスプロファイルのドロップダウンに表示される赤い枠線

ドライラン中にNetScaler認証が失敗し、デバイスプロファイルのドロップダウンに赤い枠線が表示されます。

プロファイルエラー(/en-us/netscaler-console-service/media/builtin-agent-dry-run.png)

推奨事項: NetScalerユーザー管理者資格情報を再度入力し、デバイスプロファイルを作成し、「テスト」をクリックしてドライランを再度実行します。

組み込みエージェントから外部エージェントへの移行

NetScaler Consoleを管理および監視のみに使用し始めた後、プールライセンスや分析などの他の機能を使用したいと考えるかもしれません。そのためには、組み込みエージェントから外部エージェントに移行する必要があります。

組み込みエージェントは、管理および監視機能のみをサポートしています。プールライセンスや分析などの他のNetScaler Console機能には、外部エージェントが必要です。このドキュメントでは、既存のNetScaler Console組み込みエージェントから外部のハイパーバイザーベースのエージェントに移行する手順について説明します。

開始する前に

移行を開始する前に、外部エージェントをインストールしてください。トピック「オンプレミスにNetScalerエージェントをインストールする」に記載されている手順に従ってください。

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

組み込みエージェントから外部エージェントへの移行

組み込みエージェントから外部エージェントに移行するには、次の手順に従います。

1. NetScaler Console GUIで、**Infrastructure > Instances Dashboard > NetScaler** の下にあるNetScalerインスタンスを選択し、**Edit** をクリックします。

2. サイトとエージェントを選択し、**OK** をクリックします。

3. インスタンスを再度選択し、**Select Action > Rediscover** をクリックします。

NetScaler Consoleでサイトを作成し、エージェントをサイトに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。

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

NetScaler Console に ID プロバイダーとして SAML を接続する

NetScaler Console は、管理者とサブスクライバーが NetScaler Console にサインインする際の認証に、ID プロバイダーとして SAML (Security Assertion Markup Language) を使用することをサポートしています。オンプレミスの Active Directory (AD) とともに、任意の SAML 2.0 プロバイダーを使用できます。

ほとんどの SAML プロバイダーでは、この記事の情報を使用して SAML 認証を設定します。Azure AD で SAML 認証を使用したい場合は、Azure AD アプリギャラリーから Citrix Cloud™ SAML SSO アプリを使用するオプションがあります。

前提条件

NetScaler Console での SAML 認証には、次の要件があります。

- SAML 2.0 をサポートする SAML プロバイダー
- オンプレミス AD ドメイン
- リソースの場所に展開され、オンプレミス AD ドメインに参加している 2 つの Cloud Connector。Cloud Connector は、Citrix Cloud がリソースの場所と通信できるようにするために使用されます。
- SAML プロバイダーとの AD 統合。

クラウドコネクタ

Citrix Cloud Connector™ ソフトウェアをインストールするためのサーバーが少なくとも 2 台必要です。Cloud Connector の高可用性を確保するために、少なくとも 2 台のサーバーを用意することをお勧めします。これらのサーバーは、次の要件を満たしている必要があります。

- Cloud Connector Technical Details に記載されているシステム要件を満たしていること。
- 他の Citrix コンポーネントがインストールされておらず、AD ドメインコントローラーではなく、リソースの場所のインフラストラクチャにとって重要ではないマシンであること。
- リソースが存在するドメインに参加していること。ユーザーが複数のドメインのリソースにアクセスする場合は、各ドメインに少なくとも 2 つの Cloud Connector をインストールする必要があります。

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

- サブスクライバーが Citrix Workspace を介してアクセスするリソースに接続できるネットワークに接続されていること。
- インターネットに接続されていること。

Active Directory

SAML認証を構成する前に、次のタスクを実行します。

- Oktaインスタンスにユーザーをインポートするには、Active Directoryのユーザーに対して、名、姓、およびメールアドレスのフィールドが必須です。
- ワークスペースのサブスクライバーがActive Directory (AD) にユーザーアカウントを持っていることを確認します。ADアカウントを持たないサブスクライバーは、SAML認証が構成されている場合、ワークスペースに正常にサインインできません。
- サブスクライバーのADアカウントのユーザープロパティが入力されていることを確認します。Citrix Cloudは、サブスクライバーがCitrix Workspaceにサインインする際にユーザーコンテキストを確立するためにこれらのプロパティを必要とします。これらのプロパティが入力されていない場合、サブスクライバーはサインインできません。これらのプロパティには以下が含まれます。
  - メールアドレス
  - 表示名（オプション）
  - 共通名
  - SAMアカウント名
  - ユーザープリンシパル名
  - オブジェクトGUID
  - SID
- オンプレミスのADにCloud Connectorを展開して、Active Directory (AD) をCitrix Cloudアカウントに接続します。
- ADユーザーをSAMLプロバイダーに同期します。Citrix Cloudは、ワークスペースのサブスクライバーが正常にサインインできるように、ADユーザー属性を必要とします。

SAML SSO 設定

Okta インスタンスで、**Directory integrations > Add Active Directory** に移動します。

Okta インスタンス(/en-us/netscaler-console-service/media/saml-okta-navigation.png)

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

統合を成功させるには、SAML ID プロバイダーが SAML アサーションでユーザーの特定の Active Directory 属性を Citrix Cloud に渡す必要があります。具体的には、,

- セキュリティ識別子 (SID)
- objectGUID (OID)
- ユーザープリンシパル名 (UPN)
- メール (Email)

1. 管理者資格情報を使用して Okta にログオンします。
2. **Directory > Profile Editor** を選択し、**Okta User (default)** プロファイルを選択します。Okta にユーザープロファイルページが表示されます。

3. **Attributes** で、**Add Attributes** を選択し、カスタムフィールドを追加します。

   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`

   をクリックし、このプロセスを繰り返して4つのカスタム属性を作成します。

   4つのカスタム属性を作成すると、次の詳細を表示できます。

4. Active Directory属性をカスタム属性にマッピングします。使用しているActive Directoryを **>** で選択します。
5. 属性マッピングを編集します。

   a. Oktaコンソールから、 **>** に移動します。

   b. ADの `active_directory` プロファイルを見つけます。このプロファイルは、myDomain Userという形式でラベル付けされている場合があります。ここで、myDomainは統合されたADドメインの名前です。

   c. を選択します。ADドメインの ページが表示され、ADをOktaユーザーにマッピングするためのタブが選択されます。

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

d. 列で、Active Directory属性を、作成したカスタム属性にマッピングします。

   i. `cip_email` の場合、ドメインの 列から「email」を選択します。選択すると、マッピングは `appuser.email` のように表示されます。

   ii. `cip_sid` の場合、ドメインの 列から **objectSid** を選択します。選択すると、マッピングは `appuser.objectSid` のように表示されます。

   iii. `cip_upn` の場合、ドメインの 列から `userName` を選択します。選択すると、マッピングは `appuser.userName` のように表示されます。

   iv. `cip_oid` については、お使いのドメインの**ユーザープロファイル**列から `externalId` を選択します。選択すると、マッピングは `appuser.externalId` として表示されます。

6. `https://citrix.cloud.com` でCitrix Cloudにサインインします。
7. Citrix Cloudメニューから、 を選択します。
8. **SAML 2.0**を見つけて、 をクリックします。

   ページが表示されます。

   `xml` ファイルをダウンロードし、任意のファイルエディターを使用してファイルを開きます。Oktaでの追加設定を完了した後、このページに再度戻る必要があります。
9. Oktaで、 **>** に移動します。
10. ページで、 をクリックします。
11. ページで、 を選択し、 をクリックします。
12. アプリ名、アプリのロゴ（オプション）、アプリの可視性などの詳細を入力し、 をクリックします。
13. タブで、ダウンロードした `xml` ファイルの詳細を使用する必要があります。

    a. には `https://saml-internal.cloud.com/saml/acs` 、 には `https://saml-internal.cloud.com` のURL詳細を入力します。

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

> **注:**
>
> 外部のCitrix Cloudの場合、URLは`https://saml-internal.cloud.com`ドメインの代わりに`https://saml.cloud.com/saml/acs`および`https://saml.cloud.com`である必要があります。

b. **Name ID Format** には「**Unspecified**」を選択します。

c. **Application Username** には「**Okta Username**」を選択します。

d. **Show Advanced Settings** をクリックし、**Response** と **Assertion** が **Signed** で選択されていることを確認します。

e. 次の画像に示すように、**Attribute Statements** を追加します。

属性(/en-us/netscaler-console-service/media/saml-attribute-statements.png)

f. 他のすべてのオプションはデフォルトのままにして、**Next** をクリックします。

g. 「**I'm an Okta customer adding an internal app**」を選択し、**Finish** をクリックします。

14. Oktaアプリケーションが作成されました。**View Setup Instructions** をクリックします。

セットアップ手順(/en-us/netscaler-console-service/media/saml-setup-instructions.png)

How to Configure SAML 2.0 for test Application ページが表示され、Citrix Cloudに再度追加する必要がある詳細情報が表示されます。

証明書をダウンロードして、Citrix Cloudにアップロードします。

15. Citrix Cloudの**Configure SAML**ページに戻り、以下に記載されている残りの設定を完了する必要があります。

残りの手順(/en-us/netscaler-console-service/media/saml-continue-steps.png)

ダウンロードした証明書を使用し、ファイル名拡張子を`.cert`から`.crt`に変更して、Citrix Cloud にアップロードします。

16. 証明書をアップロードした後、他のすべてのオプションはデフォルトのまま使用します。

SAMLプレビュー(/en-us/netscaler-console-service/media/saml-preview.png)

17. 次に、`appuser.userName`が **Directory-integrations > Active Directory -> Provisiong > To okta** で定義されていることを確認する必要があります。

SAMLユーザー名(/en-us/netscaler-console-service/media/saml-user-name.png)

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

注記：

場合によっては、`appuser.cip_upn` の代わりに `user.cip_upn` を使用する必要があります。この画像に示すように、OKTA統合におけるアプリケーションの定義を確認してください。

18. OktaでこのSAMLアプリケーションにユーザーを追加してみてください。ユーザーは複数の方法で割り当てることができます。

    方法1：

    a. 管理者資格情報でOktaにログオンします
    b. **Applications > Applications** に移動します
    c. 作成したSAMLアプリケーションを選択します
    d. **Assign > Assign to People** をクリックします

       ユーザーの追加(/en-us/netscaler-console-service/media/saml-adduser.png)

    e. **Assign** をクリックし、**Save and Go back** を選択します。
    f. 「**完了**」をクリックします。

    方法2：

    a. 「**Applications > Applications**」に移動します。
    b. 「**Assign Users to App**」をクリックします。

       「アプリにユーザーを割り当てる」(/en-us/netscaler-console-service/media/saml-adduser-secondway.png)

    c. アプリケーションとユーザーを選択し、「**次へ**」をクリックします。

       「ユーザーを割り当てる」(/en-us/netscaler-console-service/media/saml-adduser2.png)

    d. 「**Confirm Assignments**」をクリックします。

    方法3：

    a. 「**Directory > People**」に移動します。
    b. 任意のユーザーを選択します。
    c. 「**Assign Applications**」をクリックし、SAMLアプリケーションをユーザーに割り当てます。

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

19. ユーザーを割り当てたら、Citrix Cloudにログオンします。
20. Citrix Cloudメニューから、「**Identity and Access Management**」を選択します。
21. 「**Administrators**」タブで、「**Add Administrator/group**」をクリックします。
22. リストから「**Active Directory -** 」を選択し、ドメインを選択して、「**次へ**」をクリックします。

23. アクセス権限を指定します。
24. すべてが正しいか確認し、「**招待を送信**」をクリックします。
25. 「**認証**」タブで、SAML 2.0のサインインURLを表示できます。以下に例を示します。

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

システム要件

NetScaler Console の使用を開始する前に、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する必要があります。

サポートされるブラウザ

NetScaler Console 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
マイクロソフト エッジ	79以降
グーグル クローム	51以降
サファリ	10以降
モジラ ファイアフォックス	52以降

エージェントのインストール要件

ネットワーク環境にエージェントをインストールして構成し、NetScaler Console とデータセンター内の管理対象インスタンス間の通信を有効にします。オンプレミスのデータセンターでは、Citrix XenServer、VMware ESXi、Microsoft Hyper-V、および Linux KVM サーバーにエージェントをインストールできます。

エージェントの要件は、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です。次の表に、すべての NetScaler Console 機能を使用するためのエージェント要件を示します。

コンポーネント	要件
RAM	32 GB
仮想 CPU	8

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

コンポーネント	要件
ストレージ容量	30 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

プールまたはフレックスライセンス機能のみを使用する場合のエージェント要件については、「プールまたはフレックスライセンス用の軽量エージェント」を参照してください。

Microsoft Azure、AWS、またはGoogle Cloudにもエージェントをインストールできます。NetScaler Consoleのすべての機能を使用するには、Citrixは各クラウドマーケットプレイスから以下の仮想マシンタイプを使用することを推奨します。

クラウド	エージェント要件	推奨仮想マシンタイプ
AWS	8仮想CPU、32 GB RAM、30 GBストレージスペース	`m4.2xlarge`
マイクロソフト アジュール	8仮想CPU、32 GB RAM、30 GBストレージスペース	`Standard_D8s_v3`
グーグル クラウド	8仮想CPU、32 GB RAM、30 GBストレージスペース	`e2-standard-8`

注記：

Azure は、July 23, 2024 以降、ベースインストーラーバージョン 13.0 および 13.1 のエージェントのスケーリングアウトをサポートしなくなります。

NetScaler エージェントの場合:

- 8 仮想 CPU、32 GB RAM、30 GB のストレージスペースを持つ NetScaler エージェントは影響を受けません。これらのエージェントは、中断することなくアップグレードできます。
- バージョン 14.1 で開始された展開も影響を受けません。

軽量エージェントの場合:

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

- ベースインストーラーバージョン 13.0 または 13.1 を使用している、4 仮想 CPU、8 GB RAM、30 GB のストレージスペースを持つ軽量エージェントは、廃止日以降、スケールアップ（CPU または RAM の増加）できません。
- 今後、軽量エージェントをスケールアップするには、最新バージョンで新しいエージェントを再プロビジョニングしてください。

エージェントのインストール手順については、次のリンクを参照してください。

- Microsoft Azure Cloud にエージェントをインストールする。
- AWS にエージェントをインストールする。
- Google Cloud にエージェントをインストールする。

プールまたはフレックスライセンス用の軽量エージェント

NetScaler Console をプールまたはフレックスライセンスのみに使用する予定がある場合は、次の表に示すように、より低い仕様のエージェントを使用できます。

コンポーネント	要件
RAM	8 GB
仮想CPU	4
ストレージ容量	30 GB

低スペック（軽量）のエージェントは、NetScaler Consoleでのみサポートされます。

Citrixでは、プールライセンス機能のみを使用するために、各クラウドマーケットプレイスから以下の仮想マシンタイプを使用することをお勧めします。

クラウド	エージェント要件	推奨される仮想マシンタイプ
AWS	仮想CPU 4個、RAM 8 GB、ストレージ容量 30 GB	`m4.xlarge`。このインスタンスタイプは、仮想CPU 4個、RAM 16 GB、ストレージ容量 30 GBを提供します。既存のインスタンスタイプの中でエージェント要件のほとんどを満たしているため、

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

クラウド	エージェント要件	推奨される仮想マシンタイプ
		Citrixはこのインスタンスタイプを推奨しています。
マイクロソフト アジュール	4仮想CPU、8 GB RAM、30 GBのストレージスペース	`Standard_F4s_v2`
グーグル クラウド	4仮想CPU、8 GB RAM、30 GBのストレージスペース	`e2-standard-4`

注

Settings > Global Settings > Configurable Featuresに移動して、デフォルトのスケジューリングジョブを無効にする必要があります。

サポートされているポート

NetScalerインスタンスとエージェント間の通信には、必要なポートを開放してください。

NetScalerエージェント用のポート

この表は、エージェントで開放す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 Console サービスからNetScaler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からNetScaler Console サービスへの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 Consoleサービスへ	NetScalerからNetScalerエージェントへ

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

ポート	タイプ	詳細	通信の方向
		のSNMPイベントを受信するため。	
514	UDP	NetScalerインスタンスからNetScaler Consoleサービスへsyslogメッセージを受信するため。	NetScalerからNetScalerエージェントへ
5563	TCP	このポートはNetScaler Console Collectorサービスが実行するために必要です。NetScalerインスタンスからNetScaler ConsoleへNetScalerメトリック（カウンター）を受信するため。	NetScalerからNetScalerエージェントへ
5557/5558	TCP	NetScalerからNetScaler Consoleサービスへのログストリーム通信（WAFセキュリティ違反、Web Insight、HDX Insight用）。	NetScalerからNetScalerエージェントへ
27000および7279	TCP	NetScalerエージェントとNetScalerインスタンス間の通信用ライセンスポート。これらのポートはNetScalerプールライセンスにも使用されます。	NetScalerからNetScalerエージェントへ
5140	UDP	NetScaler Gatewayのテレメトリーデータを受信するポート	NetScalerからNetScalerエージェントへ

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

NetScalerインスタンスのポート

この表は、NetScalerインスタンス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	通信方向
80/443	TCP	NetScaler ConsoleからNetScalerインスタンスへのNITRO通信用。	NetScalerエージェントからNetScalerへ、およびNetScalerからNetScalerエージェントへ
22	TCP	エージェントとNetScaler間のSSH通信用。**注:** このポートはNetScalerテレメトリにも使用されます。	NetScalerエージェントからNetScaler
予約ポートなし	ICMP	NetScalerエージェントとNetScalerインスタンス間のネットワーク到達性を検出するため。	NetScalerエージェントからNetScaler
161	UDP	NetScalerインスタンスからイベントをポーリングするため。	NetScalerエージェントからNetScaler

NetScaler組み込みエージェントのポート

この表は、NetScaler組み込みエージェントに必要な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 ConsoleからNetScalerインスタンスへのNITRO通信用。	NetScaler Console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 Consoleへ

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

注:

NetScaler Consoleサービスのエンドポイントは、エージェントの登録時に生成される「サービスURL」と同じです。エージェントはサービスURLを使用してNetScaler Consoleを特定します。

次のエンドポイントURLへのアクセスが許可されていることを確認してください。

サービス	政府機関向けクラウド	日本	その他の地域 (APEC、EU、米国)
ダウンロードサービス	`download.adm.cloud.us`	`download.citrixnetworkapi.net`	`download.citrixnetworkapi.net`
トラストサービス	`*.citrixnetworkapi.us`	`*.citrixnetworkapi.jp`	`*.citrixnetworkapi.net`
	`trust.citrixworkspacesapi.us`	`trust.citrixworkspacesapi.jp`	`trust.citrixworkspacesapi.net`
サービスURL	`*.agent.adm.cloud.us`	`*.agent.adm.citrixcloud.jp`	`*.agent.adm.cloud.com`
	`*.adm.cloud.us`	`*.adm.citrixcloud.jp`	`*.adm.cloud.com`
	`adm.cloud.us`	`adm.citrixcloud.jp`	`adm.cloud.com`
Citrix Cloud 接続	`citrix.cloud.us`	`citrix.citrixcloud.jp`	`citrix.cloud.com`
	`accounts.cloud.us`	`accounts.citrixcloud.jp`	`accounts.cloud.com`

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

NetScaler Console Analytics ソリューションの要件

必要なCitrix Virtual Apps and Desktopsの最小バージョン

NETSCALER CONSOLEの機能	CITRIX VIRTUAL APPS AND DESKTOPSのバージョン
HDX インサイト	シトリックス バーチャルアプリおよびデスクトップ 7.0 以降

注

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

NetScaler Consoleは、Citrix Virtual AppまたはDesktopに公開され、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Citrix 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でサポートされるシンクライアント

NetScaler Consoleは、ソフトウェアバージョン11.0 Build 65.31以降で実行されているNetScalerインスタンスを監視するために、以下のシンクライアントをサポートしています。

- 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

HDX Insightに必要なNetScalerインスタンスライセンス

HDX Insight 用に NetScaler Console が収集するデータは、監視対象の NetScaler インスタンスのバージョンとインストールされているライセンスによって異なります。HDX Insight レポートは、ソフトウェアバージョン 10.5 以降を実行している NetScaler Premium および Enterprise アプライアンスでのみ表示されます。

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

NetScaler ライセンス/期間	5分	1時間	1日	1週間	1か月
スタンダード	いいえ	いいえ	いいえ	いいえ	いいえ
アドバンスト	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

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

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

オペレーティングシステム	CITRIX 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

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

ライセンス

NetScaler Consoleサービスリリース14.1-21.x以降、ライセンスされたVIPの概念は廃止されました。NetScaler Consoleサービスで無制限のVIPが利用可能になりました。VIPライセンスSKUはまもなく販売終了 (EOS) および更新終了 (EOR) となるため、NetScaler Console仮想サーバーライセンスを購入する必要はなくなりました。

NetScaler® Consoleサービスストレージの変更点は以下のとおりです。

- NetScaler ConsoleサービスストレージSKUはまもなく販売終了 (EOS) および更新終了 (EOR) となります。
- NetScaler Consoleサービスストレージのデフォルトのエンタイトルメントは5GBになりました。
- 過去に購入されたNetScaler Consoleサービスストレージは、契約期間が終了するまで有効です。
- 過去に購入されたNetScaler Console VIPライセンスで、NetScaler Consoleサービスストレージの比例的なエンタイトルメントが付与されていたものは、契約期間が終了するまで有効です。
- より高いNetScaler Consoleストレージエンタイトルメントが付与される別のパッケージを購入した場合、デフォルトの5GBは、そのエンタイトルメントに合わせて変更されます。

注:

以前に仮想サーバーを購入した場合、サブスクリプション期間が終了するまで、仮想サーバーあたり500MBのストレージが適用されます。

NetScaler Console機能に必要なNetScalerライセンス

次の表に、NetScaler Consoleの一部の機能を使用するために必要なNetScalerライセンスを示します。

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

NETSCALER CONSOLE機能グループ	NETSCALER CONSOLE機能	NETSCALERおよびGATEWAYライセンス要件
アナリティクス	HDXインサイト	Advanced (レポート作成 < 1時間) Premium (レポート作成 = 無制限)
アナリティクス	セキュリティインサイト	Premium (または) App Firewall ライセンス付き Advanced
アナリティクス	ゲートウェイインサイト	Advanced (レポート作成 < 1時間) Premium (レポート作成 = 無制限)
アプリケーション	アプリケーション統計 (App Dashboard、App Security Dashboard)	App Dashboard および App Security Dashboard の NetScaler Web App Firewall 関連情報には、Premium (または) App Firewall ライセンス付き Advanced が必要です。
アプリケーション	APIゲートウェイ	Premium (または) Advanced ライセンス
アプリケーション	StyleBook	N/A
アプリケーション	インベントリ管理 – インフラストラクチャダッシュボード、インスタンスグループ、インスタンスダッシュボード、サイト	N/A
アプリケーション	イベント管理とSyslog	N/A
アプリケーション	構成ジョブ、構成監査、構成アドバイス	N/A
アプリケーション	ネットワークレポート (インスタンスレベル)	N/A

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

NETSCALER CONSOLE機能グループ	NETSCALER CONSOLE機能	NETSCALERおよびGATEWAYライセンス要件
アプリケーション	ネットワークレポート (仮想サーバーレベル)	N/A
アプリケーション	ネットワーク機能 (仮想サーバー、サービス、サービスグループ、サーバーの可視化と管理)	N/A
アプリケーション	SSL証明書管理 (インスタンスレベル)	N/A
アプリケーション	SSL証明書管理 (仮想サーバーレベル)	N/A
システム	RBACと外部認証 (インスタンスレベル)	N/A
システム	RBACおよび外部認証 (仮想サーバーレベル)	該当なし

仮想サーバーサブスクリプションの有効期限チェックを表示

NetScaler Consoleで、インストールされているライセンスのステータスを、有効期限とライセンスに許可されているストレージ制限とともに表示できます。

ライセンスのステータスを表示するには:

1. **Settings > Analytics Configuration** に移動します。
2. **Entitlements** セクションで、次の詳細を表示できます。
   - **付与されたストレージ:** ライセンスのストレージ制限。
   - **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残り日数。

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

仮想サーバーで有効になっている分析の種類を表示

選択した仮想サーバーでAppFlow®を有効にした後、**Subscriptions** ページから、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で有効になっている分析の種類を表示できます。

1. **Settings > Analytics Configuration** に移動します。
2. **Virtual Server Analytics Summary** セクションで、ライセンスされた仮想サーバーの種類を選択します。
3. ライセンスされた仮想サーバーページには、ライセンスされた仮想サーバーのリストが表示されます。このページでは、**Analytics Status** 列に、仮想サーバーで有効になっている分析の種類が表示されます。

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

アップグレードアドバイザリ

ネットワーク管理者として、NetScaler Consoleでさまざまなリリースを実行している多数のNetScalerインスタンスを管理している場合があります。各NetScalerインスタンスのライフサイクルを監視するの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、サポート終了 (EOL) またはメンテナンス終了 (EOM) に達している、または達したNetScalerインスタンスを特定する必要があります。その後、アップグレードを計画します。

このプロセスを容易にするために、NetScaler Consoleのアップグレードアドバイザリは、次の方法でNetScalerインスタンスのライフサイクルを監視するのに役立ちます。

- EOLまたはEOMに達している、または達したインスタンスを特定します。これにより、EOLまたはEOMの日付より前にNetScalerのアップグレードを計画できます。
- 最新のリリースまたはビルドではないインスタンスを強調表示します。これらのインスタンスを最新のリリースまたはビルドにアップグレードできます。このアップグレードにより、新機能と修正された問題に関する更新を受け取ることができます。
- 推奨されるNetScalerビルドではないインスタンスを強調表示します。一部の組織では、インスタンスに推奨されるNetScalerビルドがある場合があります。NetScaler Consoleでは、ビルドの安定性、機能、その他の考慮事項に応じて、組織の推奨ビルドを設定できます。その後、推奨ビルドではないインスタンスを確認してアップグレードします。推奨ビルドを実行しているインスタンスは、星のアイコンで示されます。
- 最も人気のあるリリースまたはビルドで実行されているインスタンスを強調表示します。人気のあるビルドを実行しているインスタンスは、リボンアイコンで示されます。

アップグレードアドバイザリは、対応するリリースノートへのリンクを提供します。この情報を使用して、アップグレードするNetScalerビルドを確認し、決定できます。アップグレードアドバイザリページからNetScalerインスタンスをアップグレードするためのメンテナンスジョブの作成に進むことができます。

重要

アップグレードアドバイザリは、NetScalerソフトウェアリリースのEOLのみを監視します。NetScalerアプライアンスのEOLはチェックしません。

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

アップグレードアドバイザリを表示

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。

- NetScalerインスタンスの総数。
- サポート終了に達しているインスタンス。
- メンテナンス終了に達しているインスタンス。
- 古いビルドのインスタンス。
- 推奨ビルドではないインスタンス。
- さまざまなNetScalerリリースにおけるサポート終了 (EOL) およびメンテナンス終了 (EOM) 日付。

アップグレードアドバイザリページ(/en-us/netscaler-console-service/media/uprade-advisory-page.png)

「**アップグレードアドバイザリ**」ページには、NetScalerインスタンスがリリースごとにグループ化されています。「**リリースノート**」リンクは、特定のNetScalerリリースノートに誘導します。アップグレードを決定する前に、新機能、修正点、既知の問題を確認してください。複数の異なるリリースのNetScalerインスタンスを一度に選択してアップグレードできます。アップグレードを進めると、アップグレードジョブが作成されます。参照: NetScalerインスタンスのアップグレード。

推奨ビルドを設定する

管理者として、組織の推奨NetScalerビルドを定義できます。推奨ビルドを設定するには、次の手順を実行します。

1. **インフラストラクチャ > インスタンスアドバイザリ > アップグレードアドバイザリ**で、**設定**をクリックします。
2. 推奨リリースとビルドを選択します。

   推奨ビルドを設定する(/en-us/netscaler-console-service/media/set-preferred-build.png)

   この例では、推奨ビルドは`13.0-58.30`と`13.0-67.39`です。
3. **保存**をクリックします。

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

NetScalerインスタンスをアップグレードする

「**アップグレードアドバイザリ**」ページで、確認後、必要なNetScalerインスタンスをアップグレードするには、次の手順を実行します。

1. アップグレードするインスタンスビルドを選択し、「**アップグレードするインスタンスを選択**」をクリックします。
2. アップグレードするNetScalerインスタンスを選択し、**アップグレードワークフローに進む**をクリックします。

   アップグレードワークフロー(/en-us/netscaler-console-service/media/upgrade-workflow.png)

   このワークフローはアップグレードジョブを作成します。
3. **インスタンスの選択**タブで、,

   a. アップグレードジョブの名前を指定します。

   b. (オプション) 他のインスタンスを追加する場合は、**インスタンスの追加**をクリックします。

   c. **次へ**をクリックします。
4. **イメージの選択**タブで、イメージライブラリ、ローカル、またはアプライアンスからNetScalerイメージを選択します。

   - **イメージライブラリから選択**: リストからNetScalerイメージを選択します。このオプションには、NetScalerダウンロードWebサイトで利用可能なすべてのNetScalerイメージが表示されます。

     NetScalerイメージ(/en-us/netscaler-console-service/media/adc-images.png)

     NetScalerソフトウェアイメージには、星アイコンで推奨ビルドが表示されます。また、ブックマークアイコンで最もダウンロードされたビルドが表示されます。
   - **ローカルまたはアプライアンスから選択**: ローカルコンピューターまたはNetScalerアプライアンスからイメージをアップロードできます。NetScalerアプライアンスを選択すると、NetScaler Console GUIに`/var/mps/mps_images`にあるインスタンスファイルが表示されます。NetScaler Console GUIからイメージを選択します。
   - **選択したイメージがすでに利用可能な場合は、NetScalerへのイメージアップロードをスキップする** - このオプションは、選択したイメージがNetScalerで利用可能かどうかを確認します。アップグレードジョブは新しいイメージのアップロードをスキップし、NetScalerで利用可能なイメージを使用します。

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

- **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップする** - このオプションは、インスタンスのアップグレード後にNetScalerインスタンス内のアップロードされたイメージをクリアします。

次へをクリックして、選択したインスタンスのアップグレード前検証を開始します。

5. 「**アップグレード前検証**」タブには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**」をクリックできます。

   - 「**ディスク容量チェック**」: インスタンスでディスク容量が不足している場合、ディスク容量を確認してクリーンアップできます。参照: NetScaler のディスク容量をクリーンアップする。
   - 「**ポリシーチェック**」: NetScaler Console がサポートされていないクラシックポリシーを検出した場合、そのようなポリシーを削除してアップグレードジョブを作成できます。

   「

   注:

   」.

   クラスターIPアドレスを指定した場合、NetScaler Console は指定されたインスタンスに対してのみアップグレード前検証を実行し、他のクラスターノードに対しては実行しません。

6. オプション: 「**カスタムスクリプト**」タブで、インスタンスのアップグレード前後に実行するスクリプトを指定します。

   詳細については、カスタムスクリプトの使用を参照してください。

7. 「**タスクのスケジュール**」で、次のいずれかのオプションを選択します。

   - 「**今すぐアップグレード**」 - アップグレードジョブはすぐに実行されます。
   - 「**後でスケジュール**」 - この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したいときに「**実行日**」と「**開始時刻**」を指定します。

   NetScaler 高可用性ペアを2段階でアップグレードしたい場合は、「HAノードの2段階アップグレードを実行」を選択します。

   詳細については、NetScaler 高可用性ペアのアップグレードを参照してください。

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

8. 「**ジョブの作成**」タブで、次の詳細を指定します。

   アップグレードジョブをスケジュールする場合、インスタンスにイメージをアップロードするタイミングを指定できます。

   - **今すぐアップロード**: このオプションを選択すると、イメージがすぐにアップロードされます。ただし、アップグレードジョブはスケジュールされた時間に実行されます。
   - **実行時にアップロード**: このオプションを選択すると、アップグレードジョブの実行時にイメージがアップロードされます。

その他のオプションの詳細については、NetScaler アップグレードオプションを参照してください。

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

セキュリティアドバイザリ

安全でセキュア、かつ回復力のあるインフラストラクチャは、あらゆる組織にとって生命線です。組織は、新しい共通脆弱性識別子 (CVE) を追跡し、インフラストラクチャに対する CVE の影響を評価する必要があります。また、脆弱性を解決するための修復策を理解し、計画する必要もあります。

NetScaler Console のセキュリティアドバイザリ機能を使用すると、次のことが可能になります。

- NetScaler の構成設定を分析して、システムを攻撃にさらす可能性のある設定ミス、弱点、またはベストプラクティスからの逸脱を特定します。
- 新しい共通脆弱性識別子 (CVE) を追跡し、CVE の影響を評価し、修復策を理解し、脆弱性を解決します。
- NetScaler ビルドファイルの整合性を検査します。

セキュリティアドバイザリのランディングページ

セキュリティアドバイザリのランディングページでは、NetScaler 展開のセキュリティ体制を包括的に鳥瞰できます。このインターフェイスは、管理者とセキュリティ専門家が NetScaler インフラストラクチャの全体的な健全性と脆弱性ステータスを即座に把握できるように強化および設計されています。

NetScaler Console は、次の 3 種類のセキュリティアドバイザリを提供します。

- **セキュアな構成の推奨事項** - ベストプラクティスに従って NetScaler インスタンスを構成できます。
- **共通脆弱性識別子 (CVE) の検出** - NetScaler インスタンスを危険にさらしている CVE を特定し、修復策を推奨します。
- **ファイル整合性監視** - NetScaler ビルドファイルに変更や追加が行われたかどうかを特定できます。

Citrix Cloud 通知の画像(/en-us/netscaler-console-service/media/security-advisory-dashboard.png)

NetScaler Console のセキュリティアドバイザリダッシュボードには、次のものも含まれます。

- **全体的なセキュリティ体制の重大度** - セキュリティ体制のステータスを表し、3 種類のアドバイザリの最大重大度に基づいて計算されます。ステータスは次のいずれかになります。

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

  - **緊急**: 複数の緊急度の高い観測結果が検出され、最も高い緊急度で対処する必要があります。
  - **高**: 直ちに修正する必要がある重大な脆弱性または誤設定が検出されました。緊急の発見ほど緊急ではありませんが、これらの問題はセキュリティと安定性に重大なリスクをもたらします。
  - **中**: タイムリーに対処する必要がある重要なセキュリティ上の観測結果。これらの問題は、差し迫った重大な脅威をもたらすものではありませんが、対処せずに放置すると、悪用されたり、より深刻な問題につながる可能性があります。
  - **低**: 重大なセキュリティリスクをもたらさない軽微なセキュリティ問題またはベストプラクティス違反。これらは差し迫った脅威ではありませんが、全体的なセキュリティ体制を改善するためにこれらの問題を修正することをお勧めします。

- **最終スキャン** - 最終スキャンの日付。ダッシュボードに表示されるデータは、最終スキャンの結果に基づいています。
- **次回のスケジュール済みスキャン** - 次回のスケジュール済みシステムスキャンの日付。
- **スケジュール済みスキャン頻度** - システムスキャンが実行される頻度。
- **今すぐスキャン** - システムスキャンのスケジュール外で、必要に応じていつでもインスタンスをスキャンできるオンデマンドスキャンを許可します。
- **スキャン履歴** - NetScalerインスタンスで実行されたすべてのスキャンの履歴ビューを提供します。
- **影響を受けるNetScaler** - 影響を受けるNetScalerインスタンスを一覧表示します。
- **設定** - 必要に応じて、システムスキャン設定を構成し、イベントの通知を設定できます。

ダッシュボードで利用可能な情報により、重大な脆弱性、緩和策を含む安全な構成の推奨事項、および関連ドキュメントへのリンクを迅速に特定できます。

ランディングページでは、重要度とNetScaler IPアドレスで問題をフィルタリングできます。特定の重要度レベルが選択されている場合、その重要度レベルのNetScalerインスタンスのみが表示されます。

重要:

セキュリティアドバイザリのGUIまたはレポートでは、すべてのCVEが表示されない場合があり、1つのCVEしか表示されない場合があります。回避策として、**今すぐスキャン**をクリックし、**CVE**を選択してオンデマンドスキャンを実行します。スキャンが完了すると、対象となるすべてのCVE（約15個）がUIまたはレポートに表示されます。-->

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

セキュア構成の推奨事項

セキュア構成の推奨事項タブでは、構成の観測結果について詳細なインスタンスレベルの分析が提供され、ユーザーが実用的なインサイトを得られるように設計されています。詳細については、「セキュア構成の推奨事項」(/ja-jp/netscaler-console-service/instance-advisory/secure-configuration-recommendations.html)を参照してください。

CVE検出

CVE検出は、主にセキュリティ脆弱性の特定と軽減に焦点を当てています。詳細については、「CVE検出」(/ja-jp/netscaler-console-service/instance-advisory/cve-detection.html)を参照してください。

ファイル整合性監視

ファイル整合性監視は、NetScalerインスタンスのコアファイルに対する不正または悪意のある変更をチェックします。これはセキュリティアドバイザリの重要な部分です。詳細については、「ファイル整合性監視」(/ja-jp/netscaler-console-service/instance-advisory/file-integrity-monitoring.html)を参照してください。

今すぐスキャン

必要に応じていつでもインスタンスをスキャンでき、セキュリティ要件に基づいて実行するスキャンの種類を選択することもできます。

スキャンを実行するには、次の手順を実行します。

1. をクリックします。

2. 実行するスキャンの種類を選択します。

   - セキュリティ構成の推奨事項
   - CVE検出
   - ファイル整合性監視

3. 「**今すぐスキャン**」をクリックします。スキャンが完了すると、更新されたセキュリティの詳細がセキュリティアドバイザリダッシュボードに表示されます。

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

スキャン履歴

「**スキャン履歴**」をクリックすると、NetScalerインスタンスで実行されたすべての過去のスキャンを表示できます。

スキャンの種類（オンデマンドスキャンまたはシステムスキャン）、スキャンの開始時刻と終了時刻、全体のスキャンステータスを表示でき、各スキャンの詳細をCSVまたはPDF形式でダウンロードすることもできます。

影響を受けるNetScaler

「**影響を受けるNetScaler**」セクションには、セキュリティ構成、CVE、およびファイル整合性監視チェックによって影響を受けるすべてのNetScalerインスタンスが一覧表示されます。

「**セキュリティ推奨構成**」、「**CVE検出**」、または「**ファイル整合性監視**」の下の数字をクリックして、詳細を表示することもできます。以下は参考用のサンプル画像です。

設定

管理者として、CVEによって脆弱なNetScalerインスタンスの数を示すCitrix Cloud通知を受け取ることができます。通知を受け取るタイミングと方法を設定するには、セキュリティアドバイザリページの右上隅にある設定アイコンをクリックします。

次のアクションを実行できます。

- 通知を受け取るイベントの種類を選択します。
- 通知の受信方法を選択します。たとえば、メール、Slack、PagerDuty などです。
- システムスキャンに含めるスキャンの種類を選択します。デフォルトでは、システムスキャンに対してCVEスキャンのみが有効になっています。
- セキュリティアドバイザリのカスタムスキャンをオプトアウトします。

システムスキャンに含めるスキャンの種類を設定することもできます。

Citrix Cloud通知(/en-us/netscaler-console-service/media/secuirty-advisory-settings.png)

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

免責事項:

NetScalerファイル整合性監視（「本機能」）は、脅威アクターが関連環境を標的とする際に使用する可能性のあるすべての手法、戦術、または手順（TTP）を検出できるわけではないことにご注意ください。脅威アクターはTTPとインフラストラクチャを頻繁に変更するため、本機能は特定の脅威に関して法医学的価値が限定的であるか、まったくない場合があります。あらゆる可能性のある脅威に関連して環境を評価するために、経験豊富な法医学調査員のサービスを保持することを強くお勧めします。

本ドキュメントおよびその中に含まれる情報は現状有姿で提供されます。Cloud Software Group, Inc.は、本ドキュメントまたはその内容に関して、明示的か黙示的かを問わず、本ドキュメントまたはその中に含まれる情報がエラーフリーであること、または商品性や特定の目的への適合性のいかなる条件も満たすことを含め、いかなる保証または表明も行いません。

セキュアな構成の推奨事項

NetScalerのセキュアな構成アドバイザリは、NetScaler構成のセキュリティ体制を強化するための専門的な推奨事項と具体的な指示を提供する包括的なガイドとして機能します。この機能を使用すると、潜在的な脆弱性や進化するサイバー脅威からアプリケーションデリバリーコントローラ (ADC) インフラストラクチャを保護できます。推奨されるガイドラインを綿密に遵守することで、リスクを積極的に軽減し、システムの回復力を高め、不正アクセスや悪意のある活動に対する堅牢な防御を維持できます。

この機能は、NetScaler構成の潜在的な脆弱性をスキャンするだけでなく、それらの構成を修正するための正確なコマンドを積極的に提案します。ネットワーク管理者は、セキュリティギャップを迅速に特定し、NetScalerの展開を強化するために必要な変更を実装できます。

「**セキュアな構成の推奨事項**」タブは、潜在的な構成の脆弱性に対処するための優先順位付けされたアプローチを可能にするため、重要度別に細心の注意を払って分類された包括的なビューを提供します。

重要度に基づく優先順位付け

重要度による分類により、ユーザーは効率的に作業を割り当てることができます。観測結果は通常、次のような階層に分類されます。

- **重大**: NetScalerインスタンスのセキュリティと整合性に即座に重大なリスクをもたらす問題。これらの問題は、最優先で対処する必要があります。

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

- **高**: 悪用された場合、重大なセキュリティ侵害につながる可能性のある構成であり、迅速な対応が必要です。
- **中**: 潜在的な弱点や誤った構成を示す観測結果。これらの問題は重大ではありませんが、対処されないまま放置されると、より大規模なセキュリティインシデントにつながる可能性があります。
- **低**: 全体的なセキュリティ体制を改善するための軽微な推奨事項またはベストプラクティス。これらの問題は、差し迫った脅威を表すものではありません。

詳細なインスタンスレベルビューの利点

- **ターゲットを絞った修復**: 一般的なアドバイスではなく、各NetScalerインスタンスに合わせた具体的な推奨事項がユーザーに提供され、正確で効果的な修復が保証されます。
- **攻撃対象領域の削減**: 観測された誤った構成に体系的に対処することで、組織は攻撃対象領域を大幅に削減し、悪用が成功する可能性を最小限に抑えることができます。
- **コンプライアンス遵守**: 詳細な観測結果は、組織が規制コンプライアンス標準 (例: GDPR、HIPAA、PCI DSS) に違反する可能性のある構成を特定し、修正するのに役立ちます。
- **セキュリティ体制の改善**: 構成の弱点を積極的に特定して解決することで、全体的なセキュリティ体制が強化され、サイバー脅威に対する回復力が高まります。
- **運用効率**：明確で実用的な洞察を提供することで、システムはセキュリティ修復プロセスを効率化し、時間とリソースを節約します。

優先順位、リスク許容度、利用可能なリソースに基づいて、どの観測結果に最初に対処するかを**選択できます**。この柔軟性により、最も差し迫ったセキュリティ上の懸念が遅滞なく対処されると同時に、時間の経過とともに包括的な構成強化を達成するために必要な情報が提供されます。このオプションにより、セキュリティ管理者は情報に基づいた意思決定を行い、NetScalerの展開を保護するための断固たる行動を取ることができます。

フリーテキスト検索機能を使用すると、さまざまな主要な識別子に基づいて結果を絞り込むことができます。たとえば、一意のホスト名でインスタンスを効率的に検索でき、特定のデバイスを特定する直接的な方法を提供します。あるいは、IPアドレスで検索すると、インスタンスを特定する別の正確な方法が提供され、特にネットワーク中心の環境で役立ちます。

基本的な識別を超えて、検索はNetScalerモデルによるフィルタリングもサポートしています。これにより、MPX、SDX、VPXなどのモデルを指定して、特定のハードウェアまたはソフトウェアカテゴリに属するインスタンスのみを表示できます。また、重要度レベルで検索を絞り込むこともでき、情報アラートから重大な警告まで、インスタンスの重要度に基づいて優先順位を付けることができます。

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

構成の推奨事項を修正する

構成の観測結果を評価し、どれがアクションを必要とするかを決定すると、推奨される構成の包括的なビューが表示されます。その後、システムは次の画像に示すように専用ページを表示し、選択内容に合わせて調整された修復手順を表示します。たとえば、特定のNetScalerインスタンス（この特定のシナリオではIPアドレス10.102.56.45のインスタンス）の重大な問題のみに対処することを選択した場合、ページには関連する優先度の高い推奨事項が動的に表示され、修復プロセスを効果的にガイドします。

構成の推奨事項は、次の2つのタイプに分類できます。

- **ユーザー入力が必要な推奨事項**：このカテゴリには、NetScaler管理者またはセキュリティチームからの特定の状況に応じた情報または決定を必要とする構成の提案が含まれます。これらは通常、一般的なデフォルト値が適切でない場合、または最適な設定が独自の運用環境、セキュリティポリシー、またはアプリケーション要件に依存する場合のシナリオです。以下にいくつかの推奨事項の例を示します。
    - **特定のIPアドレスまたはIP範囲の定義**：たとえば、信頼できる内部サブネットまたは特定のクライアントIPアドレスからのトラフィックのみを許可するようにファイアウォールルールを構成します。システムはこれらの固有のネットワーク詳細を推測できません。
    - **カスタムポート番号の設定**：多くのサービスには標準ポートが存在しますが、アプリケーションはセキュリティまたは運用上の理由から非デフォルトポートを使用するように構成されている場合があります。ネットワーク管理者はポート番号を指定する必要があります。
    - **ホスト名またはドメイン名の指定**：SSL証明書、ロードバランシング仮想サーバー、またはコンテンツスイッチングポリシーを構成する場合、NetScalerインスタンスが提供または対話する正確なホスト名またはドメイン名をユーザーが指定する必要があります。
    - **認証サーバーの詳細の提供**：NetScalerをLDAP、RADIUS、SAML、OAuthなどの外部認証システムと統合するには、ユーザーがサーバーのIPアドレス、共有シークレット、ディレクトリパス、およびその他のプロトコル固有の詳細を入力する必要があります。
    - **特定のURL書き換えまたはコンテンツスイッチングポリシーの設定**: これらの高度な機能の正確なURL、パターン、およびターゲット宛先は、アプリケーションアーキテクチャに非常に固有のものであり、ユーザーが定義する必要があります。
    - **影響**: これらの推奨事項は、多くの場合、デプロイメントの特定のニーズ、セキュリティポリシー、およびネットワークトポロジに関するより深い理解を必要とします。ユーザー入力のエラーは、サービスの中断やセキュリティの脆弱性につながる可能性があり、慎重な

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

計画と検証の必要性を強調しています。これらを実装する自動ツールまたはスクリプトは、通常、必要なパラメータを要求するか、構成ファイルから読み取ります。

- **ユーザー入力を必要としない推奨事項**: このカテゴリには、普遍的に適用できる構成の提案や、固有の環境変数に依存しない標準的なベストプラクティスが含まれます。これらは、ほとんどのNetScalerデプロイメントで有益な、基盤となるセキュリティ強化またはパフォーマンス最適化であることがよくあります。以下にいくつかの推奨事項の例を示します。
  - **脆弱な暗号またはプロトコルの無効化**: SSLv3やTLS 1.0などのSSL/TLSバージョン、または特定の脆弱な暗号スイート（例：RC4、3DES）を無効にすることをお勧めします。これらは既知の脆弱性であり、それらを削除することは普遍的なセキュリティのベストプラクティスです。システムは、どの暗号が脆弱であるかを知るために特定の入力を必要としません。
  - **HTTP Strict Transport Security (HSTS) の有効化**: これは、Webブラウザによって適用されるポリシーであり、安全なHTTPS接続を使用してのみサーバーとやり取りします。これを有効にすることは、標準的なセキュリティ強化手順です。
  - **セキュアなCookieフラグの設定（例：`Secure`、`HttpOnly`）**: これらのフラグはセッションCookieのセキュリティを強化し、暗号化されていないチャネルを介して送信されたり、クライアントサイドスクリプトを介してアクセスされたりするのを防ぎます。その適用は一般的な推奨事項です。
  - **一般的なセキュリティヘッダーの有効化**: X-Frame-Options、X-Content-Type-Options、Content-Security-Policy（デフォルトの安全なポリシーを使用）などのヘッダーは、クライアントサイドのセキュリティを普遍的に向上させるため、特定のユーザー入力なしで推奨できます。
  - **一般的な攻撃に対するデフォルトのレート制限の実装**: カスタムレート制限には入力が必要な場合がありますが、一般的な攻撃ベクトル（例：過剰なログイン失敗試行）に一般的なレート制限を適用する推奨事項は、ベースラインとして適用できる場合があります。
  - **最適なバッファサイズまたはタイムアウトの構成**: 特定のアプリケーションロジックではなく、システムアーキテクチャによって決定される内部バッファサイズまたは接続タイムアウトに関連する一般的なパフォーマンス推奨事項。
  - **セキュリティイベントの適切なログレベルの確保**: セキュリティ関連イベントの特定のログレベルを確保するための推奨事項は、監査およびインシデント対応のための一般的なベストプラクティスです。
- **影響**: これらの推奨事項は、多くの場合、自動化またはベースライン構成スクリプトの優れた候補となります。特定の詳細について手動での介入を必要とせずに、複数のNetScalerインスタ

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

ンスに均一に適用できるためです。これらは、一般的な脆弱性に対処し、広く受け入れられている標準を適用することで、強力なセキュリティ体制に貢献します。

要約すると、ユーザー入力要件に基づいて構成推奨事項を分類することで、実装プロセスが効率化されます。入力が必要な推奨事項は、ユーザーからの慎重なデータ収集と検証を必要としますが、入力が不要な推奨事項は、標準的なセキュリティベースラインとして、または自動デプロイメントメカニズムを通じて適用できることがよくあります。

ユーザーが対処する構成を決定すると、既存の構成ジョブワークフローが引き継ぎ、構成変更をプッシュします。

例えば、ユーザー入力を必要とする構成推奨事項の例を次に示します。構成値は1つずつ入力することも、次の図に示すように構成値を含むファイルをアップロードすることもできます。

構成ジョブの作成(/en-us/netscaler-console-service/media/create-config-job.png)

CVE検出

NetScalerは、インスタンスのバージョン、構成、およびシステムファイルをスキャンして脆弱性を特定することにより、CVEを検出します。更新されたCVEリポジトリを使用し、詳細な影響分析と修復の提案を提供します。

セキュリティアドバイザリダッシュボードの**CVE検出**セクションには、次の情報が一覧表示されます。

- 検出されたCVEの数
- 影響を受けるNetScalerインスタンスの数
- 最終スキャン実行日
- 重大度（緊急、高、中、低）別に分類された、影響を受けるNetScalerインスタンス

管理者として、NetScalerに定期的にスケジュールされたシステムスキャンを実行させることも、必要に応じてオンデマンドスキャンを実行することもできます。

- **システムスキャン** - デフォルトですべての管理対象インスタンスをスキャンします。NetScaler Consoleがシステムスキャンの日時を決定するため、変更することはできません。
- **オンデマンドスキャン** - 必要に応じてインスタンスを手動でスキャンできます。前回のシステムスキャンからかなりの時間が経過している場合は、オンデマンドスキャンを実行して現在のセキュリティ体制を評価できます。または、修復が適用された後にスキャンを実行して、改訂

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

された体制を評価します。オンデマンドスキャンを実行するには、セキュリティアドバイザリで**今すぐスキャン**をクリックします。

CVE検出セクションをクリックすると、詳細情報を表示できます。

CVE検出セクションには、次の2つのビューがあります。

- インスタンスビュー
- CVEビュー

インスタンスビュー

インスタンスビューには、**影響を受けるインスタンス**タブと**CVEリポジトリ**タブが含まれています。

影響を受けるインスタンスタブには、影響を受けるNetScalerインスタンスのリストが表示されます。

影響を受けるインスタンスは、以下のフォームファクターに基づいて分類されます。

- MPXおよびVPX
- SDX
- CPX
- BLX

以下の条件に基づいてインスタンスを検索することもできます。

- 検出されたCVE
- ホスト名
- モデル
- NetScalerインスタンス
- 状態

この表には、以下の詳細が表示されます。

- NetScaler IPアドレス
- ホスト名
- NetScalerモデル番号

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

- NetScalerの状態
- ソフトウェアのバージョンとビルド
- NetScalerに影響を与えるCVEのリスト。

ほとんどのCVEは修復としてアップグレードが必要ですが、アップグレードと追加の手順が必要なCVEもあります。

- CVE-2020-8300の修復については、CVE-2020-8300の脆弱性を修復するを参照してください。
- CVE-2021-22927およびCVE-2021-22920については、CVE-2021-22927およびCVE-2021-22920の脆弱性を修復するを参照してください。
- CVE CVE-2021-22956については、CVE-2021-22956の脆弱性を特定して修復する
- CVE CVE-2022-27509については、CVE-2022-27509の脆弱性を修復する

> **注**
>
> NetScalerインスタンスにカスタマイズがある場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

脆弱なNetScalerインスタンスを、修正プログラムが適用されたリリースおよびビルドにアップグレードできます。アップグレードするには、次のいずれかを実行します。

- **アップグレードワークフロー** - インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。
- **構成ジョブワークフロー** - インスタンスを選択し、**構成ジョブワークフロー**をクリックします。

アップグレードワークフローが開始され、脆弱なNetScalerがターゲットNetScalerとして自動入力されます。NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「ジョブを使用してNetScalerインスタンスをアップグレードする」を参照してください。

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

注記:

- リリース13.0、12.1、12.0、11.0、10.5、およびそれ以前のバージョンは、すでにサポート終了（EOL）です。NetScalerインスタンスがこれらのリリースのいずれかで実行されている場合は、サポートされているリリースにアップグレードしてください。
- アップグレードするリリースとビルドは、お客様の判断に委ねられます。どのリリースとビルドにセキュリティ修正が含まれているかについては、修復列のアドバイスを参照してください。そして、まだサポート終了に達していない、サポートされているリリースとビルドを適切に選択してください。

CVEビューに切り替えるには、**CVEビューに切り替える**をクリックします。

CVEビュー

CVEビューには、インフラストラクチャに影響を与えるすべてのCVEと、影響を受けるすべてのNetScalerインスタンスの結果が表示され、修復が提案されます。この情報を使用して、セキュリティリスクを修正するための修復を適用できます。

NetScalerインスタンスに影響を与えるCVEの数を示す表には、次の詳細が含まれています。

- **CVE ID**: インスタンスに影響を与えるCVEのID。
- **公開日**: そのCVEのセキュリティ速報がリリースされた日付。
- **深刻度スコア**: 深刻度の種類（高/中/クリティカル）とスコア。スコアを表示するには、深刻度の種類にカーソルを合わせます。
- **脆弱性の種類**: このCVEの脆弱性の種類。
- **影響を受けるNetScalerインスタンス**: CVE IDが影響を与えているインスタンスの数。ホバーすると、NetScalerインスタンスのリストが表示されます。
- **修復**: 利用可能な修復策。通常はインスタンスのアップグレード、または構成パックの適用です。

同じインスタンスが複数のCVEの影響を受ける可能性があります。この表は、特定の1つのCVEまたは複数選択されたCVEがいくつのインスタンスに影響を与えているかを確認するのに役立ちます。影響を受けるインスタンスのIPアドレスを確認するには、**影響を受けるNetScalerインスタンス**の下にあるNetScalerの詳細にカーソルを合わせます。影響を受けるインスタンスの詳細を確認するには、表の下部にある**影響を受けるインスタンスを表示**をクリックします。 プラス記号をクリックして、表の列を追加または削除することもできます。

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

CVEリポジトリ

インスタンスビューとCVEビューの両方に、**CVEリポジトリ**タブが含まれています。このタブには、2019年12月以降にCitrixが発表した、NetScalerインフラストラクチャに影響を与える可能性のあるすべてのNetScaler関連CVEの詳細が表示されます。

- CVE ID
- 脆弱性の種類
- 公開日
- 重大度レベル
- 修復
- セキュリティ速報へのリンク

CVEリポジトリタブ(/en-us/netscaler-console-service/media/cve-repository-tab.png)

このビューを使用して、セキュリティアドバイザリの範囲内のCVEを理解し、CVEについて詳しく知ることができます。サポートされていないCVEについては、「セキュリティアドバイザリでサポートされていないCVE」を参照してください。

注意事項

- セキュリティアドバイザリは、End of Life (EOL) に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。
- CVE検出でサポートされるインスタンス: すべてのNetScaler (SDX、MPX、VPX) およびGateway。
- ファイル整合性監視でサポートされるインスタンス: MPX、VPXインスタンス、およびGateway。
- サポートされるCVE: 2019年12月以降のすべてのCVE。

> **注:**
>
> Windows用NetScaler Gatewayプラグインに影響を与える脆弱性の検出と修復は、NetScaler Consoleセキュリティアドバイザリではサポートされていません。サポートされていないCVEについては、セキュリティアドバイザリでサポートされていないCVEを参照してください。

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

- NetScaler Consoleセキュリティアドバイザリは、脆弱性を特定する際に、いかなる種類の機能の誤設定も考慮しません。
- NetScaler Consoleセキュリティアドバイザリは、CVEの特定と修復のみをサポートします。セキュリティ記事で強調されているセキュリティ上の懸念事項の特定と修復はサポートしていません。
- NetScaler、Gatewayリリースの範囲: この機能はメインビルドに限定されています。セキュリティアドバイザリは、その範囲に特別なビルドを含みません。
    - セキュリティアドバイザリは、Adminパーティションではサポートされていません。
- CVEには、次の種類のスキャンが利用可能です。
    - **バージョン スキャン**: このスキャンでは、NetScaler ConsoleがNetScalerインスタンスのバージョンと、修正が利用可能なバージョンおよびビルドを比較する必要があります。このバージョン比較により、NetScaler Consoleセキュリティアドバイザリは、NetScalerがCVEに対して脆弱であるかどうかを特定するのに役立ちます。たとえば、CVEがNetScalerリリースおよびビルドxx.yyで修正された場合、セキュリティアドバイザリは、xx.yyより低いビルドのすべてのNetScalerインスタンスを脆弱であると見なします。バージョン スキャンは、現在セキュリティアドバイザリでサポートされています。
    - **構成スキャン**: このスキャンでは、NetScaler ConsoleがCVEスキャンに固有のパターンをNetScaler構成ファイル (`nsconf`) と照合する必要があります。特定の構成パターンがNetScaler ns.confファイルに存在する場合、そのインスタンスはそのCVEに対して脆弱であると見なされます。このスキャンは通常、バージョン スキャンと組み合わせて使用されます。 構成スキャンは、現在セキュリティアドバイザリでサポートされています。
    - **カスタム スキャン**: このスキャンでは、NetScaler Consoleが管理対象のNetScalerインスタンスに接続し、スクリプトをプッシュして実行する必要があります。スクリプトの出力は、NetScalerがCVEに対して脆弱であるかどうかをNetScaler Consoleが特定するのに役立ちます。例としては、特定のシェルコマンド出力、特定のCLIコマンド出力、特定のログ、特定のディレクトリまたはファイルの存在または内容などがあります。カスタム スキャンを必要とするCVEの場合、スクリプトはスケジュールされたスキャンまたはオンデマンド スキャンが実行されるたびに実行されます。収集されるデータと特定のカスタム スキャンのオプションの詳細については、そのCVEに関するセキュリティアドバイザリのドキュメントを参照してください。
- スキャンはNetScalerの運用トラフィックに影響を与えず、NetScaler上のいかなるNetScaler構成も変更しません。

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

- NetScaler Consoleセキュリティアドバイザリは CVE緩和をサポートしていません。NetScaler インスタンスに緩和策（一時的な回避策）を適用した場合でも、NetScaler Consoleは、修復が完了するまで、そのNetScalerを脆弱なNetScalerとして識別し続けます。
- FIPSインスタンスの場合、CVEスキャンはサポートされていません。

ファイル整合性監視

ファイル整合性監視を使用すると、NetScalerファイルシステムに変更や追加が行われたかどうかを特定できます。この機能は、現在のNetScalerビルドのバイナリハッシュ値を、同じNetScalerビルドにリンクされている元のバイナリハッシュと比較することで、NetScalerファイルの整合性を評価します。

セキュリティアドバイザリダッシュボードの**ファイル整合性監視**セクションには、次の項目が一覧表示されます。

- 検出された問題の数
- 影響を受けるNetScalerインスタンスの数
- 最終スキャン実行日
- 重大度「緊急」、「高」、「中」、「低」に分類される、影響を受けるNetScalerインスタンス
- バイナリ署名と検証を使用して問題を報告した、影響を受けるNetScalerインスタンス

管理者として、定期的にスケジュールされたシステムスキャンをNetScalerに実行させることができます。または、必要に応じてオンデマンドスキャンを実行することもできます。

- **システムスキャン** - デフォルトですべての管理対象インスタンスをスキャンします。NetScaler Consoleがシステムスキャンの日時を決定し、デフォルトでは無効になっています。
- **オンデマンドスキャン** - 必要に応じて手動でスキャンをトリガーできます。オンデマンドスキャンを実行するには、セキュリティアドバイザリダッシュボードで**今すぐスキャン**をクリックします。

ファイル整合性監視セクションをクリックすると、詳細情報を表示できます。

コンソール検出

コンソール検出タブには、現在のビルドのバイナリハッシュと元のビルドハッシュを比較して、変更または新規追加されたファイルを検出し、影響を受けるNetScalerインスタンスが一覧表示されます。この表には、次の詳細が表示されます。

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

- IPアドレス - 影響を受けるインスタンスのIPアドレスです。
- スキャンステータス - スキャンエラーの結果を表示します。
- 既存ファイルの変更 - 変更された既存ファイルのリストです。
- 新規ファイルの追加 - 追加された新規ファイルのリストです。
- スキャン時間 - 最終スキャン時刻です。
- ホスト名 - 影響を受けるNetScalerのホスト名です。
- モーダル - 影響を受けるNetScalerのモーダル名です。

スキャンエラーの結果はメインダッシュボードビュー内に表示されるため、個々のスキャン結果や項目をクリックしてエラーの詳細にアクセスする必要はありません。ハッシュの不一致やスキャンエラーなどの整合性に関する問題は、ダッシュボード上で明確でアクセスしやすい形式で表示され、問題を迅速に特定し理解するのに役立ちます。

既存ファイルの変更および**新規ファイルの追加**の下にある数字をクリックして、詳細を表示します。

カスタム許可リストを作成し、特定のファイルをファイル整合性監視スキャンから除外できます。スキャンから除外するファイルを定義することで、監視を効率化し、信頼できるファイルに対する不要なアラートを減らすことができます。

ファイル整合性監視スキャンから特定のファイルを除外するには、次の手順を実行します。

1. **ファイル/ディレクトリを除外**をクリックします。
2. 必要なファイルまたはディレクトリを選択します。

   または

   新しいファイルを追加するには、**ファイル/ディレクトリの追加**をクリックします。標準のシェルグロブパターンを追加し、定義された条件に一致するパスを除外できます。ディレクトリが追加されると、そのすべてのファイルはスキャンから除外されます。**追加**をクリックします。

   特定のファイルやフォルダーを見つけるために検索を実行することもできます。`path`オプションの下にある検索バーにファイルまたはフォルダーの一部を入力して、除外リストのパスを見つけることもできます。検索機能により、除外されたパスの管理と確認が容易になります。

ファイルをスキャンから除外したくない場合は、必要なファイルまたはディレクトリを選択し、**ファイル/ディレクトリの削除**をクリックします。指定されたファイルまたはディレクトリは、次回のスケジュールされたスキャンに含まれます。

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

注意事項

- ファイル整合性監視でサポートされているインスタンス: MPX、VPXインスタンス、およびGateway。
- ファイル整合性監視では、次のスキャンが利用可能です。
  - **ファイル整合性監視スキャン**: このスキャンでは、NetScaler Consoleが管理対象のNetScalerインスタンスに接続する必要があります。NetScaler Consoleは、NetScalerでスクリプトを実行し、NetScalerシステムファイルの現在のバイナリハッシュ値を収集することで、ハッシュ値の比較を行います。比較後、NetScaler Consoleは、変更された既存ファイルの総数と新しく追加されたファイルの総数を含む結果を提供します。管理者として、スキャン結果に関するさらなる調査のために、組織のデジタルフォレンジックに連絡することができます。
- サポートされていないプラットフォームのリストは次のとおりです: BLX

デバイスレポート

デバイスレポートタブには、バイナリ署名と検証を使用して問題を報告したNetScalerインスタンスが一覧表示されます。この検証により、各ファイルのデジタル署名が検証され、信頼性が確認され、改ざんが検出されます。影響を受けるインスタンスが見つかった場合は、組織のデジタルフォレンジック活動を進めることができます。この表には、影響を受けたNetScalerインスタンスと、ホスト名、追加されたバイナリ、変更されたバイナリなどのその他の詳細が一覧表示されます。必要なインスタンスに対応する**詳細**をクリックすると、詳細情報を表示できます。

NetScaler Consoleにおける侵害の痕跡の検出

NetScaler Consoleの侵害の痕跡 (IoC) 検出機能は、NetScalerアプライアンスが脆弱性により潜在的に影響を受けているかどうかを検出するように設計されています。

CVEイベントが発生した場合、最初の懸念事項の1つは、悪意のあるアクターがその脆弱性を悪用できたかどうかです。エクスプロイトは顧客のビジネスに壊滅的な損害をもたらすため、そのようなインシデントを直ちに検出することが重要です。過去には、NetScalerの侵害の痕跡はサポートチャネルを通じて配布されていました。これは顧客のニーズを満たすものでしたが、チケットの発行、サポート担当者との会話といったサポートプロセスを経る追加の労力が必要であり、場合によっては理想的ではありませんでした。NetScaler Consoleの侵害の痕跡検出機能は、現在の

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

サポート中心のプロセスを短縮し、顧客がNetScalerインフラストラクチャを迅速に評価するのに役立つように設計されています。

前提条件

この機能を使用するには、製品使用状況テレメトリを送信する必要があります。NetScalerテレメトリの詳細については、`<https://docs.netscaler.com/ja-jp/netscaler-application-delivery-management-software/current-release/ns-telemetry.html>`を参照してください。

利点

- NetScaler Consoleの**セキュリティアドバイザリ**ページから侵害検出スキャンを実行できます。

- スキャンは次のいずれかの結果を提供します。
  - **侵害の可能性あり** – 検出ロジックがCVEに対する潜在的な侵害を検出した場合。
  - **侵害は検出されませんでした** – 検出ロジックが侵害を検出していない場合。
  - **スキップ済み** – 特定のNetScalerインスタンスに対してスキャンが手動でスキップされた場合。
  - **実行に失敗しました** – スキャンが正常に実行されなかった場合。
  - **実行中** – スキャンが進行中の場合。
- より多くのIoCが発見されるにつれて、IoCロジックは更新され続けます。そのような場合、ホームページには更新が利用可能であることが表示されます。
- IoC検出ロジックのアップデートが利用可能になると、ランディングページで確認できます。

  侵害インジケーターダッシュボード(/en-us/netscaler-console-service/media/indicators-of-compromise-dashboard.png)
- 以前のスキャンの結果は保存され、いつでも表示できます。

  侵害インジケーターのドキュメント履歴(/en-us/netscaler-console-service/media/indicators-of-comprimise-scan-history.png)
- このソリューションは、ハブアンドスポークアーキテクチャを使用しており、中央のクラウドサービスが安全なクラウドロケーションからアセットを取り込み、それらをターゲットデバイスにインストールします。

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

注:

IoC情報には、脅威アクターが関連環境を標的とする際に使用する可能性のあるすべての手法、戦術、または手順（「TTP」）が含まれているわけではありません。また、脅威アクターはTTPとインフラストラクチャを頻繁に変更します。これらの理由などにより、IoC情報は法医学的価値が限られており、実際の侵害を特定できない可能性があります。環境を評価するために、経験豊富な法医学調査員のサービスを利用することをお勧めします。

脆弱性の修復

NetScaler は CVE を検出し、それに応じた修正案を提供します。このトピックでは、以下の CVE に対して提案されている修正について説明します。

- CVE-2026-88771 の脆弱性を修正する
- CVE-2026-88772 の脆弱性を修正する
- CVE-2026-88773 の脆弱性を修正する
- CVE-2026-88774 の脆弱性を修正する
- CVE-2026-88775 の脆弱性を修正する
- CVE-2026-88776 の脆弱性を修正する
- CVE-2026-88777 の脆弱性を修正する
- CVE-2026-88778 の脆弱性を修正する
- CVE-2026-19490 の脆弱性を修正する
- CVE-2026-19489 の脆弱性を修正する
- CVE-2026-13474 の脆弱性を修正する
- CVE-2026-10817 の脆弱性を修正する
- CVE-2026-10816 の脆弱性を修正する
- CVE-2026-8655 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-8655.html)
- CVE-2026-8452 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-8452.html)
- CVE-2026-8451 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-8451.html)

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

- CVE-2026-4368 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-4368.html)
- CVE-2026-3055 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-3055.html)
- CVE-2025-12101 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-12101.html)
- CVE-2025-8424 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-8424.html)
- CVE-2025-7776 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-7776.html)
- CVE-2025-7775 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-7775.html)
- CVE-2025-6543 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-6543.html)
- CVE-2025-5349 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-5349.html)
- CVE-2025-5777 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-5777.html)
- CVE-2024-8535 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2024-8535.html)
- CVE-2020-8300 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2020-8300.html)
- CVE-2021-22927 および CVE-2021-22920 の脆弱性を修正する(/ja-jp/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2021-22927-2021-22920.html)
- CVE-2021-22956の脆弱性を特定して修正する
- CVE-2022-27509の脆弱性を特定して修正する

CVE-2026-88771の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88771を検索します。CVE-2026-88771の影響を受けるNetScalerインスタンスのリストが表示されます。

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

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88771の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始してください。

CVE-2026-88771を修正する

CVE-2026-88771の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

CVE-2026-88772の脆弱性を特定し、修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88772を検索します。CVE-2026-88772の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

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

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88772の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始してください。

CVE-2026-88772を修正する

CVE-2026-88772の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

CVE-2026-88773の脆弱性を特定し、修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-88773を検索します。CVE-2026-88773の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

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

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88773の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始してください。

CVE-2026-88773を修正する

CVE-2026-88773の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

CVE-2026-88774の脆弱性を特定して修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-88774を検索します。CVE-2026-88774の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-sepのセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-sep.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88774の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

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

CVE-2026-88774を修正する

CVE-2026-88774の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下で、インスタンスを選択し、**Proceed to upgrade workflow**をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態でアップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

CVE-2026-88775の脆弱性を特定して修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-88775を検索します。CVE-2026-88775の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88775の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

CVE-2026-88775を修正する

CVE-2026-88775の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルド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.

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

CVE-2026-88776の脆弱性を特定し、修復する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-88776を検索します。CVE-2026-88776の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

注：

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88776の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

CVE-2026-88776を修復する

CVE-2026-88776の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

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

CVE-2026-88777の脆弱性を特定し、修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、「**CVE Detection**」をクリックします。「**Impacted Instances**」タブで、CVE-2026-88777を検索します。CVE-2026-88777の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、「」を参照してください。(/ja-jp/netscaler-console-service/instance-advisory/security-advisory-dashboard.html).

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-88777の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**Scan-Now**」をクリックしてオンデマンドスキャンを開始します。

CVE-2026-88777を修正する

CVE-2026-88777の影響を受けるNetScalerインスタンスの場合、修正は1ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、「**CVE Detection > Impacted Instances**」の下で、インスタンスを選択し、「**Proceed to upgrade workflow**」をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態でアップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「」を参照してください。(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html).

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

CVE-2026-88778の脆弱性を修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードの**現在のCVE** `<number of>` **NetScalerインスタンスがCVEの影響を受けています**の下で、CVE-2026-88778によって脆弱になっているすべてのインスタンスを確認できます。CVEの影響を受けているインスタンスの詳細を確認するには、CVE-2026-88778を選択し、**影響を受けるインスタンスを表示**をクリックします。

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

CVE-2026-88778を修正する

CVE-2026-88778の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの**現在のCVE > NetScalerインスタンスがCVEの影響を受けています**の下で、ステップ1と2を確認できます。

2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。

現在のCVE > CVEの影響を受けるNetScalerインスタンスの下に、この2段階の修正プロセスについて、**アップグレードワークフローに進む**と**構成ジョブワークフローに進む**という2つの異なるワークフローが表示されます。

ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブを作成する」を参照してください。

注：

このステップは、脆弱なすべてのNetScalerインスタンスに対して一度に実行できます。

ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、`<number of>` **NetScaler instances impacted by CVEs** ウィンドウで、CVE-2026-88778 の影響を受けるインスタンスを選択し、**Proceed to configuration job workflow** をクリックします。ワークフローには次のステップが含まれます。

1. 構成をカスタマイズする。
2. 自動入力された影響を受けるインスタンスを確認する。

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

3. ジョブの変数に対する入力を指定する。
4. 変数入力が入力された最終構成を確認する。
5. ジョブを実行する。

インスタンスを選択して **Proceed to configuration job workflow** をクリックする前に、次の点に留意してください。

- CVE-2026-88778 のみに影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2026-88778 のみに影響を受けているとします。これらのインスタンスをすべて選択し、**Proceed to configuration job workflow** をクリックすると、組み込みの構成テンプレートが **Select configuration** の下に自動入力されます。

ステップ1：構成を選択する

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが **Select configuration** の下に自動入力されます。

ステップ2：インスタンスを選択する

影響を受けるインスタンスは **Select Instances** の下に自動入力されます。インスタンスを選択します。**Next** をクリックします。次のステップで構成をプレビューします。**Next** をクリックします。

注:

クラスターモードのNetScalerインスタンスの場合、セキュリティアドバイザリを使用して、NetScaler Consoleは、クラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

ステップ 3: 構成を実行する

「**完了**」をクリックして、構成ジョブを実行します。

ジョブの実行後、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、修正されたセキュリティ体制を確認できます。

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

CVE-2026-19490 の脆弱性を特定して修復する

NetScaler Console® のセキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2026-19490 を検索します。CVE-2026-19490 の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-19490 のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-19490.png)

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-19490の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

CVE-2026-19490 を修復する

CVE-2026-19490 の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances** の下でインスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Console を使用してNetScalerインスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、「CVE Detection」を参照してください。

CVE-2026-19489の脆弱性を特定し、修復する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-19489を検索します。CVE-2026-19489の影響を受けるNetScalerインスタンスのリストが表示されます。

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

CVE-2026-19489のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-19489.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-19489の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始してください。

CVE-2026-19489を修復する

CVE-2026-19489の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

CVE-2026-13474 の脆弱性を特定して修復する

NetScaler Console のセキュリティアドバイザリダッシュボードで、**Current CVEs > `<number of>` NetScaler instances are impacted by common vulnerabilities and exposures (CVEs)** の下で、この特定の CVE によって脆弱になっているすべてのインスタンスを確認できます。CVE-2026-13474 の影響を受けるインスタンスの詳細を確認するには、**CVE-2026-13474** を選択し、**View Affected Instances** をクリックします。

`<number of>` **NetScaler instances impacted by CVEs** ウィンドウが表示されます。ここでは、CVE-2026-13474 の影響を受ける NetScaler インスタンスの数と詳細が表示されます。

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

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

CVE-2026-13474 を修復する

CVE-2026-13474 の影響を受ける NetScaler インスタンスの場合、修復は 2 段階のプロセスです。GUI の **Current CVEs > NetScaler instances are impacted by CVEs** の下で、ステップ 1 とステップ 2 を確認できます。

2 つのステップは次のとおりです。

1. 脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。

Current CVEs > NetScaler instances impacted by CVEs の下には、この 2 段階の修復プロセスに対して、**Proceed to upgrade workflow** と **Proceed to configuration job workflow** の 2 つの異なるワークフローが表示されます。

ステップ 1: 影響を受ける NetScaler インスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、NetScaler アップグレードジョブの作成を参照してください。

ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、`<number of>` **CVEの影響を受ける NetScalerインスタンス**ウィンドウで、CVE-2026-13474の影響を受けるインスタンスを選択し、**構成ジョブワークフローに進む**をクリックします。ワークフローには次の手順が含まれます。

1. 構成をカスタマイズする。
2. 自動入力された影響を受けるインスタンスを確認する。
3. ジョブの入力変数を指定する。
4. 変数入力が入力された最終構成を確認する。
5. ジョブを実行する。

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

インスタンスを選択して**構成ジョブワークフローに進む**をクリックする前に、次の点に留意してください。

- CVE-2026-13474のみの影響を受ける複数のNetScalerインスタンスの場合、すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3がCVE-2026-13474のみの影響を受ける場合、これらのインスタンスをすべて選択し、**構成ジョブワークフローに進む**をクリックします。組み込みの構成テンプレートは、**構成の選択**の下に自動入力されます。

ステップ1：構成を選択する

構成ジョブワークフローでは、組み込みの基本構成テンプレートが**構成の選択**の下に自動入力されます。

ステップ2：インスタンスを選択する

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択し、**次へ**をクリックします。次のステップで、構成をプレビューし、**次へ**をクリックします。

注:

クラスターモードのNetScalerインスタンスの場合、セキュリティアドバイザリを使用すると、NetScaler Consoleはクラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

CVE-2026-13474の修復手順(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-2.png)

ステップ3：構成を実行する

構成ジョブを実行するには、**完了**をクリックします。

CVE-2026-13474の修復手順(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-3.png)

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認します。

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

CVE-2026-10817の脆弱性を特定して修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-10817を検索します。CVE-2026-10817の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-10817のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-10817.png)

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-10817の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

CVE-2026-10817を修正する

CVE-2026-10817の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、「CVE Detection」を参照してください。

CVE-2026-10816の脆弱性を特定し、修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-10816を検索します。CVE-2026-10816の影響を受けるNetScalerインスタンスのリストが表示されます。

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

CVE-2026-10816のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-10816.png)

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

注：

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-10816の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始してください。

CVE-2026-10816を修正する

CVE-2026-10816の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

CVE-2026-8655の脆弱性を特定し、修復する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-8655を検索します。CVE-2026-8655の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

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

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-8655の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

CVE-2026-8655を修復する

CVE-2026-8655の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE検出 > 影響を受けるインスタンス**の下で、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

CVE-2026-8452の脆弱性を特定して修正する

NetScaler Console® セキュリティアドバイザリダッシュボードで、「**CVE検出**」をクリックします。「**影響を受けるインスタンス**」タブで、CVE-2026-8452を検索します。CVE-2026-8452の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」(/ja-jp/netscaler-console-service/instance-advisory/security-advisory-dashboard.html)を参照してください。

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

注：

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-8452の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**今すぐスキャン**」をクリックしてオンデマンドスキャンを開始します。

CVE-2026-8452を修正する

CVE-2026-8452の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

GUIで、「**CVE検出 > 影響を受けるインスタンス**」の下でインスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html)を参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE検出を参照してください。

CVE-2026-8451の脆弱性を特定して修正する

NetScaler Console®セキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-8451を検索します。CVE-2026-8451の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

注：

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-8451の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

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

CVE-2026-8451を修正する

CVE-2026-8451の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、Create a NetScaler upgrade jobを参照してください。

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。詳細については、CVE Detectionを参照してください。

CVE-2026-4368の脆弱性を特定し、修正する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE検出**をクリックします。**影響を受けるインスタンス**タブで、CVE-2026-4368を検索します。CVE-2026-4368の影響を受けるNetScalerインスタンスのリストが表示されます。

CVE-2026-4368のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2026-4368.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-4368の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

CVE-2026-4368を修正する

CVE-2026-4368の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルド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.

GUIで、**CVE検出 > 影響を受けるインスタンス**の下でインスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

重要

脆弱なNetScalerインスタンスに/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

CVE-2026-3055の脆弱性を特定し、修復する

NetScaler Console®のセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2026-3055を検索します。CVE-2026-3055の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2026-3055の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始してください。

CVE-2026-3055を修復する

CVE-2026-3055の影響を受けるNetScalerインスタンスの場合、修復は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

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

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

重要

脆弱なNetScalerインスタンスに/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

CVE-2025-12101の脆弱性を特定して修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2025-12101を検索します。CVE-2025-12101の影響を受けるNetScaler®インスタンスのリストが表示されます。

CVE-2025-12101のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2025-12101.png)

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-12101の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

CVE-2025-12101を修正する

CVE-2025-12101の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

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

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

重要

脆弱なNetScalerインスタンスに/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、「Upgrade considerations for customized NetScaler configurations」を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

修正ワークフロー(/en-us/netscaler-console-service/media/remediation-workflow-cve-2025-12101.png)

CVE-2025-8424 の脆弱性を特定して修復する

NetScaler Console のセキュリティアドバイザリダッシュボードで、**CVE Detection** をクリックします。**Impacted Instances** タブで、CVE-2025-8424 を検索します。CVE-2025-8424 の影響を受ける NetScaler インスタンスのリストが表示されます。

CVE-2025-8424 のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2025-8424.png)

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2025-8424 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

CVE-2025-8424 を修復する

CVE-2025-8424 の影響を受ける NetScaler® インスタンスの場合、修復は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

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

GUI で、**CVE Detection > Impacted Instances** の下でインスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

重要

脆弱な NetScaler インスタンスに /etc/httpd.conf ファイルが /nsconfig ディレクトリにコピーされている場合は、NetScaler のアップグレードを計画する前に、「Upgrade considerations for customized NetScaler configurations」を参照してください。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「Create a NetScaler upgrade job」を参照してください。

修復ワークフロー(/en-us/netscaler-console-service/media/remediation-workflow-cve-2025-8424.png)

CVE-2025-7776の脆弱性を特定し、修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2025-7776を検索します。CVE-2025-7776の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-7776の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始してください。

CVE-2025-7776を修正する

CVE-2025-7776の影響を受けるNetScaler®インスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースおよびビルド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.

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

重要

脆弱なNetScalerインスタンスに/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

CVE-2025-7775の脆弱性を特定して修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**CVE Detection**をクリックします。**Impacted Instances**タブで、CVE-2025-7775を検索します。CVE-2025-7775の影響を受けるNetScalerインスタンスのリストが表示されます。

セキュリティアドバイザリダッシュボードの詳細については、「Security Advisory」を参照してください。

注記：

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-7775の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。

CVE-2025-7775を修正する

CVE-2025-7775の影響を受けるNetScaler®インスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。

GUIで、**CVE Detection > Impacted Instances**の下でインスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

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

重要

脆弱なNetScalerインスタンスに/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、「カスタマイズされたNetScaler構成のアップグレードに関する考慮事項」を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

CVE-2025-6543の脆弱性を特定し、修正する

NetScaler Consoleセキュリティアドバイザリダッシュボードの**現在のCVE** `<number of>` **CVEの影響を受けるNetScalerインスタンス**で、CVE-2025-6543によって脆弱なすべてのインスタンスを確認できます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2025-6543を選択し、**影響を受けるインスタンスを表示**をクリックします。

CVE-2025-6543のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2025-6543.png)

注:

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリの**スキャンログ**タブでCSVレポートをダウンロードします。

`<number of>` **CVEの影響を受けるNetScalerインスタンス**ウィンドウが表示されます。次のスクリーンショットでは、CVE-2025-6543の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

CVE-2025-6543の影響を受けるインスタンス(/en-us/netscaler-console-service/media/cve-2025-6543-impacted-instance.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

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

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-6543の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

CVE-2025-6543を修正する

CVE-2025-6543の影響を受けるNetScalerインスタンスの場合、修正は単一ステップのプロセスであり、脆弱なNetScalerインスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUIの**現在のCVE > CVEの影響を受けるNetScalerインスタンス**で、修正手順を確認できます。

現在のCVE > CVEの影響を受けるNetScalerインスタンスで、この単一ステップの修正プロセスとして、次のワークフローが表示されます: **アップグレードワークフローに進む**。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**アップグレードワークフローに進む**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

重要

脆弱なNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、カスタマイズされたNetScaler構成のアップグレードに関する考慮事項を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、NetScalerアップグレードジョブの作成を参照してください。

CVE-2025-5349 の脆弱性を特定して修正する

NetScaler Console のセキュリティアドバイザリダッシュボードの「**現在の CVE** `<number of>` **NetScaler インスタンスが CVE の影響を受けています**」の下で、CVE-2025-5349 によって脆弱になっているすべてのインスタンスを確認できます。CVE の影響を受けるインスタンスの詳細を確認するには、CVE-2025-5349 を選択し、「**影響を受けるインスタンスを表示**」をクリックします。

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

注:

NetScaler の脆弱性の理由を理解するには、セキュリティアドバイザリの「**スキャンログ**」タブで CSV レポートをダウンロードしてください。

「`<number of>` **NetScaler インスタンスが CVE の影響を受けています**」ウィンドウが表示されます。次のスクリーンショットでは、CVE-2025-5349 の影響を受ける NetScaler インスタンスの数と詳細を確認できます。

セキュリティアドバイザリダッシュボードの詳細については、「セキュリティアドバイザリ」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2025-5349 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**今すぐスキャン**」をクリックしてオンデマンドスキャンを開始してください。

CVE-2025-5349 を修正する

CVE-2025-5349 の影響を受ける NetScaler インスタンスの場合、修正は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする必要があります。GUI の「**現在の CVE > NetScaler インスタンスが CVE の影響を受けています**」の下で、修正手順を確認できます。

「**現在の CVE > NetScaler インスタンスが CVE の影響を受けています**」の下に、この単一ステップの修正プロセスである「**アップグレードワークフローに進む**」というワークフローが表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

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

重要

脆弱性のあるNetScalerインスタンスで/etc/httpd.confファイルが/nsconfigディレクトリにコピーされている場合は、NetScalerのアップグレードを計画する前に、「カスタマイズされたNetScaler構成のアップグレードに関する考慮事項」(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html#upgrade-considerations-for-customized-adc-configurations)を参照してください。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html)を参照してください。

CVE-2025-5777の脆弱性を修正する

NetScaler Consoleセキュリティアドバイザリダッシュボードの「**Current CVEs** `<number of>` **NetScaler instances are impacted by CVEs**」で、CVE-2025-5777によって脆弱なすべてのインスタンスを確認できます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2025-5777を選択し、「**View Affected Instances**」をクリックします。

注:

NetScalerの脆弱性の原因を理解するには、セキュリティアドバイザリの「**Scan logs**」タブでCSVレポートをダウンロードしてください。

「`<number of>` **NetScaler instances impacted by CVEs**」ウィンドウが表示されます。以下のスクリーンショットでは、CVE-2025-5777の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

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

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2025-5777の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**Scan-Now**」をクリックしてオンデマンドスキャンを開始してください。

CVE-2025-5777を修正する

CVE-2025-5777の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの「**Current CVEs > NetScaler instances are impacted by CVEs**」で、ステップ1と2を確認できます。

2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正を含むリリースおよびビルドにアップグレードする。
2. 構成ジョブで、カスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用します。

Current CVEs > NetScaler instances impacted by CVEs の下には、この2段階の修復プロセスに2つの異なるワークフローが表示されます。これらは、**Proceed to upgrade workflow** と **Proceed to configuration job workflow** です。

ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「NetScaler アップグレードジョブの作成」を参照してください。

注:

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

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

ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、**`<number of >` NetScaler instances impacted by CVEs** ウィンドウで、CVE-2025-5777 の影響を受けるインスタンスを選択し、**Proceed to configuration job workflow** をクリックします。ワークフローには次の手順が含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの実行。

インスタンスを選択して **Proceed to configuration job workflow** をクリックする前に、次の点に注意してください。

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956、CVE-2025-5777など）の影響を受けるNetScalerインスタンスの場合：インスタンスを選択して **Proceed to configuration job workflow** をクリックしても、**Select configuration** の下に組み込み構成テンプレートが自動入力されません。適切な構成ジョブテンプレートを **Security Advisory Template** の下から右側の構成ジョブペインに手動でドラッグアンドドロップする必要があります。
- CVE-2025-5777 のみに影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2025-5777 のみに影響を受けているとします。これらのインスタンスをすべて選択し、**Proceed to configuration job workflow** をクリックすると、**Select configuration** の下に組み込み構成テンプレートが自動入力されます。
- CVE-2025-5777および1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスがあり、各NetScalerに一度に1つずつ修正を適用する必要がある場合、これらのインスタンスを選択して**Proceed to configuration job workflow**をクリックすると、各NetScalerで一度に1つずつ構成ジョブを実行するように指示するエラーメッセージが表示されます。

ステップ1: 構成の選択

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが**構成の選択**の下に自動入力されます。

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

ステップ2: インスタンスの選択

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択します。このインスタンスがHAペアの一部である場合は、**セカンダリノードで実行**を選択します。**次へ**をクリックします。

注:

セキュリティアドバイザリを使用して、クラスターモードのNetScalerインスタンスの場合、NetScaler Consoleは、クラスター構成コーディネーター（CCO）ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

ステップ3: ジョブの実行

完了をクリックして、構成ジョブを実行します。

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修正手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

CVE-2024-8535の脆弱性を修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、「**現在のCVE >** `<number of>` NetScalerインスタンスは共通脆弱性識別子 (CVE) の影響を受けています」の下に、この特定のCVEによって脆弱なすべてのインスタンスが表示されます。CVE-2024-8535の影響を受けるインスタンスの詳細を確認するには、CVE-2024-8535を選択し、**影響を受けるインスタンスを表示**をクリックします。

CVE-2024-8535のセキュリティアドバイザリダッシュボード(/en-us/netscaler-console-service/media/security-advisory-cve-2024-8435.png)

「`<number of>` CVEの影響を受けるNetScalerインスタンス」ウィンドウが表示されます。ここでは、CVE-2024-8535の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

CVE-2020-8300の影響を受けるインスタンス(/en-us/netscaler-console-service/media/cve-2024-8535-impacted-instance.png)

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

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

注

セキュリティアドバイザリシステムスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2024-8535の影響が反映されるまでに時間がかかる場合があります。影響をより早く確認するには、**今すぐスキャン**をクリックしてオンデマンドスキャンを開始します。

CVE-2024-8535を修正する

CVE-2024-8535の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの「**現在のCVE > CVEの影響を受けるNetScalerインスタンス**」の下に、ステップ1と2が表示されます。

CVE-2024-8535の修正手順(/en-us/netscaler-console-service/media/remediate-steps-CVE-2024-8535.png)

2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正を含むリリースとビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。

「**現在のCVE > CVEの影響を受けるNetScalerインスタンス**」の下に、この2段階の修正プロセスには、2つの異なるワークフローが表示されます。それらは「**アップグレードワークフローに進む**」と「**構成ジョブワークフローに進む**」です。

ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、 をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

注：

この手順は、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

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

ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、**`<number of>` CVEの影響を受ける NetScalerインスタンス** ウィンドウで、CVE-2024-8535の影響を受けるインスタンスを選択し、をクリックします。

インスタンスを選択して をクリックする前に、次の点に留意してください。

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956など）の影響を受けるNetScalerインスタンスの場合：インスタンスを選択して をクリックしても、組み込みの構成テンプレートは の下に自動入力されません。適切な構成ジョブテンプレートを の下から右側の構成ジョブペインに手動でドラッグアンドドロップします。
- CVE-2024-8535のみの影響を受ける複数のNetScalerインスタンスの場合、すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2024-8535のみの影響を受けているとします。これらのインスタンスをすべて選択し、 をクリックすると、組み込みの構成テンプレートが の下に自動入力されます。
- CVE-2024-8535と1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスの場合、各NetScalerに一度に1つずつ修復を適用する必要があります。これらのインスタンスを選択して をクリックすると、各NetScalerで構成ジョブを一度に1つずつ実行するように指示するエラーメッセージが表示されます。

ステップ1：構成の選択

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが の下に自動入力されます。

Step 2: インスタンスを選択する

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択します。このインスタンスがHAペアの一部である場合は、**セカンダリノードで実行**を選択します。**次へ**をクリックします。

インスタンスの選択(/en-us/netscaler-console-service/media/select-instance-cve-2021-22956.png)

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

注:

セキュリティアドバイザリを使用するクラスターモードのNetScalerインスタンスの場合、NetScaler Consoleは、クラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートします。CCO以外のノードでは、コマンドを個別に実行してください。

Step 3: 変数値を指定する

このステップでは、変数を指定する必要はありません。**すべてのインスタンスに共通の変数値**を選択し、**次へ**をクリックします。

Step 4: 構成をプレビューする

構成に挿入された変数値をプレビューし、**次へ**をクリックします。

ジョブのプレビュー(/en-us/netscaler-console-service/media/preview-job-cve-2024-8535.png)

Step 5: ジョブを実行する

構成ジョブを実行するには、**完了**をクリックします。

構成ジョブの実行(/en-us/netscaler-console-service/media/run-job-cve-2021-22956.png)

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復ステップを完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

CVE-2020-8300 の脆弱性に対処する

NetScaler Console のセキュリティアドバイザリダッシュボードで、**Current CVEs > `<number of>` NetScaler instances are impacted by CVEs** の下には、この特定の CVE によって脆弱なすべてのインスタンスが表示されます。CVE-2020-8300 の影響を受けるインスタンスの詳細を確認するには、**CVE-2020-8300** を選択し、**View Affected Instances** をクリックします。

注

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

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

<number of> NetScaler instances impacted by CVEs ウィンドウが表示されます。ここには、CVE-2020-8300 の影響を受ける NetScaler インスタンスの数と詳細が表示されます。

CVE-2020-8300 の修正

CVE-2020-8300 の影響を受ける NetScaler インスタンスの場合、修正は 2 段階のプロセスです。GUI の **Current CVEs > NetScaler instances are impacted by CVEs** の下で、ステップ 1 と 2 を確認できます。

2 つのステップは次のとおりです。

1. 脆弱な NetScaler インスタンスを、修正を含むリリースおよびビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。このステップは、脆弱な NetScaler ごとに一度に 1 つずつ実行し、その NetScaler のすべての SAML アクションと SAML プロファイルを含めます。

Current CVEs> NetScaler instances impacted by CVEs の下には、この 2 段階の修正プロセスに対して 2 つの異なるワークフローが表示されます。それらは **Proceed to upgrade workflow** と **Proceed to configuration job workflow** です。

ステップ 1: 脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「NetScaler アップグレードジョブの作成」を参照してください。

注

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

ステップ 2: 構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、**<number of> CVE の影響を受ける NetScaler インスタンス** ウィンドウで、CVE-2020-8300 の影響を受けるインスタンスを 1 つ選択

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

し、**Proceed to configuration job workflow** をクリックします。ワークフローには次のステップが含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が設定された最終構成の確認。
5. ジョブの実行。

インスタンスを選択して **Proceed to configuration job workflow** をクリックする前に、次の点に注意してください。

- 複数の CVE (CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 など) の影響を受ける NetScaler インスタンスの場合: インスタンスを選択して **Proceed to configuration job workflow** をクリックしても、組み込みの構成テンプレートは の下に自動入力されません。適切な構成ジョブテンプレートを **Security Advisory Template** の下から右側の構成ジョブペインに手動でドラッグアンドドロップします。
- CVE-2021-22956のみの影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで一度に設定ジョブを実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2021-22956のみの影響を受けているとします。これらのインスタンスをすべて選択し、**設定ジョブワークフローに進む**をクリックすると、組み込みの設定テンプレートが**設定の選択**の下に自動入力されます。既知の問題NSADM-80913については、リリースノートを参照してください。
- CVE-2021-22956と1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスの場合、各NetScalerに一度に修正を適用する必要があります。これらのインスタンスを選択して**設定ジョブワークフローに進む**をクリックすると、各NetScalerで一度に設定ジョブを実行するように指示するエラーメッセージが表示されます。

ステップ1：設定の選択

設定ジョブワークフローでは、組み込みの設定テンプレートが**設定の選択**の下に自動入力されます。

影響を受けるNetScalerインスタンスごとに、一度に1つずつ個別の設定ジョブを実行し、そのNetScalerのすべてのSAMLアクションとSAMLプロファイルを含めます。たとえば、2つの脆弱なNetScalerインスタンスがあり、それぞれに2つのSAMLアクションと2つのSAMLプロファイルがあ

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

る場合、この設定ジョブを2回実行する必要があります。各NetScalerにつき1回、そのすべてのSAMLアクションとSAMLプロファイルをカバーするように実行します。

NETSCALER 1	NETSCALER2
ジョブ1：2つのSAMLアクション +2つのSAMLプロファイル	ジョブ2：2つのSAMLアクション +2つのSAMLプロファイル

ジョブに名前を付け、以下の仕様に合わせてテンプレートをカスタマイズします。組み込みの設定テンプレートは、あくまで概要または基本テンプレートです。以下の要件に合わせて、デプロイメントに基づいてテンプレートをカスタマイズしてください。

a. **SAMLアクションとその関連ドメイン**

デプロイメント内のSAMLアクションの数に応じて、1〜3行目を複製し、各SAMLアクションのドメインをカスタマイズする必要があります。

たとえば、2つのSAMLアクションがある場合、1〜3行目を2回繰り返し、それに応じて各SAMLアクションの変数定義をカスタマイズします。

SAMLアクションにN個のドメインがある場合は、そのSAMLアクションに対して行がN回表示されるように、`bind patset $saml_action_patset$ “$saml_action_domain1$”` の行を手動で複数回入力する必要があります。そして、以下の変数定義名を変更します。

- `saml_action_patset`: は設定テンプレート変数であり、SAMLアクションのパターンセット (patset) の名前の値を表します。実際の値は、設定ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。
- `saml_action_domain1`: は設定テンプレート変数であり、その特定のSAMLアクションのドメイン名を表します。実際の値は、設定ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。

デバイスのすべてのSAMLアクションを見つけるには、コマンド `show samlaction` を実行します。

b. **SAMLプロファイルとその関連URL**

デプロイに存在するSAMLプロファイルの数に応じて、4〜6行目を複製します。各SAMLプロファイルのURLをカスタマイズします。

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

例えば、SAMLプロファイルが2つある場合、4〜6行目を手動で2回入力し、それに応じて各SAMLアクションの変数定義をカスタマイズします。

SAMLアクションにN個のドメインがある場合は、そのSAMLプロファイルに対して行がN回表示されるように、`bind patset $saml_profile_patset$ “$saml_profile_url1$”` の行を手動で複数回入力する必要があります。そして、以下の変数定義名を変更します。

- `saml_profile_patset`: は設定テンプレート変数であり、SAMLプロファイルのパターンセット (patset) の名前の値を表します。実際の値は、設定ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。
- `saml_profile_url1`: は設定テンプレート変数であり、その特定のSAMLプロファイルのドメイン名を表します。実際の値は、設定ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。

デバイスのすべてのSAMプロファイルを見つけるには、コマンド `show samlidpProfile` を実行します。

ステップ2: インスタンスを選択する

影響を受けるインスタンスは、**Select Instances** の下に自動入力されます。インスタンスを選択し、**Next** をクリックします。

ステップ 3: 変数値を指定する

変数値を入力します。

- `saml_action_patset`: SAMLアクションの名前を追加します
- `saml_action_domain1`: `https://<example1.com>/` の形式でドメインを入力します
- `saml_action_name`: ジョブを設定しているSAMLアクションと同じものを入力します
- `saml_profile_patset`: SAMLプロファイルの名前を追加します
- `saml_profile_url1`: `https://<example2.com>/cgi/samlauth` の形式でURLを入力します
- `saml_profile_name`: ジョブを設定しているSAMLプロファイルと同じものを入力します

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

注

URLの場合、拡張子は常に `cgi/samlauth` とは限りません。使用しているサードパーティ認証によって異なり、それに応じて拡張子を設定する必要があります。

ステップ 4: 設定をプレビューする

設定に挿入された変数値をプレビューし、**Next** をクリックします。

ステップ5：ジョブを実行する

Finishをクリックして、構成ジョブを実行します。

構成ジョブを実行(/en-us/netscaler-console-service/media/run-job.png)

ジョブが実行されると、**Infrastructure > Configuration > Configuration Jobs**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

NetScaler Console Expressアカウントに関する注意事項

NetScaler Console Expressアカウントには、2つの構成ジョブのみという制限を含む、機能が制限されています。NetScaler Console Expressアカウントの詳細については、「Expressアカウントを使用したNetScaler Consoleリソースの管理」を参照してください。 CVE-2020-8300の修復には、脆弱なNetScalerインスタンスの数と同じ数の構成ジョブを実行する必要があります。したがって、Expressアカウントをお持ちで、2つ以上の構成ジョブを実行する必要がある場合は、この回避策に従ってください。

回避策: 2つの脆弱なNetScalerインスタンスに対して2つの構成ジョブを実行し、両方のジョブを削除して、次の2つの脆弱なNetScalerインスタンスに対して次の2つのジョブの実行を続行します。すべての脆弱なインスタンスをカバーするまでこれを続行します。ジョブを削除する前に、将来の参照のためにレポートをダウンロードできます。レポートをダウンロードするには、**Network > Jobs**でジョブを選択し、**Actions**の下にある**Download**をクリックします。

例: 6つの脆弱なNetScalerインスタンスがある場合、それぞれ2つの脆弱なインスタンスで2つの構成ジョブを実行し、両方の構成ジョブを削除します。この手順をさらに2回繰り返します。最終的に、6つのNetScalerインスタンスに対してそれぞれ6つの構成ジョブを実行したことになります。NetScaler Console UIの**Infrastructure > Jobs**には、最後の2つの構成ジョブのみが表示されます。

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

シナリオ

このシナリオでは、3つのNetScalerインスタンスがCVE-2020-8300に対して脆弱であり、すべてのインスタンスを修復する必要があります。次の手順に従ってください。

1. このドキュメントの**インスタンスのアップグレード**セクションに記載されている手順に従って、3つのNetScalerインスタンスすべてをアップグレードします。
2. 構成ジョブワークフローを使用して、一度に1つのNetScalerに構成パッチを適用します。このドキュメントの**構成コマンドの適用**セクションに記載されている手順を参照してください。

脆弱なNetScaler 1には、次の構成があります。

2つのSAMLアクション	2つのSAMLプロファイル

設定ジョブワークフローを開始する(/en-us/netscaler-console-service/media/scenario-config-job-workflow.png)

NetScaler 1を選択し、**設定ジョブワークフローに進む**をクリックします。組み込みテンプレートが自動入力されます。次に、ジョブ名を入力し、指定された構成に従ってテンプレートをカスタマイズします。

指定されたシナリオのテンプレートをカスタマイズする(/en-us/netscaler-console-service/media/scenario-customize-template.png)

次の表に、カスタマイズされたパラメータの変数定義を示します。

表1. SAMLアクションの変数定義

NETSCALER構成	PATSETの変数定義	SAMLアクション名の変数定義	ドメインの変数定義
SAMLアクション1には1つのドメインがあります	saml_action_patset1	saml_action_name1	saml_action_domain1
SAMLアクション2には2つのドメインがあります	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

表2. SAMLプロファイルの変数定義

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

NETSCALER構成	PATSETの変数定義	SAMLプロファイル名の変数定義	URLの変数定義
SAMLプロファイル1には1つのURLがあります	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAMLプロファイル2には2つのURLがあります	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

「**インスタンスの選択**」でNetScaler 1 を選択し、「**次へ**」をクリックします。「**変数の値を指定**」ウィンドウが表示されます。このステップでは、前のステップで定義したすべての変数に値を指定する必要があります。

次に、変数を確認します。

「**次へ**」をクリックし、次に「**完了**」をクリックしてジョブを実行します。

ジョブが実行されると、「**インフラストラクチャ > 構成 > 構成ジョブ**」に表示されます。

NetScaler 1 の2つの修復手順を完了したら、NetScaler 2 および NetScaler 3 を修復するために同じ手順に従います。修復が完了したら、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

CVE-2021-22927およびCVE-2021-22920の脆弱性を修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードの**Current CVEs > `<number of>` NetScaler instances are impacted by CVEs**で、CVE-2021-22927およびCVE-2021-22920によって脆弱なすべてのインスタンスを確認できます。これら2つのCVEの影響を受けるインスタンスの詳細を確認するには、1つ以上のCVEを選択し、**View Affected Instances**をクリックします。

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

注

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2021-22927およびCVE-2021-22920の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、**Scan-Now**をクリックしてオンデマンドスキャンを開始します。 セキュリティアドバイザリダッシュボードの詳細については、Security Advisoryを参照してください。

`<number of>` **NetScaler instances impacted by CVEs**ウィンドウが表示されます。次のスクリーンショットでは、CVE-2021-22927およびCVE-2021-22920の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

CVE-2021-22927およびCVE-2021-22920を修正する

CVE-2021-22927およびCVE-2021-22920の影響を受けるNetScalerインスタンスの場合、修正は2段階のプロセスです。GUIの**Current CVEs > NetScaler instances are impacted by CVEs**で、ステップ1と2を確認できます。

2つの手順は次のとおりです。

1. 脆弱なNetScalerインスタンスを修正を含むリリースおよびビルドにアップグレードする。
2. 構成ジョブでカスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用します。この手順を脆弱なNetScalerごとに1つずつ実行し、そのNetScalerのすべてのSAMLアクションを含めます。

注

CVE-2020-8300のNetScalerインスタンスで構成ジョブをすでに実行している場合は、手順2をスキップします。

Current CVEs > NetScaler instances impacted by CVEsの下に、この2段階の修復プロセスに対応する2つの別々のワークフローが表示されます。これらは、**Proceed to upgrade workflow**と**Proceed to configuration job workflow**です。

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

ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow**をクリックします。アップグレードワークフローが開き、脆弱なNetScalerインスタンスがすでに設定されています。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

注

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。 **注**

CVE-2021-22920およびCVE-2021-22927に対して脆弱なすべてのNetScalerインスタンスについてステップ1を完了したら、オンデマンドスキャンを実行します。**Current CVEs**の下に表示される更新されたセキュリティ態勢は、NetScalerインスタンスがこれらのCVEのいずれかに対してまだ脆弱であるかどうかを理解するのに役立ちます。新しい態勢から、構成ジョブを実行する必要があるかどうかも確認できます。 CVE-2020-8300に対して適切な構成ジョブをNetScalerインスタンスにすでに適用し、NetScalerインスタンスをアップグレードした場合、オンデマンドスキャンを実行すると、そのインスタンスはCVE-2020-8300、CVE-2021-22920、およびCVE-2021-22927に対して脆弱であるとは表示されなくなります。

ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、**`<number of >` NetScaler instances impacted by CVEs**ウィンドウで、CVE-2021-22927およびCVE-2021-22920の影響を受けるインスタンスを1つ選択し、**Proceed to configuration job workflow**をクリックします。ワークフローには次のステップが含まれます。

1. 構成のカスタマイズ。
2. 自動入力された影響を受けるインスタンスの確認。
3. ジョブの変数に対する入力の指定。
4. 変数入力が設定された最終構成の確認。
5. ジョブを実行しています。

インスタンスを選択して**Proceed to configuration job workflow**をクリックする前に、以下の点に留意してください。

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

- 複数のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956など）の影響を受けるNetScalerインスタンスの場合：インスタンスを選択して**Proceed to configuration job workflow**をクリックしても、組み込みの構成テンプレートは「Select configuration」の下に自動入力されません。適切な構成ジョブテンプレートを**Security Advisory Template**の下から右側の構成ジョブペインに手動でドラッグアンドドロップしてください。
- CVE-2021-22956のみの影響を受ける複数のNetScalerインスタンスの場合：すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3があり、これらすべてがCVE-2021-22956のみの影響を受けているとします。これらのインスタンスをすべて選択して**Proceed to configuration job workflow**をクリックすると、組み込みの構成テンプレートが**Select configuration**の下に自動入力されます。既知の問題NSADM-80913については、リリースノートを参照してください。
- CVE-2021-22956および1つ以上の他のCVE（CVE-2020-8300、CVE-2021-22927、CVE-2021-22920など）の影響を受ける複数のNetScalerインスタンスの場合で、各NetScalerに一度に修正を適用する必要がある場合：これらのインスタンスを選択して**Proceed to configuration job workflow**をクリックすると、各NetScalerで一度に構成ジョブを実行するように指示するエラーメッセージが表示されます。

ステップ1：構成の選択

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが**Select configuration**の下に自動入力されます。

注

ステップ2で構成コマンドを適用するために選択されたNetScalerインスタンスが、CVE-2021-22927、CVE-2021-22920、およびCVE-2020-8300にも脆弱である場合、CVE-2020-8300のベーステンプレートが自動入力されます。CVE-2020-8300テンプレートは、これら3つのCVEすべてに必要な構成コマンドのスーパーセットです。このベーステンプレートをNetScalerインスタンスの展開と要件に合わせてカスタマイズしてください。

影響を受けるNetScalerインスタンスごとに、一度に1つずつ個別の構成ジョブを実行し、そのNetScalerのすべてのSAMLアクションを含める必要があります。たとえば、それぞれ2つのSAMLアクションを持つ脆弱なNetScalerインスタンスが2つある場合、この構成ジョブを2回実行する必要があります。各NetScalerにつき1回、そのすべてのSAMLアクションをカバーするように実行します。

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

NETSCALER 1	NETSCALER 2
ジョブ1：2つのSAMLアクション	ジョブ2：2つのSAMLアクション

ジョブに名前を付け、以下の仕様に合わせてテンプレートをカスタマイズします。組み込みの構成テンプレートは、単なる概要またはベーステンプレートです。以下の要件に合わせて、デプロイメントに基づいてテンプレートをカスタマイズしてください。

a. **SAMLアクションとその関連ドメイン**

デプロイメント内のSAMLアクションの数に応じて、1〜3行目を複製し、各SAMLアクションのドメインをカスタマイズする必要があります。

SAMLアクションをカスタマイズ(/en-us/netscaler-console-service/media/saml-action-cve-2021-22927-2021-22920.png)

たとえば、2つのSAMLアクションがある場合、1〜3行目を2回繰り返し、それに応じて各SAMLアクションの変数定義をカスタマイズします。

また、SAMLアクションにN個のドメインがある場合、そのSAMLアクションに対して行がN回表示されるように、`bind patset $saml_action_patset$ “$saml_action_domain1$”` の行を複数回手動で入力する必要があります。そして、以下の変数定義名を変更します。

- `saml_action_patset`: は構成テンプレート変数であり、SAMLアクションのパターンセット（patset）の名前の値を表します。実際の値は、構成ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。
- `saml_action_domain1`: は構成テンプレート変数であり、その特定のSAMLアクションのドメイン名を表します。実際の値は、構成ジョブワークフローのステップ3で指定できます。このドキュメントの「ステップ3: 変数値を指定する」セクションを参照してください。

デバイスのすべてのSAMLアクションを見つけるには、コマンド `show samlaction` を実行します。

SAMLアクションを見つける(/en-us/netscaler-console-service/media/show-samlaction-command.png)

ステップ2: インスタンスを選択する

影響を受けるインスタンスは、**インスタンスの選択**の下に自動入力されます。インスタンスを選択し、**次へ**をクリックします。

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

インスタンスを選択(/en-us/netscaler-console-service/media/select-instance-cve-2021-22927-2021-22920.png)

ステップ3: 変数値を指定する

変数値を入力します。

- `saml_action_patset`: SAMLアクションの名前を追加します
- `saml_action_domain1`: `https://<example1.com>/`の形式でドメインを入力します
- `saml_action_name`: ジョブを構成しているSAMLアクションと同じものを入力します

ステップ4：構成をプレビューする

構成に挿入された変数値をプレビューし、**次へ**をクリックします。

ステップ5：ジョブを実行する

完了をクリックして構成ジョブを実行します。

ジョブが実行されると、**Infrastructure > Configuration > Configuration Jobs**の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

シナリオ

このシナリオでは、2つのNetScalerインスタンスがCVE-2021-22920に対して脆弱であり、すべてのインスタンスを修復する必要があります。次の手順に従います。

1. このドキュメントの「インスタンスのアップグレード」セクションに記載されている手順に従って、3つのNetScalerインスタンスすべてをアップグレードします。
2. 設定ジョブワークフローを使用して、一度に1つのNetScalerに設定パッチを適用します。このドキュメントの「設定コマンドの適用」セクションに記載されている手順を参照してください。

脆弱なNetScaler 1には、2つのSAMLアクションがあります。

- SAMLアクション1には1つのドメインがあります
- SAMLアクション2には2つのドメインがあります

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

設定ジョブワークフローを開始する(/en-us/netscaler-console-service/media/scenario-config-job-workflow-cve-2021-22927-2021-22920.png)

NetScaler 1を選択し、「**設定ジョブワークフローに進む**」をクリックします。組み込みのベーステンプレートが自動入力されます。次に、ジョブ名を入力し、指定された設定に従ってテンプレートをカスタマイズします。

指定されたシナリオのテンプレートをカスタマイズする(/en-us/netscaler-console-service/media/scenario-customize-template-cve-2021-22927-2021-22920.png)

次の表に、カスタマイズされたパラメータの変数定義を示します。

表。SAMLアクションの変数定義

NETSCALER構成	PATSETの変数定義	SAMLアクション名の変数定義	ドメインの変数定義
SAMLアクション1には1つのドメインがあります	saml_action_patset1	saml_action_name1	saml_action_domain1
SAMLアクション2には2つのドメインがあります	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

「**インスタンスの選択**」でNetScaler 1を選択し、**次へ**をクリックします。「**変数値の指定**」ウィンドウが表示されます。このステップでは、前のステップで定義したすべての変数に値を指定する必要があります。

- [ ] 次に、変数をレビューします。

- [ ] **次へ**をクリックし、**完了**をクリックしてジョブを実行します。

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ**の下に表示されます。

NetScaler 1の2つの修復手順を完了した後、NetScaler 2とNetScaler 3を修復するために同じ手順に従います。修復が完了したら、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

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

CVE-2021-22956の脆弱性を特定して修復する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、**Current CVEs > `<number of>`** NetScalerインスタンスが共通の脆弱性および露出 (CVE) の影響を受けているセクションの下に、この特定のCVEによって脆弱なすべてのインスタンスが表示されます。CVE-2021-22956の影響を受けるインスタンスの詳細を確認するには、CVE-2021-22956を選択し、**View Affected Instances** をクリックします。

`<number of>` NetScaler instances impacted by CVEs ウィンドウが表示されます。ここには、CVE-2021-22956の影響を受けるNetScalerインスタンスの数と詳細が表示されます。

セキュリティアドバイザリダッシュボードの詳細については、Security Advisory を参照してください。

注:

セキュリティアドバイザリシステムスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2021-22956の影響が反映されるまで時間がかかる場合があります。影響をより早く確認するには、**Scan-Now** をクリックしてオンデマンドスキャンを開始します。

CVE-2021-22956の影響を受けるインスタンスを特定する

CVE-2021-22956にはカスタムスキャンが必要です。このスキャンでは、NetScaler Consoleが管理対象のNetScalerインスタンスに接続し、スクリプトをインスタンスにプッシュします。スクリプトはNetScalerインスタンス上で実行され、Apache設定ファイル (`httpd.conf file`) と最大クライアント接続数 (`maxclient`) パラメータをチェックして、インスタンスが脆弱であるかどうかを判断します。スクリプトがNetScaler Consoleと共有する情報は、ブール値 (trueまたはfalse) での脆弱性ステータスです。スクリプトはまた、ローカルホスト、NSIP、管理アクセスを持つSNIPなど、異なるネットワークインターフェースのmax_clientsのカウントリストをNetScaler Consoleに返します。このリストの詳細レポートは、**Security Advisory** ページの **Scan Logs** タブからダウンロードできるCSVファイルで確認できます。

このスクリプトは、スケジュールされたスキャンまたはオンデマンドスキャンが実行されるたびに実行されます。スキャンが完了すると、スクリプトはNetScalerインスタンスから削除されます。

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

CVE-2021-22956を修復する

CVE-2021-22956の影響を受けるNetScalerインスタンスの場合、修復は2段階のプロセスです。GUIの **Current CVEs > NetScaler instances are impacted by CVEs** の下で、ステップ1と2を確認できます。

2つのステップは次のとおりです。

1. 脆弱なNetScalerインスタンスを、修正プログラムを含むリリースおよびビルドにアップグレードする。
2. 構成ジョブで、カスタマイズ可能な組み込み構成テンプレートを使用して、必要な構成コマンドを適用する。

「現在のCVE > CVEの影響を受けるNetScalerインスタンス」で、この2段階の修復プロセスには、2つの異なるワークフローが表示されます。それらは「アップグレードワークフローに進む」と「構成ジョブワークフローに進む」です。

ステップ1：脆弱なNetScalerインスタンスをアップグレードする

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、「**アップグレードワークフローに進む**」をクリックします。脆弱なNetScalerインスタンスがすでに設定された状態で、アップグレードワークフローが開きます。

NetScaler Consoleを使用してNetScalerインスタンスをアップグレードする方法の詳細については、「NetScalerアップグレードジョブの作成」を参照してください。

注：

このステップは、すべての脆弱なNetScalerインスタンスに対して一度に実行できます。

ステップ2：構成コマンドを適用する

影響を受けるインスタンスをアップグレードした後、「**`<number of>` CVEの影響を受けるNetScalerインスタンス**」ウィンドウで、CVE-2021-22956の影響を受けるインスタンスを選択し、「**構成ジョブワークフローに進む**」をクリックします。ワークフローには次のステップが含まれます。

1. 構成をカスタマイズする。
2. 自動入力された影響を受けるインスタンスを確認する。

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

3. ジョブの変数に対する入力を指定する。
4. 変数入力が設定された最終構成を確認する。
5. ジョブの実行。

インスタンスを選択して をクリックする前に、次の点に注意してください。

- 複数の CVE (CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 など) の影響を受ける NetScaler インスタンスの場合: インスタンスを選択して をクリックしても、組み込みの構成テンプレートは の下に自動入力されません。適切な構成ジョブテンプレートを の下から右側の構成ジョブペインに手動でドラッグアンドドロップします。
- CVE-2021-22956 のみの影響を受ける複数の NetScaler インスタンスの場合: すべてのインスタンスで構成ジョブを一度に実行できます。たとえば、NetScaler 1、NetScaler 2、NetScaler 3 があり、これらすべてが CVE-2021-22956 のみの影響を受けているとします。これらのインスタンスをすべて選択して をクリックすると、組み込みの構成テンプレートが の下に自動入力されます。
- CVE-2021-22956 と 1 つ以上の他の CVE (CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 など) の影響を受ける複数の NetScaler インスタンスの場合、各 NetScaler に一度に修正を適用する必要があります。これらのインスタンスを選択して をクリックすると、各 NetScaler で一度に構成ジョブを実行するように指示するエラーメッセージが表示されます。

手順 1：構成を選択する

構成ジョブワークフローでは、組み込みの構成ベーステンプレートが の下に自動入力されます。

手順 2：インスタンスを選択する

影響を受けるインスタンスは の下に自動入力されます。インスタンスを選択します。このインスタンスが HA ペアの一部である場合は、 を選択します。 をクリックします。

注：

クラスターモードの NetScaler インスタンスの場合、セキュリティアドバイザリを使用すると、NetScaler Console はクラスター構成コーディネーター (CCO) ノードでのみ構成ジョブの実行をサポートします。CCO 以外のノードでは、コマンドを個別に実行します。

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

手順 3：変数値を指定する

変数値を入力します。

インスタンスの変数を指定するには、次のいずれかのオプションを選択します。

すべてのインスタンスの共通変数: 変数 `max_client` に共通の値を入力します。

変数値を入力ファイルでアップロード: **入力キーファイルのダウンロード** をクリックして、入力ファイルをダウンロードします。入力ファイルで、変数 `max_client` の値を入力し、ファイルをNetScaler Consoleサーバーにアップロードします。

注:

上記のどちらのオプションでも、推奨される `max_client` の値は30です。現在の値に応じて値を設定できます。ただし、ゼロであってはならず、`/etc/httpd.conf` ファイルで設定されているmax_client以下である必要があります。NetScalerインスタンスで文字列 `MaxClients` を検索することで、Apache HTTP Server構成ファイル `/etc/httpd.conf` に設定されている現在の値を確認できます。

ステップ4: 構成をプレビューする

構成に挿入された変数値をプレビューし、**次へ** をクリックします。

ステップ5: ジョブを実行する

完了 をクリックして、構成ジョブを実行します。

ジョブが実行されると、**インフラストラクチャ > 構成 > 構成ジョブ** の下に表示されます。

すべての脆弱なNetScalerインスタンスに対して2つの修復手順を完了した後、オンデマンドスキャンを実行して、改訂されたセキュリティ体制を確認できます。

CVE-2022-27509 の脆弱性を特定し、修正する

NetScaler Consoleのセキュリティアドバイザリダッシュボードで、「**現在のCVE `<number of>` CVEの影響を受けるNetScalerインスタンス**」の下に、CVE-2022-27509によって脆弱なすべてのインスタンスが表示されます。CVEの影響を受けるインスタンスの詳細を確認するには、CVE-2022-27509を選択し、「**影響を受けるインスタンスを表示**」をクリックします。

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

注

NetScalerの脆弱性の理由を理解するには、セキュリティアドバイザリのタブでCSVレポートをダウンロードしてください。

「`<number of>` **CVEの影響を受けるNetScalerインスタンス**」ウィンドウが表示されます。次のスクリーンショットでは、CVE-2022-27509の影響を受けるNetScalerインスタンスの数と詳細を確認できます。

セキュリティアドバイザリダッシュボードの詳細については、セキュリティアドバイザリを参照してください。

注

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2022-27509の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、「**今すぐスキャン**」をクリックしてオンデマンドスキャンを開始してください。

CVE-2022-27509の影響を受けるインスタンスを特定する

CVE-2022-27509には、カスタムスキャンとバージョンスキャンの組み合わせが必要です。カスタムスキャンの一環として、NetScaler Consoleは管理対象のNetScalerインスタンスに接続し、スクリプトをインスタンスにプッシュします。このスクリプトはNetScalerインスタンス上で実行され、インスタンスが脆弱であるかどうかを判断します。このスクリプトは、スケジュールされたスキャンまたはオンデマンドスキャンが実行されるたびに実行されます。

スキャンが完了すると、スクリプトはNetScalerインスタンスから削除されます。

これらのセキュリティアドバイザリカスタムスキャンをオプトアウトすることもできます。カスタムスキャン設定とカスタムスキャンのオプトアウトの詳細については、「**セキュリティアドバイザリ**」ページの「**カスタムスキャン設定の構成**」セクションを参照してください。

CVE-2022-27509を修正する

CVE-2022-27509 の影響を受ける NetScaler インスタンスの場合、修復は単一ステップのプロセスであり、脆弱な NetScaler インスタンスを修正を含むリリースとビルドにアップグレードする必

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

要があります。GUI の **Current CVEs > NetScaler instances are impacted by CVEs** で、修復手順を確認できます。

Current CVEs> NetScaler instances impacted by CVEs で、この単一ステップの修復プロセスに対する次のワークフロー、つまり **Proceed to upgrade workflow** が表示されます。

脆弱なインスタンスをアップグレードするには、インスタンスを選択し、**Proceed to upgrade workflow** をクリックします。アップグレードワークフローが開き、脆弱な NetScaler インスタンスがすでに設定されています。

重要

脆弱な NetScaler インスタンスに /etc/httpd.conf ファイルが /nsconfig ディレクトリにコピーされている場合は、NetScaler のアップグレードを計画する前に、カスタマイズされた NetScaler 構成のアップグレードに関する考慮事項 を参照してください。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、NetScaler アップグレードジョブの作成 を参照してください。

セキュリティアドバイザリでサポートされていないCVE

NetScaler Consoleセキュリティアドバイザリは、すべての新しい共通脆弱性識別子 (CVE) を追跡し、インフラストラクチャへのCVEの影響を評価します。推奨事項を確認し、適切な措置を講じることができます。しかし、サポートされていないCVEがいくつかあり、これらの脆弱性の検出と修復は、NetScaler Consoleセキュリティアドバイザリの範囲外です。

- **CVE-2022-21827**:

  CVE-2022-21827は、Windows用NetScaler Gatewayプラグインのバージョン21.9.1.2より前のサポートされているバージョンに影響を与えます。

  Windows用NetScaler Gatewayプラグインに影響を与える脆弱性の検出と修復は、NetScaler Consoleではサポートされていません。また、NetScaler Gatewayプラグインの脆弱性は、NetScaler側でチェックを実行したり、NetScalerのバージョンを確認したり、NetScalerの設定を確認したりすることによって評価することはできません。このCVEの検出と修復は、クライアントに展開されているWindows用NetScaler Gatewayプラグインのバージョンに基づいてのみ評価できます。

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

その結果、この脆弱性の検出と修復は、NetScaler Consoleセキュリティアドバイザリの範囲外となります。

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

セットアップ

初期セットアップが完了したら、展開を完全に管理し始めるために特定の構成を行う必要があります。

- 複数のエージェントの追加。インストールするエージェントの数は、データセンターまたはクラウド内の管理対象インスタンスの数と総スループットによって異なります。Citrixでは、データセンターごとに少なくとも1つのエージェントをインストールすることをお勧めします。
- インスタンスの追加。インスタンスは、NetScaler Console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。インスタンスをサービスに追加して、それらの管理と監視を開始する必要があります。複数のエージェントをインストールした後、インスタンスを追加し、それらをエージェントに関連付ける必要があります。
- Analyticsの有効化。アプリケーションのトラフィックフローに関する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。
- インスタンスでのsyslogの構成。すべてのsyslogメッセージをNetScaler Consoleにリダイレクトするようにデバイスを構成している場合、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。syslogイベントを監視するには、まずNetScaler ConsoleをNetScalerインスタンスのsyslogサーバーとして構成する必要があります。
- ロールベースのアクセス制御の構成。NetScaler Consoleは、きめ細かなロールベースのアクセス制御（RBAC）を提供し、これにより、企業内の個々のユーザーの役割に基づいてアクセス許可を付与できます。
- Analytics設定の構成。Analytics機能を最適に利用するために、特定の構成を行うことができます。たとえば、履歴分析データを保存する期間を指定したり、目的の分析メトリックを監視するためのしきい値とアラートを設定したりできます。

複数のエージェントを追加する

インストールするエージェントの数は、データセンター内の管理対象インスタンスの数と総スループットによって異なります。Citrixは、データセンターごとに少なくとも1つのエージェントをインストールすることを推奨します。

サービスに初めてログオンするときは、1つのエージェントのみをインストールできます。複数のエージェントを追加するには、まず初期設定を完了し、次に**Infrastructure > Instances > Agents**に移動して、**Set Up Agent**をクリックします。

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

必要なハイパーバイザーのイメージをダウンロードし、Getting Startedの手順に従ってエージェントをインストールします。画面に表示されているサービスURLとアクティベーションコードを必ずコピーしてください。ハイパーバイザーにエージェントをインストールする際に、サービスURLとアクティベーションコードを入力する必要があるためです。エージェントはサービスURLを使用してサービスを特定し、アクティベーションコードを使用してサービスに登録します。

同じイメージを使用して、ハイパーバイザーに複数のエージェントをインストールできます。ただし、複数のエージェントで同じアクティベーションコードを使用することはできません。1つのエージェントをインストールした後、次のエージェント用にアクティベーションコードを再度生成します。新しいアクティベーションコードは、**Infrastructure > Instances > Agents**に移動し、**Generate Activation Code**をクリックすることで生成できます。

エージェントが正常にインストールおよび登録されたら、サービスGUIでエージェントのステータスを確認し、インスタンスを追加します。

注

Microsoft AzureクラウドまたはAWSクラウドにエージェントをインストールすることもできます。エージェントイメージは、それぞれのクラウドマーケットプレイスで入手できます。

- Microsoft Azureクラウドにエージェントをインストールする手順については、Install a NetScaler agent on Microsoft Azure Cloudを参照してください。
- AWSにエージェントをインストールする手順については、Install a NetScaler agent on AWSを参照してください。

マルチサイト展開向けにエージェントを構成する

エージェントは、NetScaler Consoleと、異なるデータセンターおよびパブリッククラウド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。NetScaler Consoleは、データセンターまたはパブリッククラウド内でのエージェントフェイルオーバーをサポートしています。

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。

- エージェントに構成されたインスタンスは、未処理のデータをNetScaler Consoleではなくエージェントに直接送信します。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NetScaler Consoleに送信して保存します。

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

- エージェントとインスタンスは同じデータセンターまたはクラウドに併置されるため、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、エージェントフェイルオーバー時にNetScalerインスタンスの再配布が提供されます。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わります。

アーキテクチャ

次の図は、エージェントフェイルオーバーを実現するために、データセンターとパブリッククラウド内の複数のエージェントに構成されたNetScalerインスタンスを示しています。

マルチサイト展開用に構成されたエージェント(/en-us/netscaler-console-service/media/agent-cluster-architecture.png)

パブリッククラウドには4つのNetScalerインスタンスと2つのエージェントがあります。エンタープライズデータセンターにも4つのNetScalerインスタンスと2つのエージェントがあります。各エージェントは2つのNetScalerインスタンスで構成されています。

エージェントは、構成されたインスタンスから直接データを受信します。エージェントはデータを受信した後、データを処理し、圧縮形式でNetScaler Consoleに送信します。エージェントは、セキュアチャネルを介してNetScaler Consoleサーバーと通信します。

パブリッククラウドでは、**エージェント1**が非アクティブ（DOWN状態）になると、エージェントフェイルオーバーが発生します。NetScaler Consoleは、**エージェント1**のNetScalerインスタンスを**エージェント2**に再配布します。データセンター内のいずれかのエージェントが失敗した場合、エンタープライズデータセンターでインスタンスの再配布が発生します。

エージェントをインストールするには、「NetScalerエージェントのインストール」を参照してください。

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つ以上の登録済みエージェントがあるサイトで発生する可能性があります。サイト内のエージェントが非アクティブ（DOWN状態）になると、NetScaler Consoleは非アクティブなエージェントのNetScalerインスタンスを他のアクティブなエージェントに再配布します。

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

重要

- エージェントフェイルオーバーはCPXインスタンスを考慮しません。
- エージェントフェイルオーバー機能がアカウントで有効になっていることを確認してください。この機能を有効にするには、「NetScaler Console機能の有効化または無効化」(/ja-jp/netscaler-console-service/settings/configure-features.html)を参照してください。
- エージェントがスクリプトを実行している場合は、そのスクリプトがサイト内のすべてのエージェントに存在することを確認してください。そのため、エージェントフェイルオーバー後、変更されたエージェントがスクリプトを実行できます。

NetScaler Console GUIでサイトをエージェントにアタッチするには：

1. **Infrastructure > Instances > Agents** に移動します。
2. サイトにアタッチするエージェントを選択します。
3. リストからサイトを指定します。新しいサイトを追加したい場合は、「**追加**」をクリックします。
4. 「**保存**」をクリックします。

エージェントフェイルオーバーを実現するには、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。

例えば、2つのエージェント 10.106.1xx.2x と 10.106.1xx.7x 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った場合、NetScaler Consoleがそれを検出し、状態をダウンとして表示します。

サイト内のエージェントが非アクティブ（ダウン状態）になった場合、NetScaler Consoleは、エージェントがアクティブ（アップ状態）になるまで数分間待機します。エージェントが非アクティブのままである場合、NetScaler Consoleは、同じサイト内の利用可能なエージェント間でインスタンスを自動的に再配布します。この再配布には約10〜15分かかる場合があります。

NetScaler Consoleは、サイト内のアクティブなエージェント間で負荷を分散するために、30分ごとにインスタンスの再配布をトリガーします。

トラップ宛先、syslogサーバー、および分析のために、同じサイト内のエージェントにインスタンスがアタッチされ、自動的に再構成されます。

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

エージェントのアップグレード設定を構成する

NetScaler Console では、ソフトウェアバージョン 12.0 ビルド 507.110 以降で実行されているエージェントは、NetScaler Console によって、より新しい推奨バージョンに自動的にアップグレードされます。エージェントは、新しいバージョンが利用可能になったとき、または指定した時間にアップグレードされます。

Infrastructure > Instances > Agents に移動して、エージェントの現在のバージョンと推奨バージョンを表示できます。

デフォルトでは、新しいバージョンが利用可能になると、エージェントは自動的にアップグレードされます。ただし、各エージェントのアップグレードをスケジュールできます。

アップグレード中、約5分間のダウンタイムが発生する可能性があります。

エージェントのアップグレード設定を構成するには：

1. **Infrastructure > Instances > Agents** に移動し、**Settings** をクリックします。

2. 各エージェントのアップグレードを開始するタイミングを指定します。

   エージェントをアップグレードするには、次のいずれかのオプションを使用できます。

   - 自動アップグレード - 新しいエージェントイメージが利用可能になったときにエージェントをアップグレードするには、**Auto-Upgrade** を選択します。値を入力しない場合、デフォルトで **Auto-Upgrade** が選択されます。
   - 特定の時間を設定：NetScaler Console がエージェントを自動的にアップグレードするタイミングで、時間（hh:mm 形式）を入力し、タイムゾーンを選択します。

   Copy to All をクリックすると、すべてのエージェントに同じアップグレード時間を適用できます。

3. **Save** をクリックします。

   これらの設定は、設定を変更するまで、今後のエージェントアップグレードにわたって保持されます。

エージェントを手動でアップグレードする

一部のシナリオでは、エージェントが自動的にアップグレードされず、古いバージョンで実行されている場合があります。このようなシナリオでは、エージェントを手動でアップグレードする必要があります。エージェントが最新バージョンで実行されているかどうかは、**Infrastructure >**

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

Instances > Agents に移動し、**Version** の下のビルドを確認することで検証できます。ダウンロードアイコンが表示されている場合、エージェントは古いバージョンで実行されています。

外部エージェントを手動でアップグレードするには：

1. **Infrastructure > Instances > Agents** で、バージョンで利用可能なダウンロードアイコンをクリックして、最新のビルドをダウンロードします。
2. FTPクライアントを使用して、エージェントパッケージ (`build-masagent.tgz`) をエージェントの `/var/mps/mps_agent_images/latest` の場所にコピーします。
3. 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ます。
4. エージェントパッケージを解凍します。

   ```
   cd /var/mps/mps_agent_images/latest
   ```

   ```
   tar -xzvf build-masagent.tgz
   ```
5. `./installmasagent` を実行します

インストールプロセスが開始され、アップグレードが完了するとエージェントが再起動します。

組み込みエージェントを手動でアップグレードするには：

Infrastructure > Instances > NetScaler に移動し、右にスクロールして **Build-in agent version** を表示します。ダウンロードアイコンが表示されている場合、エージェントは古いバージョンで実行されています。

エージェントのバージョン(/en-us/netscaler-console-service/media/built-in-agent-version.png)

1. **Infrastructure > Instances > NetScaler**で、バージョンで利用可能なダウンロードアイコンをクリックして、最新のビルドをダウンロードします。
2. FTPクライアントを使用して、mastoolsパッケージを`/var/mastools directory`の場所にコピーします。
3. SSHクライアントを使用してNetScalerにログオンします。
4. `/var/mastools/scripts/mastoolsd stop`を実行します。
5. `tar xvzf <package_name_with_path> -C /var/mastools`を実行します。

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

注:

`package_name_with_path`をパッケージの場所の正確なパスに置き換える必要があります。

6. `/bin/sh /var/mastools/scripts/admautoreg/admautoregd_ctl restart_if_running`を実行します。
7. `/var/mastools/scripts/mastoolsd restart`を実行します。

NetScaler ConsoleでのデュアルNICサポート

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、エージェントは次のことができるようになります。

- エージェントとNetScalerインスタンス間の通信を確立する - 最初のNICを使用して、NetScaler Consoleを介して送受信されるトラフィックを分離し、NetScaler Consoleとその管理対象NetScalerインスタンス間の通信を別のネットワークで確立できます。
- エージェントとNetScaler Console間の通信を確立する - 2番目のNICを使用して、ネットワーク上にあるNetScaler Consoleを管理し、管理タスクを実行できます。

注

両方のNICの機能と構成を入れ替えることはできません。

デュアルNICインフラストラクチャのブロック図(/en-us/netscaler-console-service/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 Consoleとその管理対象NetScalerインスタンス間のトラフィックのIPアドレスを構成します。
- NetScaler Consoleソフトウェアを管理するためのIPアドレスを構成し、ソフトウェア内のすべての管理タスクを実行します。

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

注

エージェントにデュアルNICを構成することは必須ではありません。これはオプションであり、エージェント、NetScaler Consoleサービス、およびNetScalerインスタンス間のトラフィックを分離する必要がある場合にのみ必要です。

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エージェント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 上の 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。

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** 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. コマンド **ifconfig** を実行します。設定した 2 つの NIC の詳細が表示されます。

   - NIC 1 – エージェントと NetScaler Communication 間の通信用
   - NIC 2 – エージェントと NetScaler Console 間の通信用

4. コマンド **networkconfig** 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。

   注:

   2 番目の NIC ネットワークアドレスは、複数の IP 値を受け入れることができます。
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。

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

インスタンスの追加

NetScaler Console を (/ja-jp/netscaler-console-service/getting-started.html) 設定する際、または後からインスタンスを追加できます。

インスタンスとは、NetScaler Console から検出、管理、監視したい NetScaler アプライアンスまたは仮想アプライアンスのことです。NetScaler Console には、次の NetScaler 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
- シトリックス セキュアウェブゲートウェイ™

インスタンスを追加するには、各 NetScaler インスタンスのホスト名または IP アドレス、あるいは IP アドレスの範囲を指定する必要があります。

NetScaler Console がインスタンスにアクセスするために使用できるインスタンスプロファイルを指定します。このインスタンスプロファイルには、サービスに追加するインスタンスのユーザー名とパスワードが含まれています。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、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。デフォルトの NetScaler 管理者資格情報がこのプロファイルを定義します。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。インスタンスが検出された後にインスタンスの資格情報を変更した場合は、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 Console にインスタンスを追加した後、NetScaler Console から NetScaler インスタンスの GUI にアクセスできます。NetScaler Console から NetScaler インスタンスにアクセスするには、Citrix ネットワークに接続している必要があります。

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

注

- クラスターで構成された NetScaler インスタンスを追加するには、クラスター IP アドレスまたはクラスター設定内の個々のノードのいずれかを指定する必要があります。ただし、NetScaler Console では、クラスター IP アドレスがクラスターを表します。
- HAペアとして設定されたNetScalerインスタンスの場合、一方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。
- NetScalerユーザーがすべての権限を持っていることを確認するには、NetScalerでそのユーザーにスーパーユーザー権限を割り当てます。詳細については、「ユーザー、ユーザーグループ、およびコマンドポリシー」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 Console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管理者資格情報を変更した場合は、それらのインスタンスのカスタムインスタンスプロファイルを定義できます。インスタンスが検出された後にインスタンスの資格情報を変更した場合は、インスタンスプロファイルを編集するか、プロファイルを作成してから、インスタンスを再検出する必要があります。

NetScalerプロファイルは、**インスタンス**ページから、またはインスタンスの追加または変更中に作成できます。

注:

インスタンスプロファイルを作成するには、スーパー管理者アカウントを使用してください。

インスタンスページからNetScalerプロファイルを作成するには:

1. **インフラストラクチャ > インスタンス**に移動します。
2. インスタンスを選択します。たとえば、NetScaler。
3. NetScalerページで、**アクションの選択**の下にある**プロファイル**を選択します。

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

4. **管理者プロファイル**ページで、**追加**を選択します。
5. **NetScalerプロファイルの作成**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 ConsoleとNetScalerインスタンス間のSSH通信に使用するポートを指定します。
   e. **HTTPポート**: NetScaler ConsoleとNetScalerインスタンス間のHTTP通信に使用するポートを指定します。

      注:

      デフォルトのHTTPポートは80です。NetScaler CPXインスタンスで設定した、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 ConsoleとNetScaler CPX間でのみ通信に使用できます。

   f. **HTTPSポート**: NetScaler ConsoleとNetScalerインスタンス間のHTTPS通信に使用するポートを指定します。

      注:

      デフォルトのHTTPSポートは443です。NetScaler CPXインスタンスで設定した、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 ConsoleとNetScaler CPX間でのみ通信に使用できます。

   g. **NetScaler通信にグローバル設定を使用**: NetScaler ConsoleとNetScalerインスタンス間の通信にシステム設定を使用する場合は、このオプションを選択します。それ以外の場合は、HTTPまたはHTTPSのいずれかを選択します。
   h. **SNMPバージョン**: **SNMPv2**または**SNMPv3**のいずれかを選択し、以下を実行します。

      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。

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

> **注:**
>
> NetScaler SDXでは、**SNMPv2**のみがサポートされています。

i. **タイムアウト設定**: 再起動後、NetScaler ConsoleがNetScalerインスタンスに接続要求を送信するまでに待機する時間を指定します。

j. **作成**を選択します。

NetScalerインスタンスをNetScaler Consoleに追加するには

> **注**
>
> NetScaler CPXインスタンスを除く、他のすべてのNetScalerインスタンスを追加するには、このタスクを実行します。

1. **Infrastructure > Instances > NetScaler**に移動します。**Instances**の下で、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。
2. 次のいずれかのオプションを選択します。
   - **デバイスIPアドレスを入力** - NetScalerインスタンスの場合、次のいずれかを指定します。
     - ホスト名
     - 各NetScalerインスタンスのIPアドレスまたはNAT IP
     - IPアドレスの範囲

     例えば、1つ以上のホスト名、IPアドレスまたはNAT IP、および/またはIPアドレスの範囲（例: 10.10.20.10-10.10.20.45）をコンマ区切りで入力します。NAT HAインスタンス検出の入力形式は10.10.20.10#10.10.20.32（両方のNetScaler HAインスタンスのNAT IPアドレス）です。
   - **ファイルからインポート** - ローカルシステムから、追加したい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。
3. （オプション）**初回ログイン失敗時にデバイスの追加を有効にする**を選択します。このオプションを使用すると、有効な資格情報がなくてもインスタンスを追加できます。
4. 「**プロファイル**名」から、適切なインスタンスプロファイルを選択するか、**+**アイコンをクリックしてプロファイルを作成します。
5. 「**サイト**」から、インスタンスを追加するサイトを選択します。

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

6. 「**エージェント**」から、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。

   NetScaler Consoleにエージェントが1つしか設定されていない場合、そのエージェントがデフォルトで選択されます。

NetScaler ConsoleでNetScaler CPXインスタンスを追加するには

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**で、**NetScaler**を選択し、CPXタブを選択します。
2. 「**追加**」をクリックします。
3. 次のいずれかのオプションを選択します。

   - 「**デバイスIPアドレスを入力**」。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。
   - 「**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. (オプション)「**初回ログイン失敗時にデバイス追加を有効にする**」を選択します。このオプションを使用すると、有効な資格情報がなくてもインスタンスを追加できます。
5. 「**ルーティング可能なIP/Docker IP**」フィールドにIPアドレスを入力します。IPアドレスは、NetScaler CPXインスタンス（到達可能な場合）またはDockerホストのいずれかです。
6. 「**プロファイル名**」フィールドで、適切なインスタンスプロファイルを選択するか、+アイコンをクリックしてプロファイルを作成します。

   「

   注

   」

   プロファイルを作成する際は、ホストのHTTP、HTTPS、SSH、SNMPポートの詳細を指定してください。また、ホストによって公開されるポートの範囲を「開始ポート」と「ポート数」フィールドで指定することもできます。

7. オプションとして、CPXインスタンスを展開するサイトを選択します。「**追加**」をクリックしてサイトを作成することもできます。
8. 利用可能な場合は、エージェントのリストからエージェントを選択します。

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

9. **OK** をクリックして、NetScaler Consoleにインスタンスを追加するプロセスを開始します。

> **注**
>
> インスタンスを再検出する場合は、次の手順を実行します。

a. **インフラストラクチャ > インスタンス > NetScaler** > **CPX** に移動します。

b. 再検出するインスタンスを選択します。

c. **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 ConsoleでスタンドアロンのNetScaler BLXインスタンスを追加するには

スタンドアロンのNetScaler BLXインスタンスは、専用ホストのLinuxサーバーで実行されている単一のインスタンスです。

1. **インフラストラクチャ > インスタンス > NetScaler** に移動します。
2. **BLX** タブで、**追加** をクリックします。
3. （オプション）「**初回ログイン失敗時にデバイスの追加を有効にする**」を選択します。このオプションを使用すると、有効な資格情報がなくてもインスタンスを追加できます。
4. **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。
5. 「**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。
6. 「**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。
7. 「**プロファイル名**」リストで、BLXインスタンスに適したプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、「**追加**」をクリックします。

> **重要**
>
> プロファイルに、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。

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

9. 「**エージェント**」リストで、インスタンスを関連付けるエージェントを選択します。

   NetScaler Consoleにエージェントが1つしか構成されていない場合、そのエージェントがデフォルトで選択されます。

10. 「**OK**」をクリックします。

NetScaler ConsoleにNetScaler BLXスタンドアロンインスタンスを追加する(/en-us/netscaler-console-service/media/add-blx-standalone-instance.png)

NetScaler Consoleで高可用性NetScaler BLXインスタンスを追加するには

高可用性NetScaler BLXインスタンスは、異なるホストLinuxサーバー上で実行されます。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. （オプション）「**初回ログイン失敗時にデバイスの追加を有効にする**」を選択します。このオプションを使用すると、有効な資格情報がなくてもインスタンスを追加できます。
3. 「**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。
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. 「**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。
7. 「**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。
8. 「**プロファイル名**」リストで、BLXインスタンスに適したプロファイルを選択するか、プロファイルを作成します。

   プロファイルを作成するには、「**追加**」をクリックします。

   重要

   プロファイルで、Linuxサーバーの正しいホストユーザー名とパスワードを指定していることを確認してください。

9. 「**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。

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

10. 「**エージェント**」リストで、インスタンスを関連付けるエージェントを選択します。

    NetScaler Consoleにエージェントが1つしか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。

11. 「**OK**」をクリックします。

NetScaler BLX高可用性インスタンスをNetScaler Consoleに追加(/en-us/netscaler-console-service/media/add-blx-ha-instance.png)

NetScaler ConsoleからインスタンスGUIにアクセスするには

1. **Infrastructure > Instances** > **NetScaler** に移動します。
2. アクセスしたいインスタンスのタイプを選択します（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。

NetScalerインスタンスを表示(/en-us/netscaler-console-service/media/view-instance.png)

インスタンスのIPアドレスは、以下の表記で展開タイプを示します。

- 高可用性ペアでは、**P** – プライマリサーバー、**S** – セカンダリサーバー。
- **C**-クラスター
- **A**-Autoscale™グループ

インスタンスに表記がない場合、それはスタンドアロン展開を示します。

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。

インスタンスの警告を解決する

以下の理由により、インスタンスに警告サインが表示されます。

- **ログイン失敗** - 有効な資格情報なしでインスタンスを追加すると、DOWN状態になり、「ログイン失敗」の警告が表示されます。NetScaler Consoleでインスタンスを管理するには、正しい資格情報を指定してください。

  インスタンスがライセンスなしの場合、インスタンスを選択すると「**License**」オプションが表示されます。ライセンスプールからインスタンスにライセンスを適用するには、「**License**」をクリックします。
- **HTTPSプロファイルを持つライセンスなしのインスタンス** - ライセンスなしのインスタンスがHTTPS接続のみを使用している場合は、NetScaler GUIからインスタンスにライセンスを適用してください。

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

インスタンスでのsyslogの設定

syslogプロトコルは、NetScalerインスタンスがイベント通知メッセージをNetScaler Consoleに送信するためのトランスポートを提供します。NetScaler Consoleは、これらのメッセージのコレクターまたはsyslogサーバーとして構成されます。

すべてのsyslogメッセージをNetScaler Consoleにリダイレクトするようにデバイスを構成している場合、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。syslogイベントを監視するには、まずNetScaler ConsoleをNetScalerインスタンスのsyslogサーバーとして構成する必要があります。インスタンスが構成されると、すべてのsyslogメッセージがNetScaler Consoleにリダイレクトされ、これらのログが構造化された方法でユーザーに表示されるようになります。

Syslogは、通信にUser Datagram Protocol (UDP) のポート514を使用します。UDPはコネクションレスプロトコルであるため、インスタンスへの確認応答は提供されません。syslogパケットサイズは1024バイトに制限されており、以下の情報が含まれています。

- ファシリティ
- 重大度
- ホスト名
- タイムスタンプ
- メッセージ

NetScaler Consoleでは、インスタンスでファシリティとログの重大度レベルを構成する必要があります。

- **ファシリティ** - syslogメッセージは、それらを生成するソースに基づいて大まかに分類されます。これらのソースは、オペレーティングシステム、プロセス、またはアプリケーションである場合があります。これらのカテゴリはファシリティと呼ばれ、整数で表されます。たとえば、0はカーネルメッセージ、1はユーザーレベルメッセージ、2はメールシステムなどに使用されます。ローカル使用ファシリティ（local0からlocal7）は予約されておらず、一般的に使用できます。したがって、事前に割り当てられたファシリティ値を持たないプロセスやアプリケーションは、8つのローカル使用ファシリティのいずれかに振り向けることができます。
- **重大度** - syslogメッセージを生成するソースまたはファシリティは、以下に示すように、1桁の整数を使用してメッセージの重大度も指定します。

  ```
  1 - Emergency: System is unusable.
  ```

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

```
2 - Alert: Action must be taken immediately.


3 - Critical: Critical conditions.


4 - Error: Error conditions.


5 - Warning: Warning conditions.


6 - Notice: Normal but significant condition.


7 - Informational: Informational messages.


8 - Debug: Debug-level messages.
```

NetScalerインスタンスでsyslogを構成するには：

1. NetScaler Consoleで、**Infrastructure > Instances**に移動します。
2. syslogメッセージを収集してNetScaler Consoleに表示するNetScalerインスタンスを選択します。
3. 「**Action**」ドロップダウンリストで、「**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。

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

これにより、NetScalerインスタンス内のすべてのsyslogコマンドが構成され、NetScaler Consoleはsyslogメッセージの受信を開始します。メッセージは、**Infrastructure > Events > Syslog Messages**に移動して表示できます。

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集中管理します。**IPFIX**と**Logstream**は、これらのAppFlowレコードをNetScalerインスタンスからNetScaler Consoleに転送するプロトコルです。詳細については、AppFlowを参照してください。

- **IPFIX**は、RFC 5101で定義されているオープンなInternet Engineering Task Force (IETF) 標準です。**IPFIX**は、一方向のデータフローに使用される信頼性の低いトランスポートプロトコルであるUDPプロトコルを使用します。IPFIXはUDPプロトコルを使用するため、IPFIX標準に準拠すると、NetScaler Consoleでより多くのリソースを処理することになります。
- **Logstream**は、Citrixが所有するプロトコルで、NetScalerインスタンスからNetScaler Consoleに分析ログデータを効率的に転送するためのトランスポートモードの1つとして使用されます。**Logstream**は信頼性の高いTCPプロトコルを使用し、データの処理に必要なリソースが少なくて済みます。

NetScalerの**11.1 Build 47.14から11.1 Build 62.8**のバージョンでは、Web Insight (HTTP) を有効にするためのデフォルトのトランスポートモードは**Logstream**であり、その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はIPFIXです。NetScalerのバージョンが**12.0から最新バージョン**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。

注

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

Logstreamをトランスポートモードとして有効にする

1. **Infrastructure > Instances**に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. **Select Action**リストから、**Configure Analytics**を選択します。

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

3. 仮想サーバーを選択し、**Enable Security & Analytics**をクリックします。

4. **Enable Security & Analytics**ウィンドウで：

   a. インサイトの種類（Web Insight、WAFセキュリティ違反、またはBot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および11.1 Build 62.8**の場合、**Logstream**はWeb Insight (HTTP) を有効にするためのデフォルトのトランスポートモードであり、IPFIXはその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バージョンでは、トランスポートモードとして**Logstream**または**IPFIX**のいずれかを選択できます。

   c. 式はデフォルトでtrueです

   d. **Save Analytics**をクリックします。

   アナリティクスを有効にする(/en-us/netscaler-console-service/media/enable-analytics.png)

   注

   - 管理パーティションの場合、**Web Insight**のみがサポートされます
   - キャッシュリダイレクション、認証、GSLBなどの仮想サーバーでは、アナリティクスを有効にできません。エラーメッセージが表示されます。

次の表は、トランスポートモードとして**Logstream**をサポートするNetScaler Consoleの機能について説明しています。

機能	IPFIX	ログストリーム
ウェブインサイト	•	•
ボットセキュリティ違反	サポートされていません	•

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

機能	IPFIX	ログストリーム
WAFセキュリティ違反	•	•
ゲートウェイインサイト	•	•
HDXインサイト	•	•
SSLインサイト	サポートされていません	•
CR インサイト	•	•
IPレピュテーション	•	•
AppFirewall	•	•
クライアント側測定	•	•
Syslog/Auditlog	•	•

委任管理者ユーザーにより多くの権限を割り当てる方法

組織の最初のユーザーがNetScaler Consoleにサインアップしてログオンすると、そのユーザーにはスーパー管理者権限が割り当てられます。それ以降にログオンするすべてのユーザーには、デフォルトで委任管理者ロールが割り当てられます。委任管理者には、ユーザー管理またはRBAC設定に関連するタスクを表示および実行する権限はありません。

ただし、委任管理者にスーパー管理者権限または特定の非スーパー管理者ロールを割り当てることで、その管理者がユーザー管理に関連するタスクを実行できるようにすることができます。

ロールベースのアクセス制御の詳細については、「ロールベースのアクセス制御の構成」を参照してください。

委任管理者へのスーパー管理者権限の割り当て

委任管理者にスーパー管理者権限を割り当てるには、スーパー管理者がデフォルトの管理者グループを委任管理者ユーザーに割り当てる必要があります。次のタスクを実行します。

1. スーパー管理者としてNetScaler Consoleにログオンします。
2. **アカウント** > **ユーザー管理** > **ユーザー** に移動します。
3. 委任管理者のユーザー名を選択し、**編集** をクリックします。

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

4. グループ **\<*tenant*_*name*\>_admin_group** を委任管理者に割り当て、**OK** をクリックします。たとえば、次の画像では、「example_admin_group」が委任管理者ユーザーに割り当てられています。

委任管理者へのカスタムロールの割り当て

委任管理者にカスタムロールを割り当てるには、スーパー管理者がグループ、ロール、およびポリシーを作成し、委任管理者ユーザーに割り当てる必要があります。これにより、委任管理者は必要な権限のみを持つことが保証されます。次のタスクを実行します。

1. スーパー管理者としてNetScaler Consoleにログオンします。
2. **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。**追加** を選択して、委任管理者が必要とする権限を持つアクセスポリシーを作成します。この例では、ユーザー管理設定への表示アクセスを許可するアクセスポリシー `custompolicy` が作成されます。

3. **アカウント** > **ユーザー管理** > **ロール** に移動します。**追加** を選択してロールを作成し、このロールを前の手順で作成したアクセスポリシーにバインドします。この例では、ロール `customrole` が作成され、`custompolicy` アクセスポリシーにバインドされています。

4. **アカウント** > **ユーザー管理** > **グループ** に移動します。**追加** を選択してグループを作成し、このグループを前の手順で作成したロールにバインドします。この例では、「custom group」グループが作成され、「custom role」ロールにバインドされています。

5. **アカウント** > **ユーザー管理** > **ユーザー** に移動します。
6. 委任された管理者のユーザー名を選択し、**編集** をクリックします。
7. 前の手順で作成したグループを委任された管理者ユーザーに割り当てます。この例では、委任された管理者ユーザーにグループ `customgroup` が割り当てられています。

ServiceNowインスタンスとの統合

NetScaler管理者として、ServiceNowを主要なITリクエストおよびサポートシステムとして使用する場合があります。重要なNetScalerイベントについては、調査、追跡、トラブルシューティングのためにチケットまたはインシデントを起票する必要があります。

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

NetScaler ConsoleとServiceNow用Citrix ITSM connectorを使用して、ServiceNowでのチケット作成を自動化できます。この自動化を開始するには、Citrix ITSMアダプターサービスをオンボードしてイベントを受信し、ServiceNowで関連するインシデントを作成します。準備と統合の手順の詳細については、「Get started in Citrix ITSM Adapter Service」を参照してください。

統合が成功したら、NetScaler ConsoleでServiceNowインシデントの自動生成を設定する。ServiceNowチケットが自動生成されているかどうかを確認するには、次の手順に従います。

1. NetScaler Consoleにログインします。
2. **Settings > Notifications**に移動し、**ServiceNow**を選択します。
3. リストからServiceNowプロファイルを選択します。
4. **Test**をクリックしてServiceNowチケットを自動生成し、構成を確認します。

   NetScaler Console GUIでServiceNowチケットを表示する場合は、**ServiceNow Tickets**を選択します。

NetScaler ConsoleをServiceNowと統合すると、以下のServiceNowインシデントの生成を自動化できます。

- すべてのNetScalerイベント
- 有効期限が近づいているSSL証明書
- NetScaler Consoleライセンスの有効期限イベント

また、NetScaler Consoleイベントポリシーをカスタマイズすることもできます。

NetScalerイベントのServiceNowインシデントを生成する

NetScaler Consoleでは、特定のイベントに対してServiceNowでチケットを自動的に発行するルールを設定できます。NetScaler Consoleは、次のようなイベントに対してServiceNowチケットを自動生成します。

- 仮想サーバーがダウンまたはサービス停止になる。
- リソース消費がしきい値を超過する。
- NetScalerインスタンスのライセンスの有効期限が切れる。

ServiceNowで自動生成されたチケットには、問題の追跡とトラブルシューティングに必要な詳細が含まれています。1つ以上のネットワークデバイスにわたる通知を単一のServiceNowコンソールから管理できます。その後、さらなる分析のために管理者に割り当てます。

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

NetScaler Consoleでイベントルールを作成するには、**インフラストラクチャ > イベント > ルール**に移動します。詳細については、「ServiceNow通知の送信」を参照してください。

有効期限が近づいているSSL証明書のServiceNowインシデントを生成する

NetScalerインスタンスのSSL証明書の有効期限が近づくと、NetScaler ConsoleはServiceNowチケットを自動生成します。これにより、ServiceNowダッシュボードで今後のSSL証明書の有効期限チケットを事前に確認できます。

SSL証明書の有効期限に関するServiceNow通知を送信するには、「SSL証明書の有効期限」を参照してください。

NetScaler Consoleライセンスの有効期限に関するServiceNowインシデントを生成する

NetScaler Consoleでは、特定のNetScaler Consoleライセンスの有効期限イベントに対してServiceNowでチケットを自動的に発行するルールを設定できます。

NetScaler Consoleライセンスの有効期限に関するServiceNow通知を送信するには、「NetScaler Consoleライセンスの有効期限」を参照してください。

NetScaler Consoleイベントポリシーをカスタマイズする

イベント属性に基づいてServiceNowがNetScaler Consoleイベントを処理する方法を制御するポリシーを定義できます。Citrix ITSMコネクタでNetScaler Consoleイベントポリシーを設定します。インシデントがADMでどのように生成、処理、報告されるかを決定できます。その後、ITSMを通じて次のアクションを実行します。

- インシデントを無視
- ダッシュボードにインシデントを表示
- インシデントを作成

詳細については、NetScaler Consoleイベントポリシーをカスタマイズを参照してください。

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

実行可能なタスクと推奨事項

注：

- 「**To Do**」タブは「**推奨事項**」に名称変更されました。「**推奨事項**」では、既存のタスクを引き続き確認し、「**Guide Me**」をクリックしてタスクを完了できます。
- 「**アーカイブ**」タブは利用できなくなりました。代わりに、リストから推奨事項を「**却下**」することを選択できます。

数百の検出されたNetScalerインスタンスがあり、各インスタンスから複数の仮想サーバー（アプリケーション）を設定している場合があります。管理者として、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インサイトを得るために、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ていることを確認する必要があります。

インフラストラクチャをさらに拡張するにつれて、インスタンスとアプリケーションに影響を与え、すぐに注意が必要な重要な問題にも焦点を当てる必要があるかもしれません。また、NetScaler Consoleの展開が効率的で、安全で、準拠していることを確認する必要があります。現在の利用状況とサブスクリプションに基づいて、NetScaler Consoleの「**タスク**」機能は、すぐにアクションを起こす必要がある実行可能な「**タスク**」と、効率的な展開を確実にするための「**推奨事項**」の両方を表示できます。

管理者として、これらの実行可能な「**タスク**」と「**推奨事項**」を使用することで、次のことができます。

- すぐにアクションが必要な観察事項や問題について、即座に可視化できます。
- NetScaler Consoleがタスクを検出するたびに通知を受け取るように設定し、積極的にアクションを起こすことができます。
- NetScaler ConsoleとNetScalerインスタンスの効率的な展開を実現します。
- 重要な問題を特定する際の重要な時間と労力を削減します。
- NetScaler Consoleのすべての機能を活用していることを確認し、展開の効率的な管理のために、製品が推奨する製品検出と機能を有効にします。

NetScaler Console GUIから、「**タスク**」をクリックして「**タスク**」と「**推奨事項**」の両方を表示します。

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

「タスク」(/en-us/netscaler-console-service/media/tasks.png)

- 「**タスク**」 - すぐに注意とアクションが必要なタスクのリストを表示できます。インフラストラクチャを拡張するにつれて、セキュリティ侵害につながるいくつかの重要な問題が見過ごされる可能性があります。例えば、CVEを持つNetScalerインスタンスはすぐに注意が必要であり、インスタンスが推奨されるビルドとバージョンで実行されていることを確認するために、すぐにアクションを起こす必要があります。「**タスク**」では、それらのインサイトをすぐに得ることができます。現在の利用状況に基づいて、合計5つのタスクを表示できます。タスクは重要度（重大および中）に基づいて表示されます。

  セットアップタスク(/en-us/netscaler-console-service/media/set-up-task.png)

- **推奨事項** - 現在の利用状況に基づいて、NetScaler Consoleの展開を改善するための特定の推奨事項を提供します。**Guide Me**オプションを使用して、任意の推奨事項を完了できます。**Guide Me**オプションを使用して完了した推奨事項は、完了済み（Completed）に移動されます。推奨事項を却下することもでき、その場合は**却下済み（Dismissed）**カテゴリに移動されます。却下された推奨事項を表示するには、**ステータス別（By Status）**フィルターを使用し、**却下済み（Dismissed）**を選択して、それらの却下された推奨事項を表示します。

  カテゴリでフィルター（Filter By Category）を使用して、カテゴリ（インフラストラクチャ、アプリケーション、セキュリティ）に基づいて特定の推奨事項をフィルターすることもできます。または、**検索（Search）**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。

  推奨事項(/en-us/netscaler-console-service/media/recommendations.png)

タスク

タスクの下には、現在のNetScaler Consoleの展開状況に応じて、以下の4つのタスクが表示されます。

- **期限切れSSL証明書** – NetScaler Consoleにインストールされている期限切れのSSL証明書に関する情報を提供します。このタスクを選択すると、以下のタブが表示されます。

  - **未使用の証明書を削除**: どのNetScalerインスタンスでも使用されていない証明書を表示します。タスクを完了するには、未使用の証明書を確認し、証明書を選択して、**表示して削除（View and Delete）**をクリックします。

    推奨されるアクション: **インフラストラクチャ > SSLダッシュボード > SSL証明書 - 期限切れ**にリダイレクトされます。証明書を削除するには、**削除（Delete）**をクリックします。

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

証明書を更新する場合は、証明書を選択して更新（Update）**をクリックします。詳細については、「インストール済み証明書を更新する方法」を参照してください。

- **証明書を更新**: すでに期限切れになっている証明書を表示します。タスクを完了するには、証明書を確認し、証明書を選択して、**表示して更新（View and Update）**をクリックします。

  推奨されるアクション: **インフラストラクチャ > SSLダッシュボード > SSL証明書 - 期限切れ**にリダイレクトされます。証明書を選択し、**更新（Update）**または**削除（Delete）**をクリックします。詳細については、「インストール済み証明書を更新する方法」を参照してください。

- **期限切れ間近のSSL証明書** – 期限切れ間近のSSL証明書に関する情報を提供します。

  推奨されるアクション: このタスクを選択すると、有効期限までの合計日数に基づいてタブが表示されます。タスクを完了するには、タブから証明書を選択し、**表示して更新（View and Update）**をクリックします。**インフラストラクチャ > SSLダッシュボード**の関連ページにリダイレクトされます。証明書を選択し、**更新（Update）**をクリックします。詳細については、「インストール済み証明書を更新する方法」を参照してください。

- **構成ドリフト** – NetScalerインスタンスにおける構成の差異（保存済みと実行中の差分、テンプレートと実行中の差分）に関する情報を提供します。このタスクを選択すると、以下のタブが表示されます。

  - **未保存の構成を持つインスタンス**: 未保存の構成を持つインスタンスを表示できます。タスクを完了するには、インスタンスを選択し、**構成を表示して保存（View and Save configuration）**をクリックします。

    推奨されるアクション: **Infrastructure > Configuration > Configuration Audit > Audit Reports** にリダイレクトされ、保存されていない構成を持つインスタンスを表示できます。このタスクを完了するには、**Save Configuration** をクリックします。詳細については、ドキュメントを参照してください。

  - **テンプレートからの逸脱があるインスタンス**: テンプレートからの逸脱があるインスタンスを表示できます。タスクを完了するには、インスタンスを選択し、**View and Run correct commands** をクリックします。

    推奨されるアクション: **Infrastructure > Configuration > Configuration Audit > Audit Reports** にリダイレクトされ、テンプレートからの逸脱があるインスタンスを表示できます。タスクを完了するには、ドキュメントに従ってください。

- **セキュリティアドバイザリ** – NetScalerインスタンスに影響を与えているCVEに関する情報を提供します。このタスクを選択して、次のタブを表示します。

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

- **検出されたCVE**: 検出されたCVEと、そのCVEに影響を受けているNetScalerインスタンスを表示します。このタスクを完了するには、CVEを選択し、**View and Remediate** をクリックします。

  推奨されるアクション: **Infrastructure > Instance Advisory > Security Advisory** の **Security Advisory**ページにリダイレクトされます。タスクを完了するには、ドキュメントに従ってください。

- **影響を受けるインスタンス**: CVEの影響を受けているNetScalerインスタンスを表示します。タスクを完了するには、インスタンスを選択し、**View and Remediate** をクリックします。

  推奨されるアクション: **Infrastructure > Instance Advisory > Security Advisory** の **Security Advisory**ページにリダイレクトされます。タスクを完了するには、ドキュメントに従ってください。

- **アップグレードアドバイザリ**: 90日以内にEnd of Life (EOL)またはEnd of Maintenance (EOM)に達した、または達する予定のNetScaler®インスタンスに関する情報を提供します。

  推奨されるアクション: **Take Action** をクリックし、インスタンスを推奨ビルドにアップグレードします。

- **SSL A+評価アップグレード**: A+評価に準拠していないアプリケーションに関する情報を提供します。

  推奨されるアクション: リストからアプリケーションを選択し、**Upgrade to A+** をクリックします。

  アップグレードが成功すると、次の成功メッセージが表示されます。

  「成功」(/en-us/netscaler-console-service/media/ssl-a-success.png)

  アップグレードが完了すると、アプリケーションの詳細はタスクから削除されます。

  注意点：

  - 選択されたアプリケーションの数によって、アップグレード完了プロセスの所要時間は異なる場合があります。
  - アップグレードプロセスを開始した後、現在進行中のプロセスが完了してから、別のアップグレードプロセスを開始することをお勧めします。

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

- アップグレードプロセスのステータスは、**Infrastructure > Configuration > Configuration Jobs** で確認することもできます。
- アップグレードプロセスが成功しなかった場合は、**Infrastructure > Configuration > Configuration Jobs** でステータスを確認できます。タスクから再度アップグレードプロセスを開始できます。
- 一括アップグレードを実行し、1つ以上のアプリケーションのアップグレードに失敗した場合、タスクで失敗したアプリケーションの詳細のみを表示できます。アップグレードプロセスを再度開始して完了させることができます。

注：

- NetScaler Console に保留中のタスクがない場合、次のページが表示されます。

「タスクなし」(/en-us/netscaler-console-service/media/no-pending-tasks.png)

- シナリオによっては、すべてのインスタンスでチェックが行われるため、すべてのタスクをロードするのに時間がかかる場合があります。

「タスクをロード」(/en-us/netscaler-console-service/media/load-tasks.png)

推奨事項

次の表は、NetScaler Console GUI で表示できる推奨事項について説明しています。

注

プールライセンスの場合、既存のプールライセンスの資格に基づいて推奨事項が表示されます。

推奨事項名	GUIにタスクが表示されるタイミング?
NetScalerインスタンスの追加	NetScaler Consoleにオンボーディングした後、NetScalerインスタンスが検出されない場合。
NetScaler Consoleの最大限の機能を利用するために外部エージェントを追加する	外部エージェントが構成されていない場合。組み込みエージェントから開始できます。ただし、分析、プールライセンスなどのすべての機

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

推奨事項名	GUIにタスクが表示されるタイミング?
	能を使用するには、外部エージェントが必要です。
組み込みエージェントから外部エージェントへのNetScalerの登録	Service Connectワークフローを使用してNetScaler Consoleにオンボーディングした後、NetScalerインスタンスは組み込みエージェントを使用してオンボーディングされます。これらのNetScalerインスタンスを外部エージェントに登録して、分析、プールライセンスなどのすべての機能を使用できます。
NetScalerで帯域幅を再割り当てしますか？簡単です！	プールライセンスがNetScaler GUIで割り当てられており、それらのNetScalerインスタンスがNetScaler Consoleで検出された場合、NetScaler Consoleを使用して再割り当てを行うことができます。
主要なエンタープライズユーザー向けにきめ細かなロールベースのアクセスを有効にする	NetScaler Console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。
ルールを構成して、NetScalerインスタンスの重要なイベントを見逃さないようにする	カスタムイベントルールがまだ設定されていない場合。
複数のアプリケーションとそのパフォーマンスを監視する必要がありますか？カスタムアプリケーションを作成するだけです。	カスタムアプリがまだ設定されていない場合。
アプリケーションの重要なイベントを通知し、見逃さないようにします。	アプリスコアの偏差、サーバー処理時間、クライアントネットワーク遅延、サーバーネットワーク遅延、または応答時間に対してアクションポリシーが設定されていない場合。
アプリケーションの停止を回避し、アプリケーション内の期限切れSSL証明書を見逃さないようにします。	期限切れSSL証明書に対してアラートまたは通知が設定されていない場合。
セキュリティアドバイザリ - NetScalerインスタンスをCVEと緩和策で最新の状態に保ちます。	NetScalerインスタンスにCVEの影響がある場合。

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

推奨事項名	GUIにタスクが表示されるタイミング?
エンタープライズポリシーを設定し、逸脱がないか監視します。	SSLエンタープライズ設定が変更されていないか、まだデフォルトのままの場合。
タスクを手動で繰り返していますか？構成ジョブを作成し、複数のNetScalerインスタンスに適用します。	**Config Job**タスクがまだ設定されていない場合。
選択したカスタムインジケーターを選択して、インスタンススコアを管理および監視します。	**Instance Score Settings**のデフォルト設定と閾値が変更されていない場合。
任意のカスタムインジケーターを選択して、アプリケーションスコアを追跡する	App Dashboard の App Score コンポーネントがデフォルトで使用されており、カスタマイズが行われていない場合。
Geo Map でクライアントリクエストを視覚化するためにプライベートIPブロックを追加する	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 上でクライアントリクエストをマッピングおよび視覚化するためのIPブロックを作成できます。
AppSec 違反をリアルタイムで Splunk にサブスクライブしてエクスポートする	NetScaler Console で Splunk 統合がまだ構成されていない場合。
Kubernetes サービスのためにデフォルトのしきい値をカスタマイズするか、新しいしきい値を作成する	サービスグラフでデフォルトのしきい値のみが使用されており、サービスに単一または二重のしきい値が適用されていない場合。
通知プロファイルを事前に構成し、通信先に通知を受け取る	通知プロファイルがまだ構成されていない場合。
定期的なエクスポートをスケジュールし、インフラストラクチャの詳細に関する通知を受け取る	**Infrastructure > Instances** でエクスポートスケジュールがまだ構成されていない場合。
ServiceNow をお持ちで、ADM との統合を検討していますか？	NetScaler Console で ServiceNow 統合がまだ構成されていない場合。
Venafi と ADM を使用して SSL 証明書管理を自動化する	NetScaler Console に Venafi サーバーがまだ構成されていない場合。

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

推奨事項名	GUIにタスクが表示されるタイミング?
期限切れになる前に、プールされたライセンスを更新してください。	既存のライセンスが30日以内に期限切れになる場合。
購入したプール帯域幅をNetScalerインスタンスに割り当てて、プールライセンスの使用を開始してください。	プールされたライセンスのエンタイトルメントの割り当てをまだ開始していない場合。
より多くのプール帯域幅容量の購入を検討してください。	プールされた帯域幅のエンタイトルメントの90%以上を利用している場合。
現在のプールされた帯域幅のエンタイトルメントは十分に活用されていません。見直し、さらに割り当てることを検討してください。	プールされたライセンス割り当ての利用率が70%未満の場合。

ガイドミーワークフローを使用して推奨事項を完了する方法?

任意のイベントのルールを設定したいとします。次のタスクで**ガイドミー**をクリックします。

ガイドミーをクリックすると、**インフラストラクチャ > イベント > ルール**にリダイレクトされます。**追加**をクリックしてルールを作成します。詳細については、イベントルールの作成を参照してください。

ルールの作成が完了すると、推奨事項は完了となり、**完了済み**に移動されます。

同様に、後で推奨事項を完了したい場合は、リストから**却下**を選択すると、**却下済み**に移動されます。

推奨事項を却下(/en-us/netscaler-console-service/media/dismiss-recommendation.png)

通知を設定する

NetScaler Console が即座の対応が必要な未完了のタスクを特定するたびに、通知を設定して受け取ることができます。通知を設定していない場合は、右上隅にある**通知の設定**をクリックできます。

通知(/en-us/netscaler-console-service/media/create-notification.png)

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

通知ページで、**メール**と**Slack**のプロファイルを設定し、**保存**をクリックして通知を受け取ることができます。通知タイプごとに、NetScaler Console GUI に設定された配布リストまたはプロファイルが表示されます。NetScaler Console は、選択された配布リストまたはプロファイルに通知を送信します。

よくある質問

1. **Guide me** がツールヒントを表示せず、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。エンタープライズ向け Pendo を有効にする 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** でツールヒントが表示されるようになります。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. 管理者向けにどのような種類の推奨事項が提示されますか？

   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、製品の発見を向上させ、管理者は、NetScaler Console にその機能が存在するかどうかを知らなくても、タスクが何を行い、どのように役立つかを知ることができます。

3. 推奨事項を却下するとどうなりますか？

   却下した推奨事項は**却下済み**に移動されます。これらの推奨事項は後で完了できます。

4. Guide me を開始して途中で中断した場合、推奨事項は**完了済み**になりますか？

   いいえ、アクションが保存または完了されない限り、推奨事項は完了しません。

5. 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。

6. 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ることができますか？

   はい！現在、合計4つの実行可能なタスクを表示できます。詳細については、タスクを参照してください。

7. NetScaler ConsoleにNetScalerインスタンスが追加されていない場合でも、すべての実行可能なタスクと20以上の推奨事項が表示されますか？

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

いいえ。すべてのタスクと推奨事項を表示するには、NetScaler ConsoleでNetScalerインスタンスと仮想サーバーの両方が利用可能である必要があります。

8. タスクはどのくらいの頻度で更新されますか？

   左側のナビゲーションペインから**タスク**をクリックすると、タスクが更新され、最新のステータスで利用可能になります。詳細が取得され、更新されます。

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

インスタンスの主要メトリックの詳細を表示する統合ダッシュボード

NetScaler Consoleでは、アプリケーションの使用状況とパフォーマンス、NetScalerインフラストラクチャ、セキュリティ（ボットとWAF）違反などに関するさまざまなインサイトを表示できます。管理者として、複数のインサイトを表示するためにNetScaler Console GUIのさまざまなオプションに移動する必要がある場合があります。たとえば、仮想サーバー（アプリケーション）とNetScalerインスタンスのインサイトを確認するには、次の手順を実行します。

- まず、アプリケーションのインサイトを表示するには、**Applications > Dashboard** に移動する必要があります。
- 次に、NetScalerインスタンスのインサイトを表示するには、**Infrastructure > Infrastructure Analytics** に移動する必要があります。

より良い監視エクスペリエンスのためには、必要なすべてのインサイトの概要を含む権限を持つことが不可欠です。**Overview > Dashboard** に移動して、以下のカテゴリに基づいた主要メトリックの詳細の概要を示すシングルペインダッシュボードを視覚化します。

- アプリケーション
- NetScalerインフラストラクチャ
- アプリケーションセキュリティ
- ゲートウェイ
- API分析

アプリケーション

Applications では、以下を表示できます。

- **Application Health** – **Down** および **Out-of-Service** 状態のアプリケーション、および **Critical**、**In Review**、**Good**、**Not Applicable** などのステータスに基づいたアプリケーションの概要を提供します。App Dashboard で詳細を表示するには、**View All Applications** をクリックします。
- **Golden Signal Anomalies** – サーバーエラーと応答時間の異常があるアプリケーションの概要を提供します。詳細については、**View Details** をクリックしてください。

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

- **Application Config Optimization** – パフォーマンスの問題があるアプリケーションの総数の概要を提供します。アプリダッシュボードで問題の詳細を表示するには、**See More** をクリックします。
- **SSL証明書** – SSL証明書の概要と有効性を提供します。**SSL証明書の管理**をクリックすると、SSLダッシュボードで詳細情報を表示できます。
- **アプリケーションSSL構成の最適化** – SSL関連の問題を抱えるアプリケーション全体の概要を提供します。**詳細を見る**をクリックすると、問題の詳細を表示できます。

NetScalerインフラストラクチャ

NetScalerインフラストラクチャでは、以下のNetScalerインスタンス関連の主要メトリックを表示できます。

- **NetScalerインスタンスの健全性** – インスタンススコアに基づいたNetScalerインスタンス全体の概要を提供します。
- **CVEの影響を受けるNetScalerインスタンス** – 共通脆弱性識別子 (CVE) の影響を受けるNetScalerインスタンス全体の概要を提供します。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。
- **NetScalerインスタンスの問題** – 問題カテゴリに応じたNetScalerインスタンスの問題の概要を提供します。詳細については、インフラストラクチャ分析を参照してください。
- **NetScalerインスタンスアップグレードの概要** – 最新ビルドではないNetScalerインスタンス全体の概要を提供します。詳細については、**NetScalerインスタンスダッシュボードの表示**をクリックしてください。

アプリケーションセキュリティ

選択した期間に報告された影響を受けるアプリケーションの総数と、違反 (ボットおよびWAF) の総数の概要を提供します。**セキュリティダッシュボードの表示**をクリックすると、セキュリティおよびボット違反の詳細を表示できます。

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

ゲートウェイ

アクティブなゲートウェイユーザーの総数、アクティブなICA®ユーザーの総数、およびアクティブなICA接続の総数の概要を提供します。エラー、ユーザーログオンの詳細、およびユーザーの場所に関する詳細を提供する地理マップも表示できます。

API 分析

NetScaler Console を介して構成された API エンドポイントのパフォーマンスと使用状況の概要を提供します。以下を表示できます。

- API エンドポイントのアプリケーションおよびサーバー応答時間の分布。
- アプリケーションおよびサーバー応答時間が高いエンドポイント。

ダッシュボードのカスタマイズ

ダッシュボードの編集オプションを使用して、選択に基づいてダッシュボードビューをカスタマイズできます。**ダッシュボードの編集**オプションを使用すると、次のことができます。

- ウィジェットをドラッグする
- ウィジェット全体を削除する（アプリケーション、NetScaler インフラストラクチャ、Gateway、またはアプリケーションセキュリティ）。
- 各ウィジェットの下にある小さなウィジェットを削除する。
- **ウィジェットの追加**をクリックし、各ウィジェットの下に表示したい必要な主要メトリックを選択します。

- デフォルトにリセット
- 最後に保存した状態にリセット

変更後、「**保存**」をクリックします。

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

「

注

」

- デフォルトでは、すべてのウィジェットが表示されます。ダッシュボードをカスタマイズして変更を保存し、再度「**デフォルトにリセット**」オプションを使用すると、すべてのウィジェットがダッシュボードに追加されます。
- 「**最後に保存した状態にリセット**」オプションは、以前に保存された構成をロードします。

エージェントの詳細を表示

統合ダッシュボードでは、エージェントの詳細の概要を視覚化できます。「**概要 > ダッシュボード**」で、「**エージェントステータス**」の横に、エージェント全体の可用性を分析できる次のステータスが表示されます。

- 「**すべて利用可能**」。すべてのエージェントが稼働中であることを示します。
- 「**すべて利用不可**」。すべてのエージェントがダウンしており、アクセスできないことを示します。
- 「 **利用不可**」。一部のエージェントがダウンしており、アクセスできないことを示します。
- 「**すべてサービス停止中**」。すべてのエージェントがサービス停止中であることを示します。
- 「 **サービス停止中**」。一部のエージェントがサービス停止中であることを示します。
- 「**外部エージェントが見つかりません**」。エージェント（ハイパーバイザー経由）が構成されていないことを示します。

「**詳細を表示**」をクリックすると、組み込みエージェントの合計数、外部エージェントの合計数、エージェントIP、ステータス、システム使用量、診断チェックなどのエージェント詳細の概要を視覚化できます。

フィルターの作成と適用

選択したインスタンスまたはアプリケーションに対してのみ、フィルターを適用してインサイトを表示できます。

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

- アプリケーション
- NetScalerインフラストラクチャ
- アプリケーションセキュリティ

デフォルトでは、すべてのアプリケーションが選択されています。タイルにあるフィルターアイコンをクリックして、ダッシュボードからカスタマイズされたフィルターを作成できます。

アプリケーションのフィルターウィンドウで：

1. **新しいフィルターを作成**を選択します。
2. 選択に基づいてフィルター名を入力します。
3. **アプリケーションの選択**をクリックし、フィルターに必要なすべてのアプリケーションを追加します。アプリケーションを選択する際、フィルター（**アプリケーション名**と**タイプ**）を使用してからアプリケーションを選択することもできます。

4. **フィルターを作成して適用**をクリックします。

フィルターが作成され、適用されました。同じ手順に従って、さらにフィルターを作成できます。フィルターを作成した後、**既存のフィルターからフィルターを選択**リストを通じてフィルターを選択し、適用できます。

フィルターの編集

リストからフィルターを選択し、「**編集**」をクリックしてフィルターを編集できます。編集オプションを使用して、アプリケーションを追加または削除し、フィルターを更新できます。

フィルターの編集(/en-us/netscaler-console-service/media/edit-filters.png)

フィルターを削除するには、リストからフィルターを選択し、「**削除**」をクリックします。

注

アプリケーションを含むフィルターを作成し、アプリケーションダッシュボードでいずれかのアプリケーションが削除された場合、統合ダッシュボードからアプリケーションの詳細がすぐに削除されます。

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

インスタンスの主要なメトリックの詳細を表示するためのカスタムダッシュボードを作成する

統合ダッシュボード (**概要 > ダッシュボード**) と同様に、カスタムダッシュボードを作成することで、選択に基づいてインスタンスのメトリック詳細を表示できます。各ダッシュボードに一意の名前を使用することで、最大30個のダッシュボードを作成できます。管理者として、この機能強化により、複数のダッシュボードを作成し、必要なインスタンスのインサイトのみを監視できるようになります。

まず、**アプリケーション**と**アプリケーションセキュリティ**の主要なメトリックを監視したいとします。

1. **概要 > カスタムダッシュボード**に移動します。
2. **+**をクリックして新しいダッシュボードを作成します。

   カスタムダッシュボードの作成ページで、:

   a. **カスタムダッシュボード名** - ダッシュボードの一意の名前を指定します。

   b. **説明** - 詳細を追加するために簡単な説明を入力します。

   c. **ダッシュボードにウィジェットを追加** - この例では、アプリケーションとアプリケーションセキュリティのウィジェットを追加する必要があります。**アプリケーション**および**アプリケーションセキュリティ**カテゴリから監視したいウィジェットを選択します。

   d. **アプリケーションフィルター** - デフォルトでは、フィルターはすべてのアプリケーションに適用されます。フィルターを作成して、特定のアプリケーションのみを選択することもできます。詳細については、「フィルターの作成と適用」を参照してください。

   e. **保存**をクリックします。

ダッシュボードが正常に作成されました。同様に、各ダッシュボードに一意の名前を指定することで、最大20個のダッシュボードを作成し、選択に基づいてカテゴリを選択できます。

カスタムダッシュボードを作成した後、次のオプションを使用できます。

- **編集**: ウィジェットの追加または削除、フィルターの適用などにより、ダッシュボードを編集できます。
- **名前の変更**: ダッシュボード名を変更できます。
- **削除**: ダッシュボードを削除できます。

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

ダッシュボードのその他のオプション

作成したカスタムダッシュボードでは、次のオプションを使用できます。

- **構成の編集**: このオプションを使用して、ウィジェットの追加または削除、フィルターの適用などにより、ダッシュボードを編集することもできます。
- **レイアウトの編集**: このオプションを使用して、ダッシュボードをさらにカスタマイズできます。
    - 上へ移動、下へ移動、または削除を選択できます。

    - ウィジェットでは、削除オプションを選択して任意のウィジェットを削除できます。

    - ウィジェットを好きな場所にドラッグして配置します。
    - 特定のインサイトの視認性を高めるために、ウィジェットのサイズを増減します。

変更を加えた後、「**保存**」をクリックして、更新されたダッシュボードを表示します。

他のユーザーとダッシュボードを共有する

他のユーザーとダッシュボードを共有できます。既存のダッシュボードを選択し、「**共有**」をクリックします。ユーザー名を入力し、「**招待**」をクリックしてダッシュボードを共有します。割り当てられたユーザーは、ダッシュボードを読み取り専用モードで表示できます。

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

APIセキュリティ

API（Application Programming Interface）は、異なるソフトウェアアプリケーションやシステムが相互に通信できるようにする一連のルール、プロトコル、およびツールです。APIは、アクセス制御、認証、暗号化を適用することで機密データを保護する上で重要な役割を果たし、許可されたエンティティのみが機密情報に安全にアクセスし、送信できるようにします。

APIは、モバイルおよびWebアプリケーションのバックエンドフレームワークとして機能します。そのため、APIが転送する機密データを保護することが重要です。APIセキュリティとは、APIへの攻撃を防止または軽減するための実践を指します。

APIセキュリティにおいて、ゲートウェイはAPIエンドポイントへのすべてのリクエストのエントリポイントとして機能します。そして、システム内のすべてのAPIエンドポイントとマイクロサービスへの安全で信頼性の高いアクセスを保証します。

APIを保護するには、次の手順を実行します。

- API定義を作成またはアップロードする
- APIインスタンスを展開する
- API展開にポリシーを追加する

次の図は、NetScaler ConsoleのAPIセキュリティがクライアントリクエストを受信し、バックエンドAPIサービスから応答を送信する仕組みを示しています。

注:

NetScaler Consoleでは、この機能はプレミアムライセンスを持つユーザーが利用できます。

APIセキュリティの利点

APIセキュリティは、次の利点を提供します。

- **APIエンドポイントを保護する**: APIセキュリティはセキュリティレイヤーを追加し、APIエンドポイントとバックエンドAPIサーバーを次のような攻撃から保護します。
    - バッファオーバーフロー

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

- SQLインジェクション
- クロスサイトスクリプティング
- サービス拒否 (Dos)

- **APIパフォーマンスの監視と向上**: APIセキュリティは、SSLオフロード、認証、認可、レート制限などのサービスを提供します。これらのサービスは、APIのパフォーマンスと可用性を向上させます。

  APIアナリティクスは、APIパフォーマンスメトリックとAPIエンドポイントへの脅威に対する可視性を提供します。詳細については、APIアナリティクスを表示を参照してください。
- **APIトラフィックの管理**: APIセキュリティは、バックエンドAPIインフラストラクチャの複雑さを抽象化します。
- **APIエンドポイントの検出**: APIセキュリティは、組織内のAPIエンドポイントを検出し、**API Discovery**ページに追加します。

APIセキュリティの構成と管理の権限を付与する

管理者として、APIセキュリティの構成と管理に対するユーザー権限を付与するためのアクセスポリシーを作成できます。ユーザー権限には、表示、追加、編集、削除があります。権限を付与するには、次の手順を実行します。

1. **Settings > User & Roles > Access policies**に移動します。
2. **Add**をクリックします。
3. **Create Access Policies**で、ポリシー名と説明を指定します。
4. **Permissions**フィールドで、**Applications**を展開し、次に**API Security**を展開します。
5. 必要な**API Security**ページを選択します。次に、付与する権限を選択します。

APIセキュリティ管理権限の付与(/en-us/netscaler-console-service/media/api-gateway-management-permissions.png)

重要:

APIセキュリティを使用するために必要な機能の権限を付与してください。たとえば、**展開**ページへのユーザーアクセスを許可する場合、以下の機能にもユーザーアクセスが必要です。

- StyleBooks

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

- IPAM
- 負荷分散（**ネットワーク機能**配下）
- コンテンツスイッチング（**ネットワーク機能**配下）
- デバイスAPIプロキシ（**API**配下）

アクセスポリシーの詳細については、NetScaler Consoleでアクセスポリシーを構成するを参照してください。

API定義を作成またはアップロードする

API定義は、OpenAPI Specification標準を使用してAPIを記述するドキュメントです。この定義には、APIリソースパスとそれらを操作するためのメソッドを含めることができます。API定義をNetScaler Consoleに追加し、APIゲートウェイ (NetScaler) に展開できます。

API定義は、次のいずれかの方法で作成できます。

- Swagger OAS仕様ファイルをアップロードする
- 独自のAPI定義を作成する

注:

現在、NetScaler Consoleは、**Swagger 2.0** または **openapi 3.0.1** を使用するOAS仕様ファイルの解析をサポートしています。

OAS仕様をアップロードする

OAS仕様はNetScaler Console GUIにアップロードできます。

1. **Security > API Security > API Definitions** に移動します。
2. **Add** をクリックします。
3. **Upload OAS Specification** を選択します。

   注:

   OAS仕様ファイルがYAMLまたはJSON形式であることを確認してください。また、このファイルには外部参照を含めないでください。

4. ローカルコンピューターからOAS仕様を参照し、NetScaler Consoleにアップロードします。

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

API定義を作成する

NetScaler Console GUIで独自のAPI定義を作成できます。

1. **Security > API Security > API Definitions** に移動します。
2. **Add** をクリックします。
3. **Create Your Definition** を選択し、以下を指定します。

   - **名前** - API定義の名前。
   - **API定義** - 定義には、タイトル、バージョン、ベースパス、ホストを含める必要があります。**ホスト** フィールドには、ドメイン名またはIPアドレスを指定できます。
   - **APIリソース** - 定義に複数のAPIリソースを追加します。各リソースにはパスとサポートされているメソッドがあります。**Add** をクリックします。リソースは **Added Resources** テーブルに追加されます。APIリソースを削除するには、**Delete** をクリックします。

   API定義を作成する(/en-us/netscaler-console-service/media/create-an-api-definition.png)
4. **Create** をクリックします。

API定義を表示する

API定義 ページには、アップロードされた定義が一覧表示されます。**View** をクリックして、以下のAPI定義の詳細を表示します。

- **名前** – API定義の名前を表示します。
- **API定義** – 定義のタイトル、バージョン、ベースパス、ホストを表示します。
- **APIリソース** – API定義内のAPIリソースと、それらを操作するためのメソッドを一覧表示します。

APIインスタンスを展開する

APIインスタンスを展開するには、APIプロキシが必要です。APIプロキシは、APIセキュリティ(NetScalerインスタンス) がAPIクライアントからAPIトラフィックを受信するフロントエンド仮想サーバーです。APIクライアントには、ブラウザ、モバイルアプリケーションなどがあります。

APIプロキシは、異なるAPI展開で共有できます。多数のAPIサービスを持つ組織では、各APIサービスに対して個別のAPIプロキシを作成できます。または、異なるAPIサービスのAPIインスタンスとAPIプロキシを作成して共有することもできます。

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

例えば、2つのAPIサービス `app1` と `app2` は、同じAPIセキュリティに展開され、同じフロントエンド仮想サーバーを使用しています。両方のAPIサービスに同じ仮想IPアドレスとSSL証明書情報を提供したいとします。この場合、必要な情報を持つAPIプロキシを追加し、個別の展開と共有できます。そのため、異なる展開上のAPIサービスは、共有APIプロキシを使用してリクエストを受信できます。

管理者として、APIインスタンスを展開するには、次の手順を実行します。

1. APIプロキシを追加する。
2. APIプロキシを使用してAPIインスタンスを展開する。

APIプロキシを追加する

APIプロキシを追加する手順は次のとおりです。

1. **Security > API Security > API Proxy > Add** に移動します。
2. 以下を指定します。

   - **プロキシ名** – APIプロキシの名前。
   - **ターゲットNetScalerインスタンス** - APIゲートウェイとして機能するNetScalerインスタンスを選択します。
   - **IPアドレス** – APIサービスをホストしている仮想サーバーのIPアドレス。
   - **ポート** – APIサービスをホストしている仮想サーバーのポート番号。
   - **プロトコル** – APIプロキシで受信したいトラフィックの種類（HTTPまたはHTTPS）に応じてプロトコルを設定します。
   - **TLSセキュリティプロファイル** – リストから「高」または「中」を選択します。「高」を選択した場合、NetScalerインスタンスのA+評価のSSLプロファイルにマッピングされます。
   - **証明書ストア** - APIセキュリティ用のSSL証明書を選択します。NetScalerエージェント証明書ストアは、SSL証明書を一元的に保存および管理するのに役立ちます。

     NetScalerエージェント証明書ストアでは、SSL証明書をNetScalerエージェントに保存し、NetScaler構成時に再利用できます。

     注:

     既存の展開でNetScalerエージェント証明書ストアにないSSL証明書またはキーを使用している場合は、同じ名前で証明書とキーをストアに追加する必要があります。

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

- **サービスFQDN** – APIサービスがホストされている完全修飾ドメイン名。例: `api.example.com`

または、IPアドレスを割り当てるIPAMネットワークを選択できます。IPAMネットワークから割り当てられたIPアドレスを表示するには、**設定 > IPAM**に移動します。IPAMの詳細については、IPAMの構成を参照してください。

3. 展開構成を保存するには、**保存**をクリックします。

このAPIプロキシをAPIセキュリティに展開する場合は、**保存して展開**をクリックします。

APIプロキシを追加した後、APIインスタンスを展開します。

APIプロキシを使用してAPIインスタンスを展開する

APIインスタンスを展開する手順は次のとおりです。

1. **セキュリティ > APIセキュリティ > 展開**に移動します。
2. 「**追加**」をクリックします。
3. 「**デプロイメント基本**情報」で、,

   a. 「**デプロイメント名**」を指定します。

   b. 「**API定義**」で、必要なAPI定義を選択します。

   c. このデプロイメントで使用する「**APIプロキシ**」を選択します。

4. 「**アップストリームサービス**」で、「**追加**」をクリックして、APIトラフィックをエグレスするバックエンド（オリジン）APIサーバーを追加します。アップストリームサービスは、ドメイン名またはIPアドレスで構成できます。

   APIインスタンスの展開中に、SNIPアドレスとネットマスクの詳細を指定できます。NetScalerインスタンスは、指定されたSNIPアドレスを使用してアップストリームサービス（バックエンド）と通信します。指定されたSNIPアドレスは、アップストリームサービスに送信されるエグレストラフィックの送信元IPアドレスになります。IPAMを使用してSNIPアドレスとネットマスクを構成することもできます。SNIPアドレスを構成しない場合、NetScalerインスタンスのデフォルトのSNIPアドレスがアップストリームサービスの送信元IPアドレスになります。

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

> **注:**
>
> デフォルトでは、SNIPアドレスとネットマスクのオプションは任意です。ただし、これらのオプションのいずれかを指定する場合は、もう一方のオプションも指定する必要があります。

a. アップストリームサービスに名前を指定します。

b. ドメインを指定します。

c. 「**サービス**」で、IPアドレスとポート値を指定します。IPアドレスを追加するには、「**新しい行を追加**」をクリックします。

d. 「**追加**」をクリックします。

5. 「**ルーティング**」で、リソースパスプレフィックスに基づいて受信APIトラフィックをルーティングするために、次の詳細を指定します。

a. ルート名を指定します。

b. APIリクエストを受信する**APIリソース**を選択します。

> **注:**
>
> カスタムパスまたはパスプレフィックスを指定することもできます。

c. APIトラフィックを転送する先のリストから**アップストリームサービス**を選択します。

6. **保存**をクリックして、展開構成を保存します。

構成をAPIセキュリティに展開する場合は、**保存して展開**をクリックします。

API展開(/en-us/netscaler-console-service/media/api-deployment.png)

API分析を有効にする

展開の分析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。

展開のAPI分析を有効にするには、次の手順を実行します。

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

1. **セキュリティ > APIセキュリティ > 展開**で、API分析を有効にする展開を選択します。
2. **分析を有効にする**をクリックします。
3. 「**Configure Analytics for deployment**」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. インサイトの種類（Web Insight、Security Insight、Bot Insight）を選択します。
   b. トランスポートモードとして「**Logstream**」または「**IPFIX**」を選択します。

      IPFIXとLogstreamの詳細については、Logstreamの概要を参照してください。

      式はデフォルトでtrueです。
   c. 「**OK**」をクリックします。

NetScaler Consoleは、選択した仮想サーバーでアナリティクスを有効にします。

API展開にポリシーを追加する

APIトラフィックに対してさまざまなセキュリティポリシーを設定できます。この設定では、トラフィック選択基準とポリシーに必要なパラメータを指定する必要があります。API定義にポリシーを追加するには、次の手順を実行します。

1. **Security > API Security > Policies** に移動します。
2. **Add** をクリックします。
3. ポリシーグループの名前を指定します。
4. リストから**Deployment** を選択します。
5. ポリシーを設定する**Upstream Service** をリストから選択します。
6. トラフィックセレクターとポリシータイプを選択するには、**Add** をクリックします。

   Traffic selector - トラフィック選択基準には、APIリソースパスまたはパスプレフィックス、メソッド、およびポリシーが含まれます。

   トラフィック選択基準を指定するには、次のいずれかのオプションを使用できます。

   - **API Resources** – ポリシーを適用するAPIリソースとそのメソッドを選択します。キーワードでAPIリソースとメソッドを検索できます。

     Traffic selector の画像(/en-us/netscaler-console-service/media/create-policy-api-definition.png)

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

この例では、`POST` メソッドを持つ `/user` のAPIリソースが一覧表示されます。

- **Custom Rule** – このタブでは、カスタムパスプレフィックスと複数のメソッドを指定できます。

  設定されたポリシーは、APIトラフィック選択のカスタムルールに一致する受信APIリクエストに適用されます。

  この例では、**No-Auth** ポリシーは、`/bill` プレフィックスと `GET` メソッドを持つ API リソースに適用されます。

ポリシーで、選択したAPIリソースとメソッドに適用するポリシーをリストから選択します。各ポリシーの詳細については、ポリシーの種類を参照してください。

7. オプションで、ポリシーの種類を移動して優先順位を設定できます。優先順位が高いポリシーの種類が最初に適用されます。
8. ポリシーを追加するには、**保存**をクリックします。ポリシーをすぐに適用する場合は、**保存して適用**をクリックします。

ポリシーの種類

APIポリシーを設定する際に、APIリソースとメソッドに適用する以下のポリシーを選択できます。

- **認証と認可**
- **レート制限**
- **WAF**
- **BOT**
- **ヘッダー書き換え**
- **URIパス書き換え**
- **拒否**

注:

APIを使用してAPIセキュリティを管理するには、APIを使用してAPIセキュリティを管理するを参照してください。

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

認証と認可

APIリソースは、アプリケーションまたはAPIサーバーでホストされます。このようなAPIリソースにアクセス制限を適用したい場合は、認証および認可ポリシーを使用できます。これらのポリシーは、受信APIリクエストがリソースにアクセスするために必要な権限を持っているかどうかを検証します。

選択したAPIリソースの認証と認可を定義するには、次のポリシーを使用します。

`No-Auth`

選択したトラフィックの認証をスキップするには、このポリシーを使用します。

`Auth-Basic`

このポリシーは、HTTP基本認証スキームで使用されるローカル認証を指定します。ローカル認証を使用するには、NetScalerでユーザーアカウントを作成する必要があります。

`OAuth`

OAuthでは、oAuth2を使用してクライアントを認証し、アクセストークンを発行するために外部IDプロバイダーが必要です。クライアントがこのトークンをAPIゲートウェイへのアクセス資格情報として提供すると、設定された値に基づいてトークンが検証されます。

- **JWKS URI** - JWT (JSON Web Token)検証用のJWK (JSON Web Key)を持つエンドポイントのURL
- **Issuer** - 認証サーバーのID (通常はURL)。
- **Audience** - トークンが適用されるサービスまたはアプリケーションのID。
- **Claims to save** - アクセス権限は、一連のクレームと期待値として表されます。クレーム値をCSV形式で指定します。
- **Introspect URI** - 認証サーバーのイントロスペクションエンドポイントURLです。このURLは、不透明なアクセストークンを検証するために使用されます。これらのトークンの詳細については、「不透明なアクセストークンのOAuth設定」(/ja-jp/citrix-adc/current-release/aaa-tm/authentication-methods/oauth-authentication/api-authentication-with-adc.html#oauth-configuration-for-opaque-access-tokens)を参照してください。

  Introspect URI を指定した後、認証サーバーにアクセスするための **Client Id** と **Client Secret** を指定します。
- **Allowed algorithms** - このオプションを使用すると、受信トークン内の特定のアルゴリズムを制限できます。デフォルトでは、サポートされているすべてのメソッドが許可されています。ただし、選択したトラフィックに必要なアルゴリズムを確認できます。

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

検証が成功すると、API Securityはクライアントへのアクセスを許可します。

重要:

選択したAPIリソースに対してOAuthまたは**Auth-Basic**ポリシーを構成する場合、残りのAPIリソースに対しては**No Auth**ポリシーを構成します。この構成は、残りのリソースの認証をスキップしたいことを明示的に示します。

承認

このポリシーは、APIリソースにアクセスするために必要な権限を検証します。アクセス権限は、一連のクレームと期待値として表されます。このポリシーを構成するには、「**Add a new Claim**」を選択し、以下を指定します。

- クレーム名
- クレーム値

重要:

API Securityは、APIトラフィックに対して認証ポリシーと承認ポリシーの両方を必要とします。したがって、認証ポリシーとともに承認ポリシーを構成する必要があります。認証ポリシーはOAuthまたは`Auth-Basic`のいずれかです。

承認チェックがない場合でも、空のクレームを持つ承認ポリシーを作成する必要があります。そうしないと、リクエストは403エラーで拒否されます。

レート制限

選択したAPIリソースに与えられる最大負荷を指定します。このポリシーを使用すると、APIトラフィックレートを監視し、予防措置を講じることができます。このポリシーを構成するには、以下を指定します。

- **HTTP ヘッダー名** - API リクエストを識別するためにトラフィックをフィルタリングするトラフィックセレクターキーです。レート制限ポリシーは、このような API リクエストにのみ適用され、監視します。
- **ヘッダー値** - これらのヘッダー値は、指定されたヘッダー名に対してカンマで区切られます。
- **しきい値** - 指定された間隔で許可されるリクエストの最大数です。**ヘッダー値**を指定した場合、このしきい値は各ヘッダー値に適用されます。

  例-1：

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

ヘッダー名 `x-api-key` にヘッダー値 (`"key1","key2","key3"`) を指定し、しきい値を `80` に設定すると、設定されたしきい値は各ヘッダー値に適用されます。

例-2：

各ヘッダー値に異なるしきい値を指定したい場合は、同じ HTTP ヘッダー名を使用して個別のレート制限ポリシーを作成します。

- **ポリシー-1**：ヘッダー名 `x-api-key` にヘッダー値 (`"key1","key2"`) を指定し、しきい値を `80` に設定します。
- **ポリシー-2**：ヘッダー名 `x-api-key` にヘッダー値 (`"key3"`) を指定し、しきい値を `30` に設定します。

ヘッダー値を指定しない場合、しきい値は指定された HTTP ヘッダー名に適用されます。

- **タイムスライス** - マイクロ秒で指定される間隔です。この間隔中、リクエストは設定された制限に対して監視されます。デフォルトでは、1000マイクロ秒 (1ミリ秒) に設定されています。
- **制限タイプ** - レート制限ポリシーを適用する方法のモードです。**バースト**または**スムーズ**制限タイプを選択できます。
- **アクション** - しきい値を超過したトラフィックに対して実行するアクションを定義します。次のいずれかのアクションを指定できます。
  - **DROP**：設定されたトラフィック制限を超過したリクエストを破棄します。
  - **RESET**：リクエストの接続をリセットします。
  - **REDIRECT**: トラフィックを設定されたredirect_urlにリダイレクトします。
  - **RESPOND**: 標準応答(`429 Too many requests`)で応答します。

WAF

このポリシーは、機密性の高いビジネス情報や顧客情報にアクセスするウェブサイトに対するセキュリティ侵害、データ損失、および不正な変更の可能性を防止します。

WAFポリシーを設定する前に、StyleBooksを使用してNetScaler ConsoleでWAFプロファイルを作成します。

WAFプロファイル名で、作成したWAFプロファイルを選択または指定します。

ボット

このポリシーは、不正なボットを識別し、高度なセキュリティ攻撃からアプライアンスを保護します。

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

BOTポリシーを設定する前に、StyleBooksを使用してNetScaler ConsoleでBOTプロファイルを作成します。

ボットプロファイル名で、作成したBOTプロファイルを指定します。

ヘッダー書き換え

このポリシーは、APIリクエストとレスポンスのヘッダーを変更するのに役立ちます。HTTPヘッダーの値を置き換えたい場合は、以下を指定します。

- **HTTPヘッダー名**: リクエストヘッダーで変更したいフィールド名。

  例: `Host`

- **ヘッダー値**: オプション。指定されたヘッダー名で変更したい値の文字列。

  例: `sample.com`

- **ヘッダーの新しい値**: 指定されたヘッダー値を置き換える新しい値です。

  ヘッダー値が指定されていない場合、受信した値を**HTTPヘッダー名**に指定された値で置き換えます。

  例: `example.com`

この例では、ヘッダー書き換えポリシーは、APIリクエストの`Host`フィールドで`sample.com`を`example.com`に置き換えます。

URIパスの書き換え

このポリシーは、APIリクエストとレスポンスのURIパスを変更するのに役立ちます。URIパス内のセグメントを置き換えたい場合は、次のいずれかのルールを追加します。

- **パスセグメントの置き換え** – このアクションタイプを選択すると、以下を指定します。
  - **現在のパスセグメント** – 置き換えたいパスセグメントです。
  - **新しいパスセグメント** – 現在のパスセグメントのみを置き換える新しいパスセグメントです。

  たとえば、URIパスのロケールを英語から中国語に変更するには、**現在のパスセグメント**に`/ja-jp/`を指定します。そして、**新しいパスセグメント**に`/zh-zh`を指定します。これにより、パスセグメントのみが置き換えられ、残りのURIパスは保持されます。

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

- **フルパスの置き換え** – このアクションタイプは、APIリクエストとレスポンスのURIパスを指定されたパスで完全に置き換えます。**新しいパスセグメント**に`/example.html`を指定すると、APIリクエストまたはレスポンスのURIパスは指定されたパスに変更されます。
- **パスセグメントの削除** – このアクションは、指定されたセグメントをURIから削除します。たとえば、URIパスから英語ロケールを削除するには、**現在のパスセグメント**に`/ja-jp/`を指定します。
- **パスセグメントの挿入** – このアクションは、指定されたセグメントをURIパスに挿入します。このルールを適用するには、セグメントを挿入したい位置と、挿入したいセグメントを指定します。

  たとえば、特定のテキストの直後にセグメントを挿入したい場合は、次の手順を実行します。

  a. 新しいセグメントを挿入する位置を指定します。
  b. **現在のパスセグメント**で、新しいセグメントを追加するテキストを指定します。
  c. **新しいパスセグメント**で、追加するセグメントを指定します。

拒否

このポリシーは、APIリクエストがAPIリソースに到達するのを拒否するのに役立ちます。

API分析を表示

API分析により、APIトラフィックの可視性が向上します。この分析により、IT管理者はAPIゲートウェイによって提供されるAPIインスタンスとエンドポイントを監視できます。APIリクエストの統合された定期的な監視を提供します。

API分析を監視する前に、以下を完了していることを確認してください。

1. API定義を追加する
2. API定義を展開する
3. API定義にポリシーを追加する
4. APIインスタンスにライセンスを適用する
5. APIインスタンスでWeb Insightを有効にする

API分析では、API定義の一部として追加されたAPIインスタンスとエンドポイントの応答時間を監視できます。また、APIインスタンスとエンドポイントによって消費される帯域幅も表示されます。

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

デフォルトでは、ダッシュボードには過去1時間のAPI分析が表示されます。期間を選択して、その間隔のAPI分析を表示できます。各タイルで**詳細を見る**をクリックすると、リスト全体が表示されます。このビューでは、**地理的位置**タイルを除き、APIインスタンスとエンドポイントを部分名で検索できます。

APIエンドポイントの分布

このグラフは、APIエンドポイントのアプリケーションおよびサーバー応答時間の分布を表示します。応答時間が非常に長いAPIエンドポイントを特定し、必要な措置を講じることができます。

APIエンドポイントは、応答時間制限に応じて、次のいずれかの色で表示されます。

- **緑** – 応答時間が30ミリ秒未満の場合。
- **オレンジ** – 応答時間が30～100ミリ秒の場合。
- **赤** – 応答時間が100ミリ秒を超える場合。

APIインスタンス

APIインスタンスタイルには、アプリケーションおよびサーバーの応答時間が高い上位APIインスタンスが表示されます。

APIインスタンス(/en-us/netscaler-console-service/media/api-instances.png)

APIインスタンスを選択して、そのパフォーマンス、使用状況、およびセキュリティの詳細を表示します。選択したAPIインスタンスには、次の情報が表示されます。

- APIエンドポイント数
- リクエスト数
- アプリケーションおよびサーバーの応答時間
- 消費帯域幅
- 認証失敗

APIインスタンスダッシュボード(/en-us/netscaler-console-service/media/api-instance-dashboard.png)

APIエンドポイント

APIエンドポイントタイルには、アプリケーションおよびサーバーの応答時間が高い上位エンドポイントが表示されます。

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

パフォーマンス、使用状況、セキュリティの詳細を表示するには、APIエンドポイントを選択します。

認証の失敗

認証の失敗タイルには、認証の失敗が多い上位のAPIエンドポイントが表示されます。認証の失敗または成功は、API定義に追加されたポリシーに基づいて発生します。

APIエンドポイントでの認証の失敗率と成功率を表示するには、次の手順を実行します。

1. **APIエンドポイント**からエンドポイントを選択します。
2. **セキュリティ**タブを選択します。このタブには、選択したエンドポイントでの認証の失敗と成功が表示されます。

インスタンスのAPIエンドポイントでの認証の失敗率と成功率を表示するには、次の手順を実行します。

1. **APIインスタンス**からインスタンスを選択します。
2. **セキュリティ**タブを選択します。このタブには、選択したインスタンスのエンドポイントでの認証の失敗と成功が表示されます。

さまざまなAPIインサイトを表示

API Analyticsをナビゲートして、次の特定の情報を表示します。

- API分析を表示
  - APIエンドポイントの分布
  - APIインスタンス
  - APIエンドポイント
  - 認証の失敗
  - さまざまなAPIインサイトを表示
    - インスタンス内の上位APIエンドポイントを表示
    - 最もアクセスされたAPIを表示
    - エンドポイントの地理的位置を表示
    - HTTPS応答ステータスを表示
    - APIリクエストの傾向を表示

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

- エンドポイントの帯域幅消費量を表示
- SSLエラーと使用状況を表示

インスタンス内の上位APIエンドポイントを表示

API Analyticsページには、応答時間の長い上位エンドポイントが表示されます。インスタンスの類似エンドポイントを表示する場合は、**API Instances**からインスタンスを選択します。

Top API Endpointsタイルには、アプリケーションおよびサーバーの応答時間が長いエンドポイントが表示されます。

「上位APIエンドポイント」(/en-us/netscaler-console-service/media/top-api-endpoints.png)

最もアクセスされたAPIを表示

API Analyticsで、APIインスタンスからAPIインスタンスを選択します。**Most Accessed APIs**タイルには、リクエストと帯域幅が多い上位のエンドポイントが表示されます。

「最もアクセスされたエンドポイント」(/en-us/netscaler-console-service/media/most-accessed-apis.png)

エンドポイントの地理的位置を表示

1. **API Analytics**で、次のいずれかを選択します。
   - **API Instances**からインスタンスを選択し、選択したインスタンスのエンドポイントがリクエストを受信した場所を表示します。
   - **API Endpoints**からエンドポイントを選択し、そのエンドポイントがリクエストを受信した場所を表示します。
2. **Performance and Usage**に、**Geo Locations**タイルが表示されます。

   応答時間、帯域幅、リクエストに基づいて場所を並べ替えることができます。

「エンドポイントの地理的位置」(/en-us/netscaler-console-service/media/geo-location-apis.png)

HTTPS応答ステータスを表示

HTTPS Response Statusタイルには、応答ステータスとその理由および発生回数が表示されます。HTTPS応答ステータスは、次のいずれかの方法で表示できます。

- **API Instances**からインスタンスを選択します。
- **API Endpoints**からエンドポイントを選択します。

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

このタイルは、**パフォーマンスと使用状況**タブに表示されます。

APIリクエストの傾向を表示

APIエンドポイントからエンドポイントを選択します。**パフォーマンスと使用状況**で、**合計リクエスト**タイルは、エンドポイントが受信した合計リクエスト数の傾向を表示します。

レート制限のためにドロップされたリクエストの傾向を表示したい場合は、**APIインスタンス**からインスタンスを選択します。**セキュリティ**で、**レート制限**タイルは、ドロップされたリクエストの傾向を表示します。また、エンドポイントが受信した合計リクエストの傾向も表示します。

この比較により、合計リクエストのうち、レート制限のためにドロップされたリクエストの数を特定できます。

エンドポイントの帯域幅消費量を表示

エンドポイントによる帯域幅消費の傾向を表示するには、APIエンドポイントからエンドポイントを選択します。**帯域幅**タイルには、帯域幅消費グラフが表示されます。

SSLエラーと使用状況を表示

APIインスタンスからインスタンスを選択します。**セキュリティ**で、次のタイルが表示されます。

- **SSLエラー** – クライアントおよびアプリケーションサーバーで発生したSSL障害を表示します。
- **SSL使用状況** – SSL証明書、プロトコル、暗号、およびキーの強度と、それらの発生回数を表示します。

エンドポイントでのSSL使用状況を表示するには、APIエンドポイントからエンドポイントを選択します。**SSL使用状況**タイルが**セキュリティ**タブに表示されます。

APIエンドポイントの検出

API Securityを使用して、組織内の検出されたAPIエンドポイントを表示できます。NetScaler Consoleは、NetScalerインスタンスおよびAPI展開で受信したAPIトラフィックに基づいてAPIエンドポイントを検出します。

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

NetScaler Consoleの **Security > API Security > API Discovery** ページに、検出されたAPIエンドポイントが表示されます。

- **仮想サーバー** - **VServer** タブには、NetScalerインスタンスからの仮想サーバーが表示されます。仮想サーバーは、指定された期間にAPIリクエストを受信すると、このタブに表示されます。
- **API展開** - このタブには、API定義を使用してNetScaler Consoleから展開されたAPI展開が表示されます。API展開が指定された期間にAPIリクエストを受信すると、このタブはAPIエンドポイントを検出します。API定義を追加して展開するには、「API定義の追加」および「API定義の展開」を参照してください。

注：

- 仮想サーバーで分析を設定し、Web Insightsを有効にしてください。「APIインスタンスでWeb Insightを有効にする」を参照してください。
- **API展開** タブの下で検出されたAPIエンドポイントにのみポリシーを追加できます。

APIエンドポイントの表示

API Discovery で仮想サーバーまたはAPI展開を選択すると、NetScaler Console GUIにAPIエンドポイントとその詳細が次のように表示されます。

- **メソッド** - APIエンドポイントで使用されるメソッドが表示されます。たとえば、`GET` メソッドと `POST` メソッドです。
- **合計リクエスト数** - APIエンドポイントでのAPIリクエストの数が表示されます。
- **応答ステータス** - 各応答ステータスの数が表示されます。たとえば、`2xx`、`3xx`、`4xx`、および `5xx` です。
- **仕様で検出** - この列はAPI展開にのみ表示されます。API定義の一部ではない内部APIが外部からトラフィックを受信することがあります。この列は、APIエンドポイントと観測されたメソッドがAPI定義の一部であるかどうかを識別するのに役立ちます。

仮想サーバー内のAPIエンドポイントは次のとおりです。

仮想サーバー内のAPIエンドポイント(/en-us/netscaler-console-service/media/vserver-api-endpoints.png)

API展開におけるAPIエンドポイントは、以下のとおり利用可能です。

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

仮想サーバー内のAPIエンドポイント(/en-us/netscaler-console-service/media/api-deployment-endpoints.png)

必要なAPIエンドポイントを選択して、詳細な分析レポートを表示することもできます。

詳細なAPIエンドポイントレポート(/en-us/netscaler-console-service/media/detailed-api-endpoint-report.png)

各セクションの詳細については、API分析の表示を参照してください。

検出されたAPIエンドポイントからAPI定義を作成する

検出されたAPIエンドポイント（APIリソースとメソッド）からAPI定義を作成するには：

1. **Security > API Security > API Discovery** に移動して、仮想サーバーとAPI展開のリストを表示します。
2. **VServers** タブで任意の仮想サーバーをクリックします。
3. 仮想サーバーページに検出されたエンドポイントのリストが表示されます。任意のエンドポイントを選択し、**Create API Definition** をクリックします。

API定義の更新(/en-us/netscaler-console-service/media/api-gateway-create-api-definition.png)

注：

エンドポイントを選択せずに **Create API Definition** をクリックすると、すべてのエンドポイントに対してAPI定義を作成するかどうかを確認するポップアップウィンドウが表示されます。すべてのエンドポイントでAPI定義を作成するには **Yes** をクリックし、それ以外の場合は **No** をクリックします。

すべてのエンドポイントのポップアップメッセージ(/en-us/netscaler-console-service/media/api-definition-all-endpoints-msg.png)

1. 「**API定義の作成**」で、以下を指定します:
   - **名前** - API定義の名前。
   - **API定義** - 定義には、タイトル、バージョン、ベースパス、ホストを含める必要があります。「**ホスト**」フィールドには、ドメイン名またはIPアドレスを指定できます。
   - **APIリソース** - 定義に複数のAPIリソースを追加します。各リソースにはパスとサポートされているメソッドがあります。
2. 「**定義の作成**」をクリックして、API定義を作成します。

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

注:

APIリソースパスをAPI定義に追加する前に編集する場合は、API定義画面でAPIリソースの並べ替え機能または検索機能を使用します。

たとえば、「/api/products/123-3243-2344334/reviews」という名前のAPIリソースを考えます。ここで、パスセグメント「123-3243-2344334」は可変の製品IDです。APIリソースを並べ替えて、リソースパスを「/api/products/{id}/reviews」として追加し、「/api/products/123-3243-2344334/reviews」のようなIDを持つすべてのAPIエンドポイントを削除できます。

検出されたAPIエンドポイントで既存のAPI定義を更新する

既存のAPI定義をAPIエンドポイント (APIリソースとメソッド) で更新するには:

1. 「**Security > API Security > API Discovery**」に移動して、仮想サーバーとAPI展開のリストを表示します。
2. 「**VServers**」タブで任意の仮想サーバーをクリックします。
3. 仮想サーバーページには、検出されたエンドポイントのリストが表示されます。既存のAPI定義に追加するエンドポイントを選択します。「**Update existing API Definition**」をクリックします。

4. 「**既存のAPI定義を選択**」ドロップダウンリストから、更新するAPI定義を選択します。「**定義を更新**」をクリックします。
5. 「**既存のAPI定義を更新**」ページが表示されます。「**APIリソース**」セクションには、次の表が表示されます。

   - **追加されたリソース** - 選択したAPIエンドポイント
   - **既存のリソース** - API定義ですでに利用可能なAPIエンドポイント

   注:

   同じAPIエンドポイントが「**追加されたリソース**」と「**既存のリソース**」の両方で利用可能な場合、そのエンドポイントはAPI定義に1回だけ追加されます。

6. 「**定義を更新**」をクリックします。

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

APIインスタンスのデプロイ解除

NetScalerインスタンスからAPIインスタンス構成を削除し、NetScaler ConsoleにAPIインスタンスオブジェクトを下書きとして保持したい場合に、デプロイ解除オプションを使用できます。このアクションにより、デプロイステータスが「下書き」に設定されます。また、デプロイ済みのAPIインスタンス構成にのみ適用できます。

重要:

- APIデプロイをデプロイ解除する前に、関連付けられているすべてのAPIポリシーがデプロイ解除または削除されていることを確認してください。「APIポリシーのデプロイ解除」を参照してください。
- APIプロキシをデプロイ解除する前に、関連付けられているすべてのAPIデプロイがデプロイ解除または削除されていることを確認してください。「APIデプロイのデプロイ解除」を参照してください。

APIポリシーのデプロイ解除

APIポリシーをデプロイ解除するには、次の手順に従います。

1. **Security > API Security > Policies**で、デプロイ解除するポリシーを選択します。
2. **Undeploy**をクリックします。

このアクションにより、**ポリシーのステータス**が「下書き」に設定されます。

APIデプロイのデプロイ解除

APIデプロイをデプロイ解除するには、次の手順に従います。

1. **Security > API Security > API Deployments**で、デプロイ解除するAPIデプロイを選択します。

   注:

   選択したデプロイに関連付けられているすべてのポリシーがデプロイ解除または削除されていることを確認してください。

2. 「**展開解除**」をクリックします。

この操作により、**展開ステータス**が「下書き」に設定されます。

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

APIプロキシの展開解除

APIプロキシを展開解除するには、次の手順に従います。

1. **Security > API Security > API Proxies**で、展開解除するAPIプロキシを選択します。

   注:

   APIプロキシは複数のAPI展開と共有できます。そのため、選択したプロキシに関連付けられているすべての展開が展開解除または削除されていることを確認してください。

2. 「**展開解除**」をクリックします。

この操作により、**プロキシステータス**が「下書き」に設定されます。

APIを使用してAPIセキュリティを管理する

APIセキュリティを作成、構成、および展開するために、APIにアクセスできます。

注:

この機能を構成するためにAPIセキュリティAPIを使用する方法を理解するには、Nitro APIドキュメントを参照してください。

	手順	リソースURL
1	API定義を作成する	`https://adm.cloud.com/{customerid}/apisec/nitro/v1/config/apidefs`
2	APIプロキシを追加する	`https://adm.cloud.com/apiproxies`
3	APIプロキシを使用してAPIインスタンスを展開する	`https://adm.cloud.com/apiproxies/{customerid}/deployments`
4	APIポリシーを追加する	`https://adm.cloud.com/{customerid}/apisec/nitro/v1/config/policies/{id}`

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

各APIポリシーには異なる`config_spec`オブジェクトがあります。これは、特定の値を持つ`policytype`を構成するためのJSON辞書を含む不透明なオブジェクトです。

このオブジェクトでは、以下のオプションを使用してAPIリソースとそのメソッドを選択できます。

- `api-resource-paths` - API定義で定義されているAPIリソースのパスとメソッドを指定します。

  例：

  ```
  {
  "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
     "get": true,
     "post": false,
     "put": false,
     "delete": false
  }
  ```

- `custom-rules` - API定義に存在しない可能性があるカスタムAPIリソースのパスとメソッドを指定します。

  例：

  ```
  {
  "endpoints": ["/pet/categories", "/pet/findByName"],
     "get": true,
     "post": false,
     "put": false,
     "delete": false
  ```

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

```
}
```

この構成により、ポリシーは指定されたAPIリソースパスに一致する受信トラフィックリクエストをフィルタリングします。

各ポリシータイプの`config_spec`に関する情報については、ポリシータイプのAPI例を参照してください。

ポリシータイプのAPI例

このセクションでは、サポートされているAPIポリシータイプとその構成について説明します。

- レート制限
- オーオース
- 基本認証
- 認証なし
- ボット
- WAF
- ヘッダー書き換え
- URIパス書き換え
- 承認
- 拒否

レート制限

`Ratelimit`ポリシータイプの構成例を次に示します。`config_spec`オブジェクトに次の構成を指定します。

```
{

    "policytype": "Ratelimit",

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
```

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

```
            "get": true,
            "post": false,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "threshold": "10",
        "timeslice": "20000",
        "limittype": "BURSTY",
        "api-respondertype": "DROP",
        "header_name": "x-api-key",
        "per_client_ip": true
    },
    "order_index": 1,
    "policy_name": "ratelimit_policy"
}
```

各属性の詳細については、レート制限ポリシーを参照してください。

オース

`JWT Auth validation`ポリシータイプのAPI構成例を次に示します。`config_spec`オブジェクトに次の構成を指定します。

```
{
    "policytype": "JWT Auth Validation",
```

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

```
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "jwks-uri": "https://uri.petstore.com",
        "issuer": "https://issuer.petstore.com",
        "audience": "petstore",
        "introspect-uri": "https://introspect.uri.com",
        "clientid": "client",
        "clientsecret": "clientsecret",
        "claims-to-save": ["scope", "scope2"],
        "allowed-algorithms": {
            "hs256": true,
            "rs256": true,
            "rs512": true
        }
    },
```

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

```
    "order_index": 2,
    "policy_name": "Jwt_auth_policy"
}
```

各属性の詳細については、OAuthポリシーを参照してください。

基本認証

`BasicAuth`ポリシータイプのAPI設定例を次に示します。

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false
        },
        "custom-rules": {}
    },
    "order_index": 3,
    "policy_name": "Auth_BaSIC",
    "policytype": "BasicAuth"
}
```

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

各属性の詳細については、基本認証ポリシーを参照してください。

認証なし

`NoAuth`ポリシータイプのAPI設定例を次に示します。

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": true,

            "post": false,

            "put": false

        },

        "custom-rules": {}

    },

    "order_index": 4,

    "policy_name": "no_auth_policy",

    "policytype": "NoAuth"

}
```

ボット

`Bot`ポリシータイプのAPI設定例を次に示します。

```
{

    "config_spec": {
```

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

```
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": false,
            "post": false,
            "put": false
        },
        "bot-prof-name": "apisec_test_profile",
        "custom-rules": {}
    },
    "order_index": 5,
    "policy_name": "bot_policy",
    "policytype": "Bot"
}
```

各属性の詳細については、ボットポリシーを参照してください。

WAF

WAFポリシータイプのAPI設定例を次に示します。

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
```

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

```
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": false,
            "post": false,
            "put": false
        },
        "waf-prof-name": "apisec_waf_profile",
        "custom-rules": {}
    },
    "order_index": 6,
    "policy_name": "waf_policy",
    "policytype": "WAF"
}
```

各属性の詳細については、WAFポリシーを参照してください。

ヘッダー書き換え

ヘッダー書き換えポリシータイプのAPI設定例を次に示します。この設定は`config_spec`オブジェクトで指定します。

```
{
    "policytype": "Header Rewrite",
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
```

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

```
            "post": true,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "rewrite-policy-header-field-name": "org",
        "rewrite-policy-header-field-val": "Citrix",
        "rewrite-policy-header-field-new-val": "Citrite"
    },
    "order_index": 7,
    "policy_name": "header_rewrite_pol"
}
```

各属性の詳細については、ヘッダー書き換えポリシーを参照してください。

URIパス書き換え

URIパス書き換えポリシータイプのAPI設定例を次に示します。

```
{
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/store/order", "/store/inventory"],
            "delete": false,
            "get": true,
```

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

```
            "post": true,
            "patch": false,
            "put": false
        },
        "custom-rules": {
            "delete": false,
            "endpoints": [],
            "get": false,
            "post": false,
            "patch": false,
            "put": true
        },
        "path-rewrite-params": [
        {
            "insert-segment-position": "beginning",
            "new-path-value": "v3",
            "old-path-value": "v2",
            "action-type": "replace path segment"
        },
        {
            "insert-segment-position": "beginning",
            "new-path-value": "begin",
```


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

```
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "end",
            "new-path-value": "end",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "before",
            "new-path-value": "before",
            "old-path-value": "store",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "after",
            "new-path-value": "after",
            "old-path-value": "store",
            "action-type": "insert path segment"
        }
        ]
    },
        "order_index": 24,
```

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

```
        "policy_name": "eats_uripathrewrite",

        "policytype": "URI Path Rewrite”

}
```

各属性の詳細については、URI Path Rewrite policyを参照してください。

認証

以下は、`Authorization`ポリシータイプのAPI構成例です。`config_spec`オブジェクトに以下の構成を指定します。

```
{

    "policytype": "Authorization",

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": true,

            "post": true,

            "put": false,

            "delete": false

        },

        "custom-rules": {},

        "claims": [{

            "name": "scope",

            "values": ["value1", "value2"]

        }]
```

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

```
    },
    "order_index": 8,
    "policy_name": "authorization"
}
```

各属性の詳細については、Authorization policyを参照してください。

拒否

以下は、`Deny`ポリシータイプのAPI構成例です。`config_spec`オブジェクトに以下の構成を指定します。

```
{
    "policytype": "Deny",
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "api-denytype": "RESPONDWITH"
    },
    "order_index": 9,
```

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

```
    "policy_name": "deny_policy"

}
```

`api-denytype`では、次のいずれかの値を指定できます。

- RESPONDWITH
- RESET

各属性の詳細については、Deny ruleを参照してください。

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できる場合、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。詳細については、「API セキュリティ」(/ja-jp/netscaler-console-service/api-security.html)を参照してください。

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 Console 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、次の手順を実行します。

1. NetScaler Console で、**Applications** > **Configurations** > **StyleBooks** の順に移動します。`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 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の値を入力できます。

2. 次のパラメータの値を指定します。

   - **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。

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

- **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、HTTP、JSON、または XML 保護チェックを指定するには、**Security Settings** を有効にします。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」(/ja-jp/citrix-adc/13/application-firewall/profiles/creating-profiles.html)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. **Create** 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。

1. NetScaler Console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。
2. **BOT Profile Name** に、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。

   - **IPレピュテーションチェックを有効にする** - このオプションは、不要なリクエストを送信している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からのリクエストを事前に拒否できます。
   - **BOT署名を有効にする** - BOT署名名を指定します。指定された署名からのリクエストをブロックします。
   - **許可リスト** - 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リクエストをバイパスできます。
   - **拒否リスト** - 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リクエストをブロックできます。

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

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。

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

アプリケーション

NetScaler Console のアプリケーション分析および管理機能を使用すると、アプリケーション中心のアプローチでアプリケーションを監視できます。このアプローチは、次のことに役立ちます。

- アプリケーションのスコアを確認し、全体的なパフォーマンスを分析する
- サーバーまたはクライアントで発生している問題をチェックする
- アプリケーションのトラフィックフローの異常を検出し、是正措置を講じる

> **注**
>
> アプリケーションとは、インスタンス (NetScaler) 上に構成されている1つ以上の仮想サーバーを指します。

アプリケーションは、1時間、1日、1週間、1か月などの期間で監視できます。

前提条件

- NetScaler Console に NetScaler インスタンスを追加していることを確認します。
- NetScaler インスタンスの有効なライセンスがあることを確認します。詳細については、「ライセンス」を参照してください。

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)

ディスクリートアプリケーション

NetScaler® Console で検出されたすべての仮想サーバーは、ディスクリートアプリケーションと呼ばれます。

© 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。

例えば、データセンター1のカテゴリを作成し、そのNetScalerインスタンスを追加できます。カテゴリを定義し、データセンター1のインスタンスを追加すると、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アプリケーションダッシュボードに表示されます。

注意事項

- カスタムアプリケーションに追加されたディスクリートアプリケーションは、ディスクリートアプリケーションから削除されます。
- いずれのカテゴリにも追加されていないすべてのアプリケーションは、**「その他」**として利用できます。

マイクロサービスアプリケーション

Kubernetesクラスターでは、NetScalerはNetScaler MPX (ハードウェア)、NetScaler VPX (仮想化)、およびNetScaler CPX (コンテナ化) 用のIngress Controllerを提供します。詳細については、NetScaler Ingress Controllerを参照してください。

NetScaler CPXインスタンスを使用して構成されたディスクリートアプリケーションは、マイクロサービスアプリケーションと呼ばれます。

アプリケーション管理とアプリケーションダッシュボード

NetScaler Consoleでは、**ダッシュボード**ページからアプリケーションを管理し、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。

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

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

- アプリ名、アプリの種類、アプリのカテゴリ、関連付けられた仮想サーバー、関連付けられたサービスなどのアプリケーションの詳細を表示します。
- カスタムアプリケーションの編集または削除

アプリケーションを追加、編集、または削除すると、その詳細はアプリケーションページにすぐに反映されます。

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。

約10〜15分経過してもアプリケーション分析が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」の手順を実行してください。

ダッシュボードの列でデータを並べ替える

アプリケーションダッシュボードの表形式ビューでは、次の列でデータを並べ替えることができます。

- **アプリスコア**
- **アプリ名**
- **応答時間**
- **合計リクエスト数**
- **スループット**
- **データ量**
- **クライアント接続**
- **サーバー接続**

並べ替えを適用すると、ダッシュボードはすべてのページで利用可能なアプリケーションで整理されます。たとえば、ダッシュボードが5ページで構成されている場合、それらすべての5ページで並べ替えが行われ、結果がそれに応じて表示されます。

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

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、NetScaler Consoleに分析データがある間（最大1か月間）、ダッシュボードには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にアプリケーションを削除したシナリオを考えてみましょう。このシナリオでは、次のようになります。

  - 過去1日、1週間、1か月の期間を選択した場合、ダッシュボードはJan 4, 2020に削除されたアプリケーションをまだ表示できます。
  - 過去1週間と1か月の期間を選択した場合、ダッシュボードはJan 5, 2020に削除されたアプリケーションをまだ表示できます。
  - 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日間）、Jan 12, 2020（過去1週間）、およびFebruary 5, 2020以降（過去1か月間）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。
  - ダッシュボードから削除されたアプリケーションをクリックすると、次のメッセージが表示されます。

    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により到達できない場合：

    -NetScalerインスタンスに関連付けられたアプリケーションは、**アプリケーション**ページでのみ表示され、ダッシュボードには表示されません。
    -NetScalerインスタンスが稼働状態になると、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。

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

アプリケーションの詳細を表示

アプリの詳細(/en-us/netscaler-console-service/media/manage-applications.png)

- **アプリケーション名** – アプリケーション名を示します
- **状態** – **Up**、**Down**、**Partially Up**、**Out of Service**、**NA** などの現在のアプリケーションステータスを示します
  - **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稼働中です。
  - **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停止しています
  - **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停止しているか、サービス停止中です
  - **Out of Service** – アプリケーションに関連付けられているすべての仮想サーバーがサービス停止中です
  - **NA** – アプリケーション用に仮想サーバーが構成されていません
- **タイプ** – アプリケーションがカスタムまたはディスクリートのどちらに属するかを示します
- **カテゴリ** – グループ化されたアプリケーションカテゴリを示します
- **仮想サーバー/状態** – 構成されている仮想サーバーの合計数とすべての仮想サーバーのステータスを示します。マウス ポインターを合わせると、仮想サーバーの合計数、仮想サーバーの種類、仮想サーバーのステータスなどの詳細が表示されます

  仮想サーバーのステータス(/en-us/netscaler-console-service/media/virtual-server-status.png)
- **サービス/状態** – 設定されているサービス総数とすべてのサービスのステータスを示します
- **サービスグループ/状態** – 設定されているサービスグループ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
- **サーバー/状態** – アプリケーション用に設定されているサーバー総数とすべてのサーバーのステータスを示します
- **アクション** – カスタムアプリケーションを編集または削除できます

アプリケーションの追加

1. **新しいアプリケーション**をクリックして、アプリケーションを作成します

   アプリケーションの定義ページが表示されます

2. 次のパラメータを設定します。

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

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。クリックすると、 ページが表示されます。カテゴリを選択し、**選択**をクリックします。カテゴリを追加するには:
	1. **追加**をクリックします
	2. 任意の名前を入力します。
	3. **作成**をクリックします
既存のアプリケーションを選択	NetScalerインスタンスに追加された既存のアプリケーションを選択できます。
アプリケーションの追加	インスタンスで構成されているすべての仮想サーバーが表示されます。リストからアプリケーションを選択し、**OK**をクリックします。
選択基準の定義	仮想サーバー範囲、またはオリジンサーバー/サービスIPアドレス範囲でアプリケーションを定義するオプション。
	- **サーバー。** アプリケーションが実行されているバックエンドサーバーのサーバーまたはサービスIPアドレス、サーバー名、またはポートを指定します。1つのIPアドレス、IPアドレスの範囲、またはコンマで区切られた両方の組み合わせを入力できます。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、またはコンマで区切られた両方の組み合わせを入力できます。たとえば、10.102.29.20、

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

フィールド	説明
	10.102.43.10-60、10.216.43.45と入力できます。
StyleBookからアプリケーションを作成	StyleBookを使用してアプリケーションを作成できます。詳細については、「StyleBookを使用してアプリケーションを作成する」を参照してください。

3. **OK**をクリックします。

> **注:**
>
> 現在、アプリケーションダッシュボードは、ロードバランシングとコンテンツスイッチングの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。

StyleBookを使用してアプリケーションを作成する際は、アプリケーションの展開中に必要なライセンスの消費を確認してください。

確認メッセージで**はい**をクリックします。NetScaler Consoleは、必要なライセンスをアプリケーションに割り当てます。

StyleBookを使用してアプリケーションを作成する

StyleBookを使用してアプリケーションを作成するには：

1. NetScaler Consoleで、**Applications** > **Dashboard** に移動し、**Manage Apps** をクリックします。
2. **Category** セクションからアプリケーションカテゴリを選択します。NetScaler Consoleでは、ユーザー定義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。
3. **Create a new application from a StyleBook** をクリックして選択し、**OK** をクリックします。

   「Choose StyleBook」ページが表示されます。このページには、NetScaler Consoleで利用可能なすべてのデフォルトStyleBookが含まれています。
4. StyleBookを選択します。 **Configuration Details** ページが表示されます。

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

5. StyleBookのすべてのパラメータに値を入力します。また、使用する前にView Definition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、「Use Default StyleBooks」を参照してください。

6. **Create** をクリックします。

   必要なライセンスを消費し、アプリケーションを展開するための確認メッセージが表示されます。

7. 「**はい**」をクリックします。

選択したNetScalerインスタンスでNetScaler Consoleが作成しようとする構成を確認するために、「**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、選択したNetScalerでの実際の構成は、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

「**アプリケーションの管理**」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。アプリケーションを編集するには編集ボタンを、アプリケーションを削除するには削除ボタンをクリックします。

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 Console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。アプリケーション管理者は、頻繁に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 Consoleの他のレポートエクスポートオプションとは異なり、アプリ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。

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

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のページから、セカンドレベルのページに移動してレポートとしてエクスポートすることもできます。現在、一度に1つのアプリケーションのレポートのみをダウンロードできます。

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。

注:

14.1 20.x ビルド以降、NetScaler管理パーティションから作成されたアプリケーションのメトリック詳細を表示できます。

ダッシュボードには、次のアプリケーションの詳細が表示されます。

- **アプリ名** – アプリケーション名を示します。
- **インスタンス** – NetScalerインスタンスを示します。
- **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。
- **状態** – アプリケーションの現在の可用性（**稼働中**、**停止中**、**部分稼働中**、**サービス停止中**、**NA**など）を示します。
  - **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または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。
- **アプリケーションタイプ** – **カスタム**、**ディスクリート**、または**Kubernetesサービス**などのアプリケーションタイプを示します。
- **アプリケーションカテゴリ** – アプリケーションに割り当てられているカテゴリを示します。

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

- **最も多い問題** – アプリケーションで最大のエラー数を記録している問題を示します。
- **最も多い問題のカテゴリ** – 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。
- **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で計算されます。
- **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。

マイクロサービスアプリケーションの表示

マイクロサービスアプリケーションを表示するには、**アプリケーションタイプ**フィルターで**K8s_Discrete**オプションを選択します。

マイクロサービスアプリケーションは、**App Dashboard**で次の名前形式で表示できます。

```
<k8s service>_<k8s namespace>_<k8s cluster_name>
```

例えば、`tea-beverage_sg-demo_adm-cluster`は、クラスター`adm-cluster`内の`sg-demo`という名前空間を持つ「tea-beverage」というサービスを指します。

選択した期間のダッシュボードには、以下のメトリックが表示されます。

- **App Name** – アプリケーション名を示します。
- **Instance** – NetScaler CPXインスタンスのIPアドレスを示します。
- **App Score** – アプリケーションスコアを示します。
  - **Critical** – アプリケーションスコアが0から40未満の場合
  - **Review** – アプリケーションスコアが40から75未満の場合
  - **Good** – アプリケーションスコアが75より大きい場合
- **State** – 現在のアプリケーションステータスを示します。
- **App Category** – アプリケーションがホストされているクラスター名を示します。
- **Top Issue** – 現在の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。

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

- **Top Issue Category** – アプリケーションに影響を与える問題のカテゴリを示します。
- **Issue Count** – アプリケーションに影響を与える問題の総数を示します。問題の概要を表示するには、問題の数にマウスポインターを合わせます。

- **レスポンス時間** – アプリケーションが受信した平均レスポンス時間を示します。
- **エラー率** – アプリケーションの5xxエラーの平均エラー率を示します。
- **総リクエスト数** – アプリケーションが受信したリクエストの総数を示します。
- **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示します。
- **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。データ量は、アプリケーションの総リクエストバイトとレスポンスバイトとして計算されます。
- **クライアント接続** – アプリケーションによって確立された平均クライアント接続を示します。これは、選択したサービスに接続されている関連する送信サービスを指すこともあります。
- **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を示します。これは、選択したサービスに接続されている関連する受信サービスを指すこともあります。

ダッシュボードに表示するオプションを追加または削除するには、**+** オプションをクリックします。

アプリケーションをクリックして、アプリケーションの詳細を表示します。詳細については、マイクロサービス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、カスタムアプリケーションごとに個別のアプリケーションを作成するのではなく、同じアプリケーションを複数のカスタムアプリケーションで再利用できます。

それぞれ**ComABC**と**ComCDE**という名前の2つのeコマースポータルを管理しており、両方のポータルで**PaymentApp**という名前の決済ゲートウェイサーバーを使用したいとします。このシナリオでは、次のことを行う必要があります。

- **ComABC**と**ComCDE**という名前の2つのカスタムアプリを作成します。
- **PaymentApp**という名前のアプリケーションを作成し、**ComABC**と**ComCDE**に関連付けます。

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

このシナリオを実装するには、次のことを行う必要があります。

- **カスタムアプリ (ComABC および ComCDE)** を作成します。
  a. **アプリケーション > ダッシュボード**に移動し、**アプリの管理**をクリックします。
  b. **新しいアプリケーション**をクリックします。
  c. 名前とカテゴリを指定します。
  d. アプリケーションを選択するタイプを選択します。この例では、**既存のアプリケーションを選択**オプションが選択されています。詳細については、「アプリケーションの追加」を参照してください。
  e. **アプリケーション**の下で、**アプリケーションの追加**をクリックします。
  f. リストからアプリケーションを選択し、**OK**をクリックしてカスタムアプリを作成します。
- **PaymentApp**を作成します。これには、個別のアプリをカスタムアプリに変換する必要があります。
  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。
- 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**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**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。

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

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か月など、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

5 – フィルターを適用してアプリケーションを表示できます。クリックして詳細を表示します。

カルーセルスライダーを使用すると、すべてのオプションに簡単にアクセスできます。

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
    - **良好** – アプリケーションスコアが40から75未満
    - **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構成された仮想サーバーがないか、仮想サーバーのタイプが負荷分散またはコンテンツスイッチングではない場合。

      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。

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

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)**、**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。

  例えば、仮想サーバーの健全性が0から20の間のアプリケーションを表示したい場合は、仮想サーバーの健全性ヒストグラムをドラッグして結果をフィルターします。

  注記:

  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。

  適用されたフィルターをクリアするには、**すべてクリア**をクリックします。

  以下は、フィルターを適用できるアプリケーションの概要です。

  - **アプリケーションスコア – 重大、レビュー、良好、該当なし**に基づいてアプリケーションを表示できます。

    注記:

    デフォルトでは、重大、レビュー、良好のステータスにあるアプリケーションを表示できます。N/Aステータスのアプリケーションを表示するには、**該当なし**オプションを選択する必要があります。

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

- **状態** – アプリケーションの状態（アップ、**ダウン**、**サービス停止中**など）に基づいてアプリケーションを表示できます。
- **現在の問題** – **パフォーマンス**、**インスタンスの健全性**、**構成**、**システムリソース**などの問題の種類を選択することで、特定の問題の影響を受けるアプリケーションのリストを取得できます。
- **アプリの種類** – **カスタム**、**ディスクリート**、**Kubernetesサービス**などのアプリケーションの種類に基づいてアプリケーションを表示できます。
- **アプリのカテゴリ** – 割り当てられたカテゴリに基づいてアプリケーションを表示できます。
- **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。
- **合計リクエスト数** – アプリケーションが受信したリクエストの合計数を表示するヒストグラム。
- **スループット** – アプリケーションによって処理されたネットワークスループットの合計を表示するヒストグラム。
- **データ量** – アプリケーションによって処理された合計データを表示するヒストグラムです。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を表示するヒストグラムです。
- **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を表示するヒストグラムです。
- **送信パケット** – アプリケーションによって送信された合計パケットを表示するヒストグラムです。
- **受信パケット** – アプリケーションによって受信された合計パケットを表示するヒストグラムです。
- **仮想サーバーの健全性** – スコア範囲0%から100%の間の合計アプリケーションを表示するヒストグラムです。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%になります。

検索バーを使用して結果を検索およびフィルターする

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.

フィルターを保存

アプリダッシュボードでフィルターを適用し、フィルターを保存できます。その後、リストからフィルター名を選択し、必要に応じてカスタマイズされたダッシュボードを表示できます。

Upステータスのアプリケーションのフィルターを作成したいとします。**App Dashboard**でフィルターを適用した後、**Save Filter**をクリックします。

任意の名前を指定し、**Save**をクリックします。

「**デフォルトフィルターとして設定**」を選択して、このフィルターをアプリダッシュボードのデフォルトビューにすることもできます。

複数のフィルターを保存し、必要に応じてリストからフィルター名を選択して、カスタマイズされたダッシュボードを表示できます。

フィルターの選択(/en-us/netscaler-console-service/media/app-filter-list.png)

デフォルトフィルターを削除するか、フィルターを削除するには、フィルターリストの横にあるフィルターアイコンをクリックします。

フィルターの編集(/en-us/netscaler-console-service/media/app-edit-filter.png)

アプリケーションにタグを作成して適用する

多数のアプリケーションがある場合は、アプリケーションにタグを作成して適用できます。これらのタグは検索機能を向上させます。

例:

次の手順では、負荷分散アプリケーションのタグを作成する手順を説明します。

1. **App Dashboard**で、タグを作成する負荷分散アプリケーションを選択し、**Tags**をクリックします。

   タグ(/en-us/netscaler-console-service/media/app-tags.png)
2. **タグの更新**で:
   - 任意の名前を指定します。例: **Type**。
   - タグを割り当てることができる値を指定します。複数の値を入力することもできます。例: **Loadbalance**。
   - **適用**をクリックします。

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

タグを作成(/en-us/netscaler-console-service/media/app-tags1.png)

タグが作成されました。

タグを適用してロードバランシングアプリケーションを取得するには、次のようにします。

1. アプリダッシュボードの検索バーで、テキストボックス内をクリックして作成されたタグを表示し、タグ名を選択します。

   検索バー(/en-us/netscaler-console-service/media/app-tags2.png)

2. 演算子 (**IN**) と作成された値を選択し、**検索**をクリックします。

   タグ(/en-us/netscaler-console-service/media/app-tags3.png)

   Loadbalanceの下にタグ付けされたすべてのロードバランシングアプリケーションが一覧表示されます。同様に、他のアプリケーションのタグを作成することもできます。

アプリケーションの詳細

注:

14.1 20.x ビルド以降、NetScaler 管理パーティションから作成されたアプリケーションのメトリック詳細を表示できます。

ダッシュボードからアプリケーションをクリックすると、さらに詳細な情報をドリルダウンして表示できます。

選択したアプリケーションページが表示されます。

アプリケーションの詳細ページから:

- リストから期間を選択して、特定の期間の詳細を表示します
- 選択したアプリケーションのサービスグラフを表示するには、**サービスグラフ**をクリックします。詳細については、「Service Graph for Applications」を参照してください。
- 選択したアプリケーションの詳細なトランザクションを表示するには、**トランザクションログ**をクリックします
- 詳細な監査ログ情報を表示するには、**監査ログ**をクリックします

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

- 選択したアプリケーションのサービスおよびサービスグループ構成を表示または編集するには、**構成**をクリックします
- アプリケーションにバインドされているサービスを表示するには、**サービス**をクリックします

期間を選択すると、次のアプリケーションの詳細が表示されます。

- **アプリケーションスコア** – 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から合計ペナルティを引いた値**として計算されます。

  アプリケーションスコア(/en-us/netscaler-console-service/media/app-score.png)

  このダッシュボードでは、アプリケーション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。

  IPアドレス(/en-us/netscaler-console-service/media/app-ip-address.png)

  カスタムアプリケーションに関連付けられているすべての仮想サーバーを表示します

  仮想サーバー(/en-us/netscaler-console-service/media/app-detail-vir-ser.png)

  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。

  仮想サーバーの詳細(/en-us/netscaler-console-service/media/app-detail-vir-ser-details.png)

- **すべてのサービス** – アプリケーションにバインドされているサービス

  すべてのサービス(/en-us/netscaler-console-service/media/app-detail-all-serv.png)

  クリックしてサービスの詳細を表示し、サービス設定を管理します

  すべてのサービスの詳細(/en-us/netscaler-console-service/media/app-detail-all-serv-details.png)

- **問題** – 選択したアプリケーションに適用される問題。そのカテゴリとともに、以下の問題を表示できます。

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

パフォーマンス	インスタンスの健全性	構成	システムリソース
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再構成キューの制限ヒット	
アプリCPU使用率			
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			
サーバー応答時間			
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、問題が発生した日時、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** ページの以前のビューです。

現在、**Issues** セクションですべての問題を、**App Activity Investigator** ページで表示できたカテゴリとともに表示できます。

- **Current** タブに表示される問題は、選択した期間のアプリケーションの問題を指します。
- **All** タブに表示される問題は、すべてのアプリケーションの問題を指します。

次の例は、1日間のアプリケーションの問題です。**Current** タブは、アプリのスコアに影響を与える現在の問題がないことを示しています。

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

「**すべて**」タブには、1日間の期間で検出された合計問題が表示されます。

アプリケーションのモニターの状態を確認する

NetScaler Console GUIの「**Applications > Dashboard**」にあるアプリケーションダッシュボードを使用して、アプリケーションのヘルスモニターの状態と、もしあれば障害メッセージを表示できます。ヘルスモニターは、アプリケーションのサービスまたはサービスグループにバインドでき、1つのサービスまたはサービスグループには複数のモニターをバインドできます。モニターはサービスの監視に役立ちます。

モニターの状態を表示するには、次の手順に従います。

1. NetScaler Console GUIから「**Applications > Dashboard**」に移動します。「**Applications**」の下で、健全性を確認したいアプリケーションを選択します。

2. アプリケーションをクリックします。アプリスコアダッシュボードが表示されます。

3. 右上隅にある「**Services**」タブ、または「**Group Name**」の下にあるサービスグループをクリックします。
4. 「**Services**」タブをクリックした場合は、次の画面でサービスグループを選択します。
5. サービスグループをクリックすると、「**Service Group**」ウィンドウが表示されます。インスタンスを選択し、「**Bound Monitors**」をクリックします。

   バインドされたモニター画面が表示され、アプリケーションのヘルスモニターの状態が示されます。

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計算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観点から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。

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

App Score設定(/en-us/netscaler-console-service/media/app-score-setting.png)

App Scoreの構成ページで、コンポーネントを選択し、最終的なApp Scoreを決定するためのしきい値を設定できます。

App Scoreコンポーネント(/en-us/netscaler-console-service/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
NetScaler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しきい値と高しきい値。
NetScaler CPU使用率	はい	NetScalerインスタンスにおける合計CPU使用率に対する低しきい値と高しきい値。
応答時間	はい	リクエストパケットの送信から、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。
アプリケーションCPU使用率	はい	アプリケーションによる合計CPU使用率に対する低しきい値と高しきい値。
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	いいえ	仮想サーバーでの永続性の使用率が低いかどうかを示します。

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

APP SCOREコンポーネント	ユーザーが設定したしきい値	説明
サーバーエラー (5xx)	いいえ	Webサーバーが5xxエラーで応答するかどうかを示します。
異常に大きいHTTPパケット	いいえ	HTTPヘッダーサイズを持つHTTPメッセージがNetScalerインスタンスで設定された値を超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	いいえ	SSLトラフィックを分析してリアルタイムトラフィックを特定し、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	いいえ	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る、一定期間にわたるセッションの蓄積を示します。
セッション再利用率の低下	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接続上の順序が異なるパケットが、設定された順序が異なるパケットキューサイズを超えているかどうかを示します。

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

デフォルトでは、すべてのコンポーネントが有効になっています。いずれかのコンポーネントを無効にすると、NetScaler Consoleは選択されたコンポーネントに基づいてのみ最終的なアプリスコア計算を実行します。

マイクロサービスアプリケーションのアプリケーション詳細

ダッシュボードからマイクロサービスアプリケーションをクリックすると、さらに詳細な情報が表示されます。

選択したアプリケーションページが表示されます。

アプリケーション詳細ページから:

- リストから期間を選択して、特定の期間の詳細を表示します
- 選択したアプリケーションのサービスグラフを表示するには、**サービスグラフ**をクリックします。詳細については、「アプリケーションのサービスグラフ」を参照してください。
- 選択したアプリケーションの詳細なトランザクションを表示するには、**トランザクションログ**をクリックします
- 詳細な監査ログ情報を表示するには、**監査ログ**をクリックします

期間を選択すると、次のアプリケーション詳細が表示されます。

- **アプリスコア** – 選択した期間のアプリケーションスコア。現在のアプリケーションの問題 (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) も表示できます。最終スコアは、**100 - 合計ペナルティ**として計算されます。

  1 – 現在のアプリスコアを示します

  2 – CPX IPアドレス、ロードバランシングやコンテンツスイッチングなどのアプリケーションタイプ、およびサービスがホストされているサービス名前空間とクラスター名を示します

  3 – 現在のアプリケーションスコアに影響を与える問題を示します

  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「Issues」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。

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

- **サービス名** – サービスの名前
- **クラスター名** – サービスがホストされているクラスターの名前
- **名前空間** – サービスに割り当てられている名前空間
- **サービスラベル** – サービスに割り当てられているサービスラベル

- **Podの詳細**

  Podは、Kubernetesクラスターでホストされているコンテナのグループです。Pod内には、複数のコンテナ化されたアプリケーションをデプロイできます。各PodにはIPアドレスが関連付けられています。

  Podの状態をクリックして詳細を表示します。

  - **Pod IPアドレス** – PodのIPアドレスを示します
  - **ホスト名** – Podに割り当てられているホスト名を示します
  - **インスタンス** – NetScaler CPXのIPアドレスを示します
  - **PODの状態** – ポッドの現在のステータスを示します

- **主要メトリック** – **応答時間、5xxエラー、1秒あたりのリクエスト数、スループット、クライアント接続、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、選択した期間の平均値と差分値を表示できます。差分値は、選択した期間の**最初の値から最後の値を引いたもの**として計算されます。

  選択した期間の以下のインスタンスメトリックをグラフ形式で表示できます。

  次の画像は**データ量**の例で、選択された期間は1か月です。202.66 MBという値は1か月間の合計データ量であり、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、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。カテゴリとともに以下の問題を表示できます。

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

パフォーマンス	インスタンスの健全性	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	不適切な永続性タイプ
低いセッション再利用	メモリ使用量	異常に大きなHTTPパケット	NICカードの飽和
SurgeQueueの蓄積		TCP再構築キュー制限ヒット	
SSLリアルタイムトラフィック			

各問題をクリックして、以下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-console-service/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**」タブに表示される問題は、アプリケーションの総問題数を指します。

以下は、1日間のアプリケーションの問題の例です。「**現在**」タブは、アプリスコアに影響を与える現在の問題がないことを示しています。

- [ ] 「**すべて**」タブには、1日間の期間で検出された総問題数が表示されます。

- [ ]

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、機械学習とルールアルゴリズムを使用してアプリケーションのパフォーマンスの問題を特定できます。NetScaler Consoleのインテリジェントアプリ分析機能は次のとおりです。

- NetScalerインスタンスを介して提供されるアプリケーションの監視とトラブルシューティングのための、簡単でスケーラブルなソリューションを提供します。

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

- アプリケーションのすべてのレベルを監視して、問題のトラブルシューティングにかかる時間を短縮し、アプリケーション全体の稼働時間を向上させます。

一般的な展開では、何千ものサーバーがユーザーのデータニーズに対応します。これらのサーバーに送信されるトラフィックは、NetScalerアプライアンスで構成された仮想サーバーによって負荷分散され、監視されます。各仮想サーバーは、バックエンドサーバーを表す複数のサービスにバインドされています。このような展開では、インテリジェントアプリ分析機能は次のことに役立ちます。

- 停止やその他のイベント中に監視、管理、意思決定を行う
- アプリケーション用に構成された仮想サーバーとサービスを監視する
- 仮想サーバーとサービスに関する重要な情報を表示し、アプリケーションによる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。

Application > **Dashboard** に移動し、アプリケーションを選択して、**Issues** セクションでパフォーマンスインジケーター を表示します。

インテリジェントアプリ分析を構成する

注:

14.1-21.x以降のビルドから、NetScaler Consoleに追加された新しいNetScalerインスタンスでは、Metrics Collectorはデフォルトで無効になっています。既存の管理対象インスタンスのメトリックコレクター構成は変更されません。

インテリジェントアプリ分析機能は、**NetScaler 12.1 Build 50.28以降**でのみサポートされています。Metrics CollectorはNetScalerのカウンターデータをNetScaler Consoleにプッシュし、これはアプリケーションの問題を検出するために使用されます。インテリジェントアプリ分析機能を使用するには、各NetScalerインスタンスで**Metrics Collector**を構成する必要があります。

14.1-28.xビルド以降、Metrics Collectorとリーン使用状況分析は、インスタンスレベルではなく仮想サーバーレベルで有効になります。この機能強化により、Metrics Collectorとリーン使用状況分析は、トラフィックの多いアクティブな仮想サーバーでのみ有効になります。詳細については、「ピークおよびリーン使用状況分析」を参照してください。

仮想サーバーを確認し、他の仮想サーバーでMetrics Collectorとリーン使用状況を有効にできます。

Metrics Collectorを確認して有効にするには:

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

1. **Settings > Analytics Configuration**に移動します。
2. **Virtual Server Metrics Summary**の下にある**Configure Metrics**をクリックします。

3. **All Virtual Servers**ページで、各仮想サーバーのメトリックコレクターのステータスを表示できます。有効にする仮想サーバーを選択し、**Enable Metrics**をクリックします。

4. Metrics Collectorを有効にするには、**Enable Metrics**を選択します。リーン期間の使用状況分析を有効にして表示したい場合は、**Lean Data**も選択できます。選択後、**Save Configuration**をクリックします。詳細については、「ピークおよびリーン使用状況分析」を参照してください。

または、NetScaler®インスタンスページから仮想サーバーのメトリックコレクターとリーン使用状況を有効にすることもできます。

1. **Infrastructure > Instances**に移動し、インスタンスタイプを選択して、**Select Action**リストから**Metrics Collector**を選択します。
2. メトリクスコレクターを有効にする仮想サーバーを選択し、**Enable Metrics**をクリックします。
3. メトリクスコレクターを有効にするには、**Enable Metrics**を選択します。リーン期間の使用状況分析を有効にして表示したい場合は、**Lean Data**も選択できます。選択後、**Save Configuration**をクリックします。

仮想サーバーで**Metrics Collector**オプションが有効になったら、**Applications** > **Dashboard**に移動します。**Issues**セクションで異常を表示するには、インスタンスを選択します。

サーバーエラー (5xx) の詳細なWebトランザクションなどの問題を視覚化するために、分析も有効にすることをお勧めします。詳細については、Enable Analyticsを参照してください。

アプリケーション分析のパフォーマンス指標

NetScaler Webアプリケーションで発生するパフォーマンス指標とそのカテゴリを表示できます。これらの指標を表示するには、NetScalerインスタンスで分析とメトリクスコレクターを有効にする必要があります。

分析とメトリクスコレクターを有効にすると、**Applications** > **Dashboard** に移動し、アプリケーションを選択して **Issues** セクションまでスクロールすることで、以下の指標を表示できます。

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

応答時間

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。**Response Time** タブをクリックして、問題の詳細を表示します。

Recommended Actions で、> 500 ms の応答時間を持つアプリケーションを表示する **Transaction Logs** をクリックします。

Details では、以下を表示できます。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルターを適用し、詳細を表示します。
- 問題が発生した日時
- 選択した期間の合計発生回数
- 低、中、高などの問題の重大度
- 設定されたしきい値を超過した合計トランザクション応答時間を示す検出メッセージ。

アクティブなサービス

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なサービスの割合が、設定されたしきい値よりも少ない場合に検出されます。**Active Services** タブをクリックして、問題の詳細を表示します。

アクティブサービス(/en-us/netscaler-console-service/media/pi-active-services.png)

推奨されるアクションで、クリックして仮想サーバーにバインドされているサービスの詳細を表示します。

詳細で、以下を表示できます。

- 選択した期間の総イベント数を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生した日時
- 選択した期間の総発生回数
- 低、中、高などの問題の重大度
- アクティブなサービスセッションの割合と設定されたしきい値を示す検出メッセージ。

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

平均CPU使用率

この問題は、このアプリケーションのNetScaler CPU使用率が設定されたしきい値を超えた場合に検出されます。**平均CPU使用率**タブをクリックして、問題の詳細を表示します。

平均CPU(/en-us/netscaler-console-service/media/pi-average-cpu.png)

詳細で、以下を表示できます。

- 選択した期間の総イベント数を示すグラフ。クリックしてフィルターを適用し、詳細を表示します
- 問題が発生した日時
- 選択した期間の総発生回数
- 低、中、高などの問題の重大度
- NetScalerの平均CPU使用率%と設定されたしきい値を示す検出メッセージ。

平均アプリケーションCPU使用率

この問題は、アプリケーションのCPU使用率が設定されたしきい値を超えた場合に検出されます。**App CPU Usage**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
- アプリケーションの平均CPU使用率%と設定されたしきい値を示す検出メッセージ

メモリ使用率

この問題は、このアプリケーションのNetScalerメモリ使用率が設定されたしきい値を超えた場合に検出されます。**Memory Usage**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。

- 選択した期間の合計イベントを示すグラフ。クリックしてフィルターを適用し、詳細を表示します。

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

- 問題が発生した日時
- 選択した期間の合計発生回数
- 低、中、高などの問題の重大度
- NetScalerの平均メモリ使用率（%）と設定されたしきい値を示す検出メッセージ。

NIC破棄

パケット破棄は次の場合に発生する可能性があります。

- 受信したパケットにフォーマットエラーがある場合
- 受信デバイスにパケットを格納する十分なストレージがない場合

NIC破棄インジケーターを使用して、NICから破棄された合計パケットを表示できます。**NIC破棄**タブをクリックして詳細を表示します。

詳細では、以下を表示できます。

- 異常が発生した時刻
- NICから破棄された合計パケットを示すメッセージ

サービスフラップ

ネットワーク管理者として、アプリケーションの最適な可用性を確保する必要があります。ネットワークの問題や構成の問題が発生すると、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。

- 特定の期間にどのサービスがDOWNステータスであるかを理解する
- 特定の期間にいくつのサービスがUPまたはDOWN状態であるかを理解する

サービスフラップの詳細を表示するには、**Service Flaps**タブをクリックします。

サービスフラップ(/en-us/netscaler-console-service/media/service-flaps.png)

Recommended Actionsで、仮想サーバーにバインドされているサービスの詳細を表示するにはクリックします。

発生回数や最終発生時刻などの詳細を表示できます。

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

Detailsの下で、以下を表示できます。

- サービスフラップ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

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。サーバーからの応答を受信すると、NetScalerインスタンスはクライアントとのセキュアなトランザクションを完了します。キャッシュされたセッションパラメータを使用して、NetScalerインスタンスは連続するリクエストのSSLハンドシェイクプロセスを完了します。

これらのセッションが再利用されない場合、NetScalerインスタンスにとってオーバーヘッドとなります。**低セッション再利用**インジケーターを使用すると、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。

低セッション再利用タブをクリックして、問題の詳細を表示します。

低セッション再利用(/en-us/netscaler-console-service/media/iaa-low-session.png)

問題のトラブルシューティングのための**推奨されるアクション**は、セッションの再利用を無効にするか、セッションタイムアウトを短縮することです。詳細については、セッション再利用を参照してください。

詳細の下で、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
- 低セッション再利用の異常が発生した時刻
- 総発生回数
- 高、低、中などの異常の重大度
- 設定されたセッションの%のみが再利用されていることを示す検出メッセージ

不適切なパーシステンスタイプ

仮想サーバーによって表されるサーバー上の接続の状態を維持したい場合（たとえば、eコマースで使用される接続など）、仮想サーバーにパーシステンスを設定する必要があります。アプライ

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

アンスは、サーバーの初期選択に設定された負荷分散方法を使用しますが、同じクライアントからの後続のすべてのリクエストを同じサーバーに転送します。

パーシステンスは、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。パーシステンスセッションの再利用率が低い場合、NetScalerで作成されたセッションは単なるオーバーヘッドになります。

不適切なパーシステンスタイプインジケーターを使用すると、仮想サーバーでのパーシステンスの使用率が低いかどうかを判断できます。**不適切なパーシステンスタイプ**タブをクリックして、問題の詳細を表示します。

不適切なパーシステンスタイプ(/en-us/netscaler-console-service/media/iaa-improper-persistence.png)

問題のトラブルシューティングを行うための**推奨されるアクション**は、永続化タイプを確認するか、永続化を無効にすることです。詳細については、「永続化設定」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
- 異常の重大度（高、低、中など）
- 未使用のセッションの割合を示す検出メッセージ

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、ステータスコードで応答します。これらのエラーは、エラーのさまざまなシナリオを定義するエラーコードで表示されます。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信しました。
- **503 Service Unavailable** サーバーは利用できません。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信しませんでした。

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実装す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、クライアントの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。

不安定なサーバータブを選択して、問題の詳細を表示します。

推奨されるアクションで、クリックして、応答コード5xxエラーのアプリケーションを示す**トランザクションログ**を表示します。

次のトラブルシューティング方法も試すことができます。

- 5xxエラーで応答するサーバーに対して、適切なパラメータでL7モニターを設定します。モニターは、サービスの健全性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、定期的にサーバーをプローブします。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。モニターの設定の詳細については、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、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間
- サービス/サービスグループ名
- 合計発生回数
- 高、低、中などの異常の重大度
- このサービスからの応答の%が5xxエラーを報告していることを示す検出メッセージ

サーバーエラーのWebトランザクションの詳細については、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。

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、遅延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.

問題のトラブルシューティングに対する**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遅延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。

詳細では、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

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。

異常に大きいHTTPパケットタブをクリックして、問題の詳細を表示します。

問題のトラブルシューティングに対する**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て、ヘッダーサイズが正規のものであるか判断します。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、ソースをブロックリストに追加して攻撃を回避します。

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に設定されている現在のHTTPヘッダー長を示す検出メッセージ

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

TCP再アセンブルキュー制限ヒット

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、パケットをランタイムメモリに保持する必要があるため、この設定はNetScalerのメモリに影響を与えます。

これは、ネットワークの種類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に維持する必要があります。

TCP再アセンブル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えているかどうかを確認できます。

問題の詳細を表示するには、**TCP再アセンブルキュー制限ヒット**タブをクリックします。

TCP再アセンブルキュー制限ヒット(/en-us/netscaler-console-service/media/iaa-tcp-limit.png)

問題のトラブルシューティングのための**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、攻撃である場合は送信元をブロックリストに追加します。
- これ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、それ以上の操作は不要です。

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

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ある仮想サーバーを表示できます。**サージキューの蓄積**タブをクリックして、問題の詳細を表示します。

サージキュー(/en-us/netscaler-console-service/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。

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

- 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
- 仮想サーバー上のサージキューの蓄積を示す検出メッセージ

SSL評価

アプリケーションがA+ SSL評価ではない場合、アプリスコアに影響が出ます。**A+ SSL評価以外**インジケーターを使用して、アプリケーションがA+ SSL評価ではない理由を分析できます。**A+ SSL評価以外**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、A+ SSL評価にアップグレードすることです。詳細については、A+ SSL評価へのアップグレードを参照してください。

詳細の下で、問題カテゴリ、問題、推奨事項などの問題の詳細を表示できます。

Appダッシュボードのトラブルシューティング

App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手順について説明します。

- アプリケーションをクリックしても、指定された期間（10〜15分）が経過しても、選択したアプリケーションの分析に必要なデータが表示されない。

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

- CSまたはLBアプリケーションがAppダッシュボードで常に灰色（**該当なし**ステータス）で表示される。

注

このドキュメントに記載されているトラブルシューティング手順は、**コンテンツスイッチング**および**負荷分散**仮想サーバーにのみ適用されます。

トラブルシューティングのシナリオ

アプリケーション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。

- **NetScaler Console** - **設定 > ライセンスと分析設定**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、「仮想サーバーのライセンス管理と分析の有効化」を参照して仮想サーバーをライセンスしてください。

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**メトリックコレクター**が有効になっていることを確認する必要があります。

注:

14.1-21.x以降のビルド以降、Metrics CollectorはNetScaler Consoleに追加された新しいNetScalerインスタンスではデフォルトで無効になっています。既存の管理対象インスタンスのメトリックコレクター設定は変更されません。

メトリックコレクターが有効になっていることを確認するには:

1. **Settings > Analytics Configuration**に移動します。
2. **Virtual Server Metrics Summary**の下にある**Configure Metrics**をクリックします。

3. **All Virtual Servers**ページで、各仮想サーバーのメトリックコレクターのステータスを表示できます。有効にする仮想サーバーを選択し、**Enable Metrics**をクリックします。

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

4. Metrics Collectorを有効にするには、**Enable Metrics**を選択します。リーン期間の使用状況分析を有効にして表示したい場合は、**Lean Data**を選択することもできます。選択後、**Save Configuration**をクリックします。

または、NetScaler®インスタンスページから仮想サーバーのメトリックコレクターとリーン使用状況を有効にすることもできます。

1. **Infrastructure > Instances**に移動し、インスタンスタイプを選択し、**Select Action**リストから**Metrics Collector**を選択します。
2. メトリックコレクターを有効にする仮想サーバーを選択し、**Enable Metrics**をクリックします。
3. Metrics Collectorを有効にするには、**Enable Metrics**を選択します。リーン期間の使用状況分析を有効にして表示したい場合は、**Lean Data**を選択することもできます。選択後、**Save Configuration**をクリックします。

メトリック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AppFlowコレクターで、**47.xビルドより前のもの**。
- NetScalerインスタンスビルドの**47.x以降**のアナリティクスプロファイル。

47.xビルドより前のNetScalerインスタンス

NetScalerの場合：

1. 次のコマンドを実行して、コレクターがポート5563で**UP**状態で実行されていることを確認します:

   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```

2. コレクターが利用できない場合は、NetScaler Consoleでインスタンスの手動ポーリングを実行します。

   a. **インフラストラクチャ > ネットワーク機能 > 今すぐポーリング** に移動します

   b. インスタンスを選択し、**Start Polling**をクリックします。

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

ポーリングが失敗した場合は、NetScaler ConsoleからNetScalerインスタンスを削除し、再度NetScalerインスタンスを追加します。NetScalerインスタンスを追加すると、コレクターがNetScalerに追加されます。

コレクターが**Down**ステータスを示している場合:

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. NetScalerインスタンスがNetScaler Consoleに到達可能であることを確認してください。

   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。

47.xビルド以降のNetScalerインスタンス

NetScaler Console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てください。

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: NetScaler Console** でフィルタリングします。
3. `adm_metric_collector_svc_<adm_receiver ip>`が利用可能であることを確認してください。IPアドレスは、NetScaler Console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てください。

それでもデータが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。

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**ダウン**状態を示している場合:

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

1. SNIPが構成されていることを確認します。

   SNIPが構成されていない場合は、SNIPを構成する必要があります。詳細については、SNIPの構成を参照してください。

2. NetScalerインスタンスがNetScaler Consoleに到達可能であることを確認します。

   pingテストを実行して検証できます。`ping -S <SNIP> <adm_receiver_ip>`を実行します

3. telnetを介したトラフィック接続がサービスに接続できることを確認します。

   telnetがサービスに接続できる場合、ファイアウォールが存在し、メトリックデータフローをブロックしています。ファイアウォールのブロック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。

NetScaler Consoleでインスタンスの手動ポーリングを実行する必要があります。

1. **インフラストラクチャ > ネットワーク機能 > 今すぐポーリング**に移動します
2. インスタンスを選択し、「**ポーリング開始**」をクリックします。

   ポーリングが失敗した場合は、次のコマンドを使用してNetScalerインスタンスでコレクターサービスを直接追加します。

   ```
   add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
   ```

   ```
   unset analyticsprofile ns_analytics_time_series_profile -collectors
   ```

   ```
   set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled
   ```

   分析時系列プロファイルが更新されます。

記載されているすべてのトラブルシューティング手順を実行しても問題がまだ解決しない場合は、**NetScalerサポート**にお問い合わせください。

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

アプリケーションの使用状況と異常

管理者として、アプリケーションがどのように利用されているかを確認する必要があります。アプリケーションの主要メトリックは、アプリケーションの使用状況を特定するのに役立ちます。アプリケーションへのトラフィック範囲は予測できないため、特定の期間に異常なアプリケーションパフォーマンスの逸脱が発生する可能性があります。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と思うかもしれません。

NetScaler Console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。**Applications > Dashboard** に移動し、アプリケーションをクリックして、**Key Metrics** タブを選択します。NetScaler Consoleはトラフィックパターンを監視し、主要メトリックが期待される範囲内にあるかどうかを分析します。期待される範囲から逸脱がある場合、NetScaler Consoleはそ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

詳細を表示するには、**Metrics with Anomalies** タブをクリックします。

各メトリックで、**See more** 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。

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
- 問題のトラブルシューティングを行うための**推奨アクション**
- **詳細**の下にある時間と異常の詳細

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

ピーク時と閑散時の使用状況分析

Webアプリケーションは、トラフィックが多い場合も少ない場合もあり、日ごとまたは時間ごとのトラフィック範囲は予測できません。同様に、Webアプリケーションは、スケジュールされたメンテナンスやアップグレード中に特定の期間のダウンタイムも必要とします。管理者として、トラフィックを分析し、適切な時間を見つける必要があります。

- Webアプリケーションをスケールアップする
- Webアプリケーションのダウンタイムを計画する

NetScaler Consoleのピーク使用量と閑散期分析機能を使用すると、選択した期間の主要なメトリックを分析できます。これらのメトリックから、トラフィックを分析し、Webアプリケーションをスケールアップする時期やスケジュールされたダウンタイムを計画する時期を決定できます。

アプリのスケーリング制限を評価する

App Dashboardからアプリケーションをクリックし、**Key Metrics**タブを選択して、すべてのメトリックの統合ビューを視覚化します。リストから期間を選択して、メトリックを分析します。

各メトリックについて、以下を表示できます。

- **最大** – 選択した期間の最大値を示します
- **平均** – 選択した期間の平均値を示します

画像の例によると、応答時間の最大値は1.3秒を示しています。グラフチャートから、選択した期間に高い応答時間が何回発生したかを分析できます。同様に、他のメトリックの詳細を表示し、アプリケーションがピーク使用量を受け取ったかどうかを分析し、本番環境をスケールアップする決定を下すこともできます。

上位5つのアプリメンテナンス期間を特定する

App Dashboardからアプリケーションをクリックし、**Key Metrics**タブを選択して、アプリケーションの閑散期を表示します。アプリケーションの一般的なダウンタイムは、要件に応じて1時間、2時間、または4時間です。ダウンタイムを計画したい時間 (1時間、2時間、または4時間) をリストから選択できます。リストから時間を選択した後、合計リクエスト数、スループット、データ量などのメトリックのトラフィックを分析できます。アプリケーションの使用量が少ないときに、ダウンタイムをスケジュールする適切な時間を選択できます。 次の例は、1時間のダウンタイムを分析するものです。

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

ヒートマップビューは、選択した期間のアプリケーションの使用状況を示します。色が濃いほど（青色）、アプリケーションの使用状況が高いことを示します。

ヒートマップビューは、アプリケーションのダウンタイムを計画するための上位5つの最も少ない期間（1、2、3、4、および5）も示しています。

1 – 水曜日の午後4時から午後5時までの最初の提案を示します

2 – 木曜日の午後9時から午後10時までの2番目の提案を示します

3 – 日曜日の午前7時から午後8時までの3番目の提案を示します

4 – 水曜日の午後12時から午後1時までの4番目の提案を示します

5 – 月曜日の午前7時から午後8時までの5番目の提案を示します

他のすべての日のトラフィックを分析した後で、ダウンタイムをスケジュールするために他の任意の日時を選択することもできます。

詳細を表示をクリックして、さらに詳細な情報を表示します。**合計リクエスト数**、**スループット**、または**データ量**タブをクリックして、上位5つの最も少ない期間と他の日の詳細を表示します。

リーン使用状況の詳細(/en-us/netscaler-console-service/media/lean-usage1.png)

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

アプリケーション使用状況分析

アプリケーション所有者は、パフォーマンスと使用状況の観点から、アプリケーション全体を評価し、視覚化できる必要があります。

改善された**App Dashboard**を使用すると、すべてのアプリケーションのパフォーマンスと使用状況のメトリックをまとめて表示できます。アプリケーションをクリックすると、既存のアプリケーションパフォーマンスメトリックに加えて、**Web Insight**タブに、以下の詳細なメトリックが表示されます。

- アプリケーションの使用状況を把握する。
- パフォーマンスの偏差を使用状況のメトリックと関連付ける。

  Web Insightの画像(/en-us/netscaler-console-service/media/web-insight-usage.png)

注:

- **14.1-51.x**リリース以降、Web InsightアナリティクスはIPv6アドレスで構成された仮想サーバーで表示されます。
- **14.1-1.16**以降のリリースでは、メトリックをドリルダウンすると、時系列グラフのアナリティクスビューに、選択した期間のnil値（例：0ミリ秒、0リクエスト）が表示されます。以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、アナリティクスビューはこれらのnil値をスキップしてグラフを表示していました。
- 各メトリックについて、最大値と合計値を示すオプションを表示できます。例：

```
>-  ![Example1](https://docs.netscaler.com/content/dam/netscaler/us/en/
netscaler-console-service/media/wi-sample.png) - The maximum client
network latency for the selected duration. Consider that you have the
network latency for client 1 = 30 ms, client 2 = 15 ms, and client 3 =
3 ms. In this scenario, the **Client Network Latency** displays 30 ms.

>

>-  ![Example2](https://docs.netscaler.com/content/dam/netscaler/us/en/
```

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

```
netscaler-console-service/media/wi-sample1.png) - The total bandwidth
consumed across all available clients/servers for the selected
duration. Consider that you have the bandwidth consumption for client 1
= 30 MB, Client 2 = 45 MB, Client 3 = 40 MB. In this scenario, the
Bandwidth displays (30 MB + 45 MB + 40 MB) = 115 MB.
```

選択した期間について、**Web Insight**タブから表示できるメトリックは次のとおりです。

- **アプリケーションサマリー** - アプリケーションメトリックの概要を表示します。
  - **リクエスト** – アプリケーションが受信した合計リクエストを表示します。**リクエスト**タブには、合計リクエストと上位5つのクライアントリクエストのグラフビューが表示されます。トグルオプションを使用してビューをカスタマイズできます。
  - **帯域幅** – アプリケーションによって処理された合計帯域幅を表示します。**帯域幅**タブには、合計帯域幅と上位5つのサーバー帯域幅のグラフビューが表示されます。トグルオプションを使用してビューをカスタマイズできます。
  - **応答時間** – アプリケーションからの平均応答時間を表示します。**リクエスト時間**タブには、選択した期間の応答時間の内訳、クライアント遅延、サーバー遅延、およびサーバー処理時間のグラフビューが表示されます。トグルオプションを使用してビューをカスタマイズできます。
  - **クライアントネットワーク遅延** – クライアントからの平均遅延を表示します。**クライアントネットワーク遅延**タブには、選択した期間の遅延の内訳のグラフビューが表示されます。
  - **サーバーネットワーク遅延** – サーバーからの平均遅延を表示します。**サーバーネットワーク遅延**タブには、選択した期間の遅延の内訳のグラフビューが表示されます。
  - **サーバー処理時間** – サーバーからの平均処理時間を表示します。**サーバー処理時間**タブには、選択した期間の処理時間の内訳のグラフビューが表示されます。

    概要タブでは、リクエスト、帯域幅、応答時間の相関関係をグラフビューで視覚化できます。

- **クライアント** – アプリケーションにアクセスしているクライアントのインサイトを表示します。

  - **合計クライアント** – アプリケーションにアクセスしている合計クライアントを表示します。**リクエスト**タブをクリックして表示します。
    - **クライアント** – クライアントの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。
- **クライアントネットワーク遅延 (最大)** – クライアントからの最大ネットワーク遅延。
- **リクエスト** – クライアントからの合計リクエスト数。
- **リクエストごとのパーセンテージ分布** – リクエストに基づいたパーセンテージ分布。たとえば、合計クライアントが4で、各クライアントが100リクエストの場合、各クライアントのパーセンテージ分布は25%です。

◦ **クライアントネットワーク遅延** – クライアントからNetScalerへのネットワーク遅延を表示します。**クライアントネットワーク遅延**タブをクリックして表示します。

- **クライアント** – クライアントのIPアドレス。
- **クライアントネットワーク遅延 (平均)** – クライアントからの平均ネットワーク遅延。
- **クライアントネットワーク遅延 (最大)** – クライアントからの最大ネットワーク遅延。
- **リクエスト** – クライアントからの合計リクエスト。
- **リクエストによる割合分布** – リクエストに基づく割合分布。

◦ **レンダリング時間** – サーバー応答のレンダリングにかかった時間を表示します。**レンダリング時間**タブをクリックして表示します。

- **クライアント** – クライアントのIPアドレス。
- **レンダリング時間 (平均)** – クライアントからの平均レンダリング時間。
- **リクエスト** – クライアントからの合計リクエスト。
- **リクエストによる割合分布** – リクエストに基づく割合分布。

- **サーバー** – アプリケーションにアクセスしているサーバーのインサイトを表示します。

> **注**
>
> 統合キャッシュリクエストの場合、IC通知とともにNetScaler仮想サーバーのIPアドレスを表示できます。詳細については、「統合キャッシュリクエスト」を参照してください。

◦ **合計サーバー** – アプリケーションにアクセスしている合計サーバーを表示します。**リクエスト**タブをクリックして表示します。

- **サーバー** – サーバーのIPアドレス。
- **サーバーネットワーク遅延 (平均)** – サーバーからの平均ネットワーク遅延。

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

- **サーバーネットワーク遅延 (最大)** – サーバーからの最大ネットワーク遅延。
- **リクエスト** – サーバーからの合計リクエスト数。
- **リクエストによる割合分布** – リクエストに基づいた割合分布。たとえば、合計サーバーが10台で、各サーバーが1000リクエストを持つ場合、各サーバーの割合分布は10%です。

- **サーバーネットワーク遅延 (最大)** – サーバーからNetScalerへの最大ネットワーク遅延を表示します。**サーバーネットワーク遅延**タブをクリックして表示します。
  - **サーバー** – サーバーのIPアドレス。
  - **サーバーネットワーク遅延 (平均)** – サーバーからの平均ネットワーク遅延。
  - **サーバーネットワーク遅延 (最大)** – サーバーからの最大ネットワーク遅延。
  - **リクエスト** – サーバーからの合計リクエスト数。
  - **リクエストによる割合分布** – 合計リクエスト数に基づいた割合分布。
- **サーバー応答時間 (最大)** – サーバーがリクエストに応答するのにかかった最大時間を表示します。**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数。
  - **リクエスト別の割合分布** – 総リクエスト数に基づく割合分布。
- **帯域幅** – サーバーによって消費された総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総帯域幅。
  - **リクエスト** – サーバーからの総リクエスト数。
  - **リクエスト別の割合分布** – 総リクエスト数に基づく割合分布。

- **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。

  - **総ロケーション数** – 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ロケーション数を表示します。

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

- **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** – すべてのロケーションのクライアントによって消費された総帯域幅を表示します。
- **リクエスト** – すべてのクライアントロケーションからの総リクエスト数を表示します。

  各タブをクリックして表示します。

  - **国** – ロケーション名。
  - **応答時間** – クライアントの場所からの平均応答時間。
  - **Bandwidth** – クライアントの場所から消費された帯域幅。
  - **Requests** – クライアントの場所からの合計リクエスト。
  - **リクエストによる割合の分布** – 合計リクエスト数に基づく割合の分布。例えば、合計ロケーションが10、合計リクエストが100万、国Aだけで90万のリクエストを受け取った場合、国Aの割合の分布は90%になります。他の国々は、それぞれの国で受け取ったリクエスト数に基づいて残りの割合の分布を受け取ります。

- **URL** – ロード時間とレンダリング時間が長いURLのインサイトを表示します。

  - **合計URL** – 合計URLを表示します。**Requests**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のロードにかかる平均時間。
    - **リクエスト** – そのURLからの合計リクエスト。
    - **リクエストによる割合の分布** – 合計リクエスト数と各URLにおける割合の分布。
  - **ロード時間** – URLのロードにかかる時間を表示します。**Load Time**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のロードにかかる平均時間。
    - **リクエスト** – そのURLからの合計リクエスト。
    - **リクエストによる割合の分布** – 合計リクエスト数に基づく割合の分布。
  - **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。「**Render Time**」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.

- **レンダリング時間 (平均)** – URLがレンダリングされるまでにかかった平均時間。
- **リクエスト** – URLからの合計リクエスト数。
- **リクエストごとの割合分布** – 合計リクエスト数に基づく割合分布。

- **HTTP応答ステータス** – 特定の完了したHTTPリクエストに関するインサイトを表示します。

  - **応答ステータス** – 2xx、4xx、5xxなどの応答コードを表示します。
  - **応答ステータスの理由** – 内部サーバーエラー、見つかりません、などの応答理由を表示します。
  - **発生回数** – 合計発生回数を表示します。

- **オペレーティングシステム** – アプリケーションにアクセスしているOSに関するインサイトを表示します。

  - **リクエスト** – 各オペレーティングシステムからの合計リクエスト数を表示します。
  - **帯域幅** – 各オペレーティングシステムによって消費された合計帯域幅を表示します。
  - **ロード時間** – 各オペレーティングシステムがサーバーからロードするまでにかかった合計時間を表示します。

- **ブラウザ** – クライアントがアプリケーションにアクセスするために使用する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および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**タブをクリックして、SSLエラーの種類と合計発生数を表示します。
  - **バックエンド** – バックエンドサーバーからのSSLエラーの合計数を表示します。**バックエンド**タブをクリックして、SSLエラーの種類と合計発生数を表示します。

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

- **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**タブをクリックして、証明書名と合計ヒット数を表示します。
  - **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**タブをクリックして、SSL/TSLプロトコルと合計ヒット数の詳細を表示します。
  - **暗号** – 暗号の合計数を表示します。**暗号**タブをクリックして、各暗号スイート名と合計ヒット数の詳細を表示します。
  - **キー強度** – SSL証明書で使用されている合計キー強度を表示します。**キー強度**タブをクリックすると、各キー強度と合計ヒット数の詳細が表示されます。

メトリックの詳細をグラフ形式で表示

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、グラフ形式で詳細を表示できます。**>**をクリックすると、グラフ形式で詳細が表示されます。

グラフ形式(/en-us/netscaler-console-service/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以下の詳細を表示できます。

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
	クライアントネットワーク遅延 (最大)	クライアントからNetScalerインスタンスへの最大ネットワーク遅延を示します
	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
	レンダリング時間 (平均)	クライアントがサーバー応答をレンダリングするのにかかった平均時間を示します
	リクエスト	クライアントからの合計リクエスト数を示します

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

インサイト名	メトリック	説明
サーバー	サーバー	サーバーリストおよびNetScaler仮想サーバー (統合キャッシュリクエストの場合) 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
	サーバーネットワーク遅延 (最大)	サーバーからNetScalerインスタンスへの最大ネットワーク遅延を示します
	サーバー応答時間 (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
	サーバー応答時間 (最大)	サーバーがリクエストを処理するのにかかった最大時間を示します
	リクエスト	サーバーが受信した合計ヒット数を示します
	統合キャッシュヒット	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示します
	統合キャッシュミス	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示します
地理的位置	国	クライアントの場所を示します
	応答時間 (平均)	クライアントの場所からの平均応答時間を示します
	帯域幅	その場所から消費された合計帯域幅を示します

© 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	その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読み込むのにかかった平均時間を示します
	読み込み時間 (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
	リクエスト数	URLからの総ヒット数を示します
HTTP応答ステータス	応答ステータス	OK、Not found、Internal Server Errorなどの応答ステータス名を示します
	応答ステータス理由	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
	発生回数	応答コードからの総ヒット数を示します
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。
	レンダリング時間	オペレーティングシステムがサーバーからレンダリングされるまでにかかった合計時間を示します。
	帯域幅	オペレーティングシステムによって消費された合計帯域幅を示します。
	リクエスト	オペレーティングシステムからの合計リクエスト数を示します。

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

インサイト名	メトリック	説明
ブラウザ	ブラウザ	Mozilla Firefox、Chromeなどのブラウザ名を示します。
	レンダリング時間	ブラウザがサーバーからレンダリングされるまでにかかった合計時間を示します。
	帯域幅	ブラウザによって消費された合計帯域幅を示します。
	リクエスト	ブラウザからのリクエストの合計数を示します
SSLエラー	SSL障害タイプ	CLIENTAUTH FAILUREなどのエラー名を示します
	発生回数	SSLエラーの総発生回数を示します
SSL使用状況	TLS、SSLなどのプロトコル名とバージョンを示します	
	発生回数	プロトコルからの総ヒット数を示します

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

SSL証明書管理を自動化する

デジタルセキュリティを維持するには、環境内のSSL証明書の管理を自動化する必要があります。すべての証明書をプロアクティブに管理および監視し、有効期限が近づいている証明書を通知し、有効期限が切れる前に証明書を自動的に更新する方法が必要です。期限切れのSSL証明書はセキュリティリスクにつながります。NetScalerインスタンスにインストールされているSSL証明書の管理を自動化するために、Venafi Trust Protection PlatformサーバーをNetScaler Consoleで構成できます。

NetScaler ConsoleでVenafiを使用すると、SSL証明書をそのライフサイクル全体にわたって管理できます。NetScaler Consoleの**アプリケーション**ダッシュボードで、次のタスクを実行できます。

- SSLの問題とアプリケーションスコアを確認します。
- SSLの問題をトラブルシューティングし、推奨される修復を適用します。
- アプリケーションにバインドされている証明書を確認します。
- 証明書を迅速に作成、インストール、更新します。
- 証明書の更新を自動化します。
- 生成された証明書をNetScaler仮想サーバーにバインドして、アプリケーションを保護します。
- 特定のアプリケーションに関するすべてのSSLタスク関連ログを確認します。

NetScaler ConsoleでVenafiサーバーを構成する

Venafiサーバーの構成は2段階のプロセスです。まず、NetScaler ConsoleにVenafiサーバーを追加します。次に、Venafiサーバーでポリシーを構成します。NetScaler ConsoleにVenafiサーバーを追加するには、NetScaler Console GUIから**インフラストラクチャ > SSLダッシュボード > サードパーティCA**に移動します。**追加**をクリックします。

Venafiサーバーを追加する(/en-us/netscaler-console-service/media/add-venafi-server.png)

提供されたフィールドに詳細を入力します。証明書を自動的に更新する場合は、**自動更新**オプションをオンにします。各フィールドの詳細については、フィールドにカーソルを合わせ、`i`アイコンをクリックしてください。

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

注

ポリシーフォルダにはサブフォルダが設定されている必要があります。

例:

```
"policy_folder": "\\VED\\Policy\\TLS
TLS Certificates
NetScaler Console"
```

Venafiサーバーを設定したら、NetScaler Consoleダッシュボードを使用してSSL証明書を管理できます。

SSL証明書のライフサイクルを管理する

アプリケーションダッシュボードは、SSL証明書をエンドツーエンドで管理するためのワンストップの場所です。NetScaler Console GUIから、**Applications > App Dashboard**に移動します。**Issue Categories**の下で、**SSL Config**を選択します。**Current Issues**の下で、アプリケーションのSSL関連の問題を確認できます。SSLレポートを表示するには、**Applications**の下でアプリにカーソルを合わせます。レポートの詳細を表示するには、アプリをクリックします。この例では、スコアが27のアプリケーションがあります。

- [ ] さらに、重大またはレビューなどの**アプリケーションスコア**を使用して問題をフィルタリングできます。SSLアプリケーションスコアは、ダッシュボードの右上隅にある**Manage Apps**設定でデフォルトで有効になっているSSLパラメータに基づいています。

- [ ] SSLパラメータのいずれかを無効にするには、チェックボックスをオフにして**OK**をクリックします。SSLレポートの詳細を表示するには、**Applications**の下で、レポートを表示したいアプリをクリックします。

- [ ] パフォーマンススコアを確認し、ページを下にスクロールして、アプリが持つ仮想サーバー、仮想サーバーにバインドされている証明書、および証明書の問題などの詳細を確認できます。証明書の詳細を表示するには、**Certificate Name**の下のリンクをクリックします。期限切れの証明書については、更新できます。

証明書の更新には、証明書の作成、インストール、および仮想サーバーへのバインドが含まれます。

SSL証明書の確認と更新(/en-us/netscaler-console-service/media/ssl-cert-link.png)

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

注

NetScaler Console に Venafi サーバーを追加する際に、自動更新オプションを有効にすると、証明書は有効期限が切れる前に自動的に更新されます。

SSL証明書の更新をクリックすると、**SSL**タブに移動します。そこには、アプリケーションの仮想サーバーにバインドされているすべての証明書が一覧表示されます。このタブを使用して、証明書を作成およびインストールし、仮想サーバーにバインドできます。また、特定のアプリケーションに関するすべてのSSLタスク関連ログを、特定のアプリケーションのSSLタスク関連ログで確認できます。

SSLタブ(/en-us/netscaler-console-service/media/ssl-tab.png)

証明書を作成するには、**証明書の作成**をクリックして詳細を入力します。ダウンロードされた証明書は暗号化されているため、パスワードを入力し、**作成**をクリックします。NetScaler Console は Venafi サーバーに接続して証明書を作成します。証明書がダウンロードされたら、**閉じる**をクリックします。

Venafi を使用して証明書を作成(/en-us/netscaler-console-service/media/download-ssl-cert-venafi.png)

次に、**SSL**タブで**証明書のインストール**をクリックします。ダウンロードした証明書を選択し、**インストール**をクリックします。NetScaler Console を使用して NetScaler に SSL 証明書をインストールする方法の詳細については、トピック「NetScaler インスタンスに SSL 証明書をインストールする」の「NetScaler Console から SSL 証明書をインストールする」セクションを参照してください。

次に、**証明書のバインド**をクリックします。必要に応じて、証明書のバインドを解除することもできます。次回のSSLポーリング後、アプリケーションダッシュボードは新しいデータで更新されます。特定のアプリケーションに関するすべてのSSLタスクログを確認したい場合は、**証明書タスクログ**をクリックします。

証明書タスクログ(/en-us/netscaler-console-service/media/certificate-task-log.png)

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

A+ SSL評価分析

注記:

準拠していないSSL証明書の一括アップグレードには、**タスクのSSL A+評価アップグレード**を使用できます。

アプリケーションは、SSLトランザクションにセキュアな暗号とプロトコルを使用する必要があります。そうしないと、アプリケーションにアクセスするユーザーのプライバシー、データ整合性、およびセキュリティに影響を与える可能性があります。NetScaler Consoleは、アプリケーションの仮想サーバーSSL設定をNetScalerセキュアフロントエンドプロファイルでレビューします。A+評価に必要な設定は、セキュアフロントエンドプロファイルにプリロードされています。

アプリケーション所有者は、自分のアプリケーションが**A+**評価であるかどうかを評価できます。また、アプリケーションのプロトコルと暗号スイートのスコアを表示することもできます。アプリケーションが**A+**評価でない場合は、**A+**評価にアップグレードできます。

アプリケーションのSSL評価を表示するには：

1. **Applications > Dashboard**に移動します。
2. SSL評価に基づいてアプリケーションをフィルタリングします。

   評価がないアプリケーションは、**NA**に分類されます。
3. GUIから必要なアプリケーショングリッドを選択します。
4. **SSL**タブを選択します。このタブには、アプリケーションのSSL評価が表示されます。

SSLタブには、アプリケーションの評価を変更またはアップグレードするための次のいずれかのオプションが用意されています。

- A+ SSL評価にアップグレード
- SSL評価をロールバックする(#roll-back-ssl-rating)

A+ SSL評価にアップグレードする

アプリケーションをA+ SSL評価にアップグレードすると、NetScalerインスタンスのデフォルトSSLプロファイルのステータスに応じて、以下の変更が発生します。

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

- デフォルトのSSLプロファイルが無効になっている場合、NetScaler ConsoleはSSL仮想サーバーの推奨SSL設定に変更します。
- デフォルトのSSLプロファイルが有効になっている場合、NetScaler Consoleはセキュアプロファイルに基づいて、推奨されるA+設定を持つ新しいSSLプロファイルを作成します。

A+評価のないアプリケーションは、影響を受ける仮想サーバーの詳細をSSLタブに表示します。

App Detailsでは、セキュアなフロントエンドプロファイルに準拠していない仮想サーバーの詳細を確認できます。また、**Recommendation**列には修復策が表示されます。これらの対策は、アプリケーションをセキュアなフロントエンドプロファイルに準拠させるために提供されます。

この例では、仮想サーバーにいくつかのセキュリティ問題があります。**Protocol TLSv1.0 enabled**はそのような問題の1つです。**App Details**セクションでは、この問題を解決するための適切なアクションを推奨しています。それぞれの推奨事項に従って、これらの問題をすべて解決するには、次の手順を実行します。

1. **Upgrade to A+ rating**をクリックします。

   確認メッセージには、仮想サーバーで実行されるコマンドが表示されます。これらのコマンドは、アプリケーションのトラフィックに影響を与える可能性があります。
2. コマンドを確認し、**Confirm**をクリックします。

SSL評価をロールバックする

注記:

アプリケーションをA+ SSL評価にアップグレードした場合、アップグレード後7日以内であれば元の評価に戻すことができます。

アプリケーションをA+評価にアップグレードした後、SSL insightで受信トラフィックを分析できます。このページには、SSLトランザクションがネゴシエートされる暗号とプロトコルが表示されます。

ただし、正当なトラフィックの一部がドロップされていることに気付いた場合は、アプリケーションに設定されているセキュアなフロントエンドプロファイルをロールバックできます。このアクションにより、SSL評価が以前の評価に戻ります。

SSL評価をロールバックするには、次の手順を実行します。

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

1. をクリックします。

   確認メッセージには、仮想サーバーで実行されるコマンドが表示されます。
2. コマンドを確認し、 をクリックします。

アプリケーショントラフィックに対するSSL評価の影響を判断する

SSL評価をアップグレードすると、アプリケーションのトラフィックに影響が出る可能性があります。 で、アップグレード後に接続が切断されたかどうかを確認できます。この情報に基づいて、SSL評価を継続するかロールバックするかを決定できます。

次のグラフの例では、SSL評価を**A+**にアップグレードした後、一部の接続が切断されています。

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

Web Insight ダッシュボード

注:

14.1-51.x リリース以降、Web Insight 分析は IPv6 アドレスで構成された仮想サーバーで表示できます。

改善されたWeb Insight機能は拡張され、Webアプリケーション、クライアント、およびNetScalerインスタンスの詳細なメトリックに対する可視性を提供します。この改善されたWeb Insightにより、パフォーマンスと使用状況の両方の観点からアプリケーション全体を評価および視覚化できます。管理者として、Web Insightを次の目的で表示できます。

- アプリケーション。**アプリケーション > ダッシュボード**に移動し、アプリケーションをクリックして、**Web Insight**タブを選択すると、詳細なメトリックが表示されます。詳細については、「アプリケーション使用状況分析」を参照してください。
- すべてのアプリケーション。**アプリケーション > Web Insight**に移動し、各タブ（アプリケーション、クライアント、インスタンス）をクリックして、次のメトリックを表示します。

アプリケーション	クライアント	URL	インスタンス
応答時間異常のあるアプリケーション	クライアント	URL	インスタンスメトリック
アプリケーション	地理的位置		アプリケーション
サーバー	HTTPリクエストメソッド		ドメイン
ドメイン	HTTP応答ステータス		URL
地理的位置	URL		HTTPリクエストメソッド
URL	オペレーティングシステム		HTTP応答ステータス

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

アプリケーション	クライアント	URL	インスタンス
HTTPリクエストメソッド	ブラウザ		クライアント
HTTP応答ステータス	SSLエラー		サーバー
SSLエラー	SSL使用状況		オペレーティングシステム
SSL使用状況			ブラウザ

Webインサイト(/en-us/netscaler-console-service/media/web-insight-app.png)

各メトリックで、上位5つの結果を表示できます。クリックしてさらにドリルダウンし、問題を分析してトラブルシューティングアクションをより迅速に実行できます。

注

- **14.1-1.16**以降のリリースでは、メトリックをドリルダウンすると、時系列グラフの分析ビューに、選択した期間のnil値（たとえば、0ミリ秒と0リクエスト）が表示されます。以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、分析ビューはそれらのnil値をスキップしてグラフを表示していました。
- 一部のシナリオでは、NetScalerが一部のトランザクションのRTT値を計算できない場合があります。そのようなトランザクションの場合、NetScaler ConsoleはRTT値を次のように表示します。
  - **NA** – NetScalerインスタンスがRTTを計算できない場合に表示されます。
  - **< 1ms** – NetScalerインスタンスが0ミリ秒から1ミリ秒の間の小数でRTTを計算する場合に表示されます。たとえば、0.22ミリ秒です。

暗号関連の問題の詳細を表示

SSLエラーの下で、以下のSSLパラメータの詳細を表示できます。

- 暗号の不一致
- サポートされていない暗号

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

SSLエラーの下で、SSLパラメータ（暗号の不一致またはサポートされていない暗号）をクリックすると、SSL暗号名、推奨されるアクション、影響を受けるアプリケーションとクライアントの詳細などの詳細を表示できます。

選択したSSLパラメータの詳細ページが表示されます。次のことができます。

- **推奨されるアクション**で提供されている提案を確認します。
- **SSL暗号**の下で、暗号名と発生回数を表示します。
- 影響を受けるアプリケーションとクライアントの合計数を表示します。

選択したSSL暗号の影響を受けるアプリケーションとクライアントを表示するには、**SSL暗号名**をクリックします。

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ラウンドトリップを必要とせずにWebコンテンツをユーザーに提供します。

統合キャッシュリクエストは現在、**サーバー**の下に表示され、NetScaler仮想サーバー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-console-service/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、**サーバーメトリック**に統合キャッシュヒットとミスのタブが表示されます。

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-console-service/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。

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

統合キャッシュミス(/en-us/netscaler-console-service/media/web-insight-server-integrated-miss.png)

その他のユースケース

1ヶ月間のサーバーネットワーク遅延を分析し、本番環境をスケールアップまたはスケールダウンするかどうかを決定したいとします。これを分析するには:

1. リストから「過去1ヶ月」を選択し、**アプリケーション**タブから**サーバー**までスクロールして、サーバーをクリックします。

   アプリケーションWeb Insight(/en-us/netscaler-console-service/media/app-wi-server.png)

   選択したサーバーのメトリック詳細が表示されます。
2. 遅延を分析するには、**サーバーネットワーク遅延**タブを選択します。

   サーバーネットワーク遅延(/en-us/netscaler-console-service/media/app-wi-serverlatency.png)

   平均レイテンシは10.01秒を示しており、グラフから、過去1か月のサーバーネットワークレイテンシ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。

アプリケーションの遅延の根本原因を分析する

アプリケーションの遅延は、ビジネスへの影響や生産性の低下につながるため、どの組織にとっても大きな懸念事項です。管理者として、ビジネスへの影響を避けるために、すべてのアプリケーションが最適に動作することを確認する必要があります。ユーザーがアプリケーションへのアクセスに遅延を感じた場合、問題が次のいずれかにあることを確認する必要があります。

- クライアントネットワークの遅延
- サーバーネットワークの遅延
- サーバー処理時間

NetScaler Consoleは、特定の前提条件に基づいて、1時間ごとに異常チェックを実行し、過去1時間のトラフィックの異常を報告します。たとえば、誤検知を避けるために、応答時間が1ミリ秒未満の場合、その結果に対する異常チェックはスキップされます。

「**アプリケーション > Web Insight**」ページでは、選択した期間の応答時間異常があるアプリケーションを表示できます。「**応答時間異常のあるアプリケーション**」メトリックには、合計異常数

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

に基づいて上位5つのアプリケーションが表示されます。すべてのアプリケーションを表示するには、「**詳細を表示**」をクリックします。

アプリケーション応答時間の異常(/en-us/netscaler-console-service/media/app-anomalies.png)

- **アプリケーション** – アプリケーション名を示します。
- **合計異常数と寄与要因** – アプリケーションからの合計異常数を示します。マウスカーソルを合わせると、クライアントネットワークの遅延、サーバーネットワークの遅延、およびサーバー処理時間からの合計異常数をそれぞれ表示できます。
- **応答時間範囲** – アプリケーションからの予想される応答時間範囲を示します。
- **最大異常応答時間** – アプリケーションからの最高の応答時間を示します。
- **最大異常寄与要因** – アプリケーションの最大異常数が、クライアントネットワークの遅延、サーバーネットワークの遅延、またはサーバー処理時間のいずれに起因するかを示します。

アプリケーションのドリルダウン

アプリケーションをクリックすると、選択した期間の「**アプリケーションメトリック**」の詳細が表示されます。

「**アプリケーションメトリクス**」では、以下を表示できます。

- **概要** – 応答時間、リクエスト、帯域幅などのアプリケーションパフォーマンスを視覚化するための概要
- **リクエスト** – アプリケーションが受信した合計リクエスト。合計リクエストに基づいて、上位5つのクライアントからのリクエストも表示できます。
- **帯域幅** – アプリケーションによって処理された合計帯域幅。合計帯域幅消費量に基づいて、上位5つのサーバーからの帯域幅消費量も表示できます。
- **応答時間** – クライアントネットワーク遅延、サーバーネットワーク遅延、サーバー処理時間を同じグラフで視覚化するための概要
- **クライアントネットワーク遅延** – 平均クライアントネットワーク遅延（クライアントからNetScalerまで）
- **サーバーネットワーク遅延** – 平均サーバーネットワーク遅延（NetScalerからサーバーまで）
- **サーバー処理時間** – 平均サーバー処理時間（サーバーからNetScalerまで）

アプリケーションに異常がある場合、その異常がクライアントネットワーク遅延、サーバーネットワーク遅延、またはサーバー処理時間のいずれに起因するかを確認できます。各タブをクリックして詳細を表示します。

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

クライアントネットワーク遅延タブと**サーバーネットワーク遅延**タブでは、以下を表示できます。

- **検索バー** - 検索バーをクリックすると、すべてのクライアント（クライアントネットワーク遅延）およびサーバー（サーバーネットワーク遅延）のIPアドレスが表示されます。IPアドレスを選択して結果をフィルタリングできます。
- **エクスポートオプション** - **CSVのダウンロード**をクリックして、詳細をCSV形式でエクスポートします。

応答時間

Anomaly Detailsで、応答時間の寄与者（クライアントからサーバーまで）の詳細を表示するにはクリックします。以下の例では、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間の異常があります。また、予想される範囲と、予想範囲を超えて発生した違反も表示できます。

Recommended Actionsは、異常に対する考えられる解決策を提案します。

同様に、**Client Network Latency**、**Server Network Latency**、および**Server Processing Time**タブをクリックして、以下を表示できます。

- 予想範囲を超えた異常。
- 考えられる解決策を提案する推奨アクション。

アプリケーションが正常に動作している場合、アプリケーションメトリックは異常なしとして表示されます。

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

サービスグラフ

NetScaler Console のサービスグラフ機能を使用すると、すべての Kubernetes サービスをグラフィカルに監視できます。この機能では、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。**Applications > Service Graph** に移動して、次のサービスグラフを表示します。

- すべての NetScaler インスタンスで構成されたアプリケーション(#service-graph-for-applications-across-all-pagecitrix-adc-generic-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` ビューを包括的に視覚化できます。この単一ペインのサービスグラフビューから、管理者として次のことができます。

- ユーザーが特定のアプリケーション（3層Webアプリおよびマイクロサービスアプリ）にどの地域からアクセスしているかを把握する
- 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いずれから発生しているかを把握する
- 問題をトラブルシューティングするためにさらにドリルダウンする

Applications > Service Graph に移動し、**Global** タブをクリックして表示します。

- 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

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

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。

- 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、次の操作を行います。

- エンドツーエンドのアプリケーション全体のパフォーマンスを確保する
- アプリケーションのさまざまなコンポーネント間の相互依存性によって生じるボトルネックを特定する
- アプリケーションのさまざまなコンポーネントの依存関係に関するインサイトを収集する
- Kubernetesクラスター内のサービスを監視する
- 問題のあるサービスを監視する
- 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
- クライアントメトリックとクライアントトランザクションの概要詳細を表示する

NetScaler Consoleでこれらのメトリックを視覚化することで、問題の根本原因を分析し、必要なトラブルシューティングアクションをより迅速に実行できます。サービスグラフは、アプリケーションをさまざまなコンポーネントサービスとして表示します。Kubernetesクラスター内で実行

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

されているこれらのサービスは、アプリケーション内外のさまざまなコンポーネントと通信できます。開始するには、「サービスグラフの設定」を参照してください。

3層Webアプリケーションのサービスグラフ

アプリケーション > サービスグラフに移動し、**Webアプリ**タブをクリックして表示します。

- アプリケーションがどのように構成されているか（コンテンツスイッチング仮想サーバーと負荷分散仮想サーバーを使用）に関する詳細

  GSLBアプリケーションの場合、データセンター、NetScalerインスタンス、CS、およびLB仮想サーバーを表示できます。
- クライアントからサービスへのエンドツーエンドトランザクション
- クライアントがアプリケーションにアクセスしている場所
- クライアント要求が処理されるデータセンター名と、関連するデータセンターNetScalerメトリック（GSLBアプリケーションのみ）
- クライアント、サービス、および仮想サーバーのメトリック詳細
- エラーがクライアントからのものか、サービスからのものか
- **Critical**、**Review**、**Good**などのサービスステータス。NetScaler Consoleは、サービス応答時間とエラー数に基づいてサービスステータスを表示します。
  - **重大 (赤)** - 平均サービス応答時間 > 200 ミリ秒 AND エラー数 > 0 の場合を示します
  - **確認 (オレンジ)** - 平均サービス応答時間 > 200 ミリ秒 OR 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 ミリ秒の場合を示します
- **重大**、**確認**、**良好**などのクライアントステータス。NetScaler Console は、クライアントのネットワーク遅延とエラー数に基づいてクライアント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 ミリ秒 AND エラー数 > 0 の場合を示します
  - **確認 (オレンジ)** - 平均クライアントネットワーク遅延 > 200 ミリ秒 OR 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 ミリ秒の場合を示します
- **重大**、**確認**、**良好**などの仮想サーバステータス。NetScaler Console 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。

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

- **重大 (赤)** - アプリスコア < 40 の場合を示します
- **確認 (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:

- 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。
- 仮想サーバーとWebアプリケーション間にアクティブなトランザクションがない場合、サービスグラフで詳細を表示できるのは、ロードバランシング、コンテンツスイッチング、GSLB仮想サーバー、サービスなどの構成データに基づいている場合のみです。
- アプリケーション構成に変更があった場合、サービスグラフに反映されるまでに10分かかることがあります。

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

NetScaler Consoleのサービスグラフ機能を使用すると、Kubernetesアプリケーションをグラフィカルに監視できます。サービスグラフのオンボーディングと設定、サービスとイングレスの詳細の表示、しきい値の構成、リクエストのトレース、マイクロサービス全体の問題のトラブルシューティングを行うことができます。

以下のトピックは、Kubernetesアプリのサービスグラフの設定と使用に役立ちます。

- サービスグラフのオンボーディングの簡素化
- サービスグラフの設定
- サービスグラフでの詳細の表示
- サービスグラフでのしきい値の構成
- 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

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

- 診断の表示

サービスグラフ - 簡素化されたオンボーディング

サービスグラフのオンボーディングプロセスは簡素化されており、サービスグラフをオンボーディングするには、次の方法があります。

- Kubernetesジョブとしてエージェントを自動的に展開する(#automatically-deploying-an-agent-as-a-kubernetes-job)。
- サービスグラフを手動で構成する(#manually-configuring-service-graph)。

Kubernetesジョブとしてエージェントを自動的に展開する

サービスグラフのオンボーディングプロセスを自動化でき、このプロセスは自動的に次のことを行います。

- エージェントに必要なYAMLをダウンロードします。
- エージェントを構成します。
- NetScaler ConsoleにKubernetesクラスターを登録します。
- NetScaler Consoleでサービスグラフを生成するために必要な設定を実行します。

前提条件

次のものがあることを確認してください。

- Citrix Cloudアカウント。
- Kubernetesバージョン1.19以降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。
- 必要なポートを開きました。
- 静的ルートを設定して接続を確立しました。エージェントを使用してNetScaler ConsoleにNetScaler MPXまたはVPXを登録するには、クラスターノードとNetScaler MPXまたはVPX間の接続を確立する必要があります。

> **注:**
>
> 静的ルートを設定したくない場合は、ノードコントローラーを設定できます。詳細については、`https://github.com/citrix/citrix-k8s-node-controller`および`https://github.com/citrix/citrix-helm-charts/tree/master/citrix-node-controller`を参照してください。

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

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

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

1. citrix.cloud.comにログオンします
2. **ホーム**アイコンをクリックし、**Identity and Access Management**を選択します

3. **API Access**タブから、安全なクライアント名を入力し、**Create Client**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**をクリックしてCSVファイルを保存します。

5. Kubernetesメインノードで、IDとシークレットを使用して認証トークンを作成するには、次のコマンドを実行します。 `wget https://raw.githubusercontent.com/citrix/citrix-helm-charts/master/generate_token.py`

   `python3 generate_token.py --accessID=<accessID> --accessSecret=<accessSecret>`

   注

   > 認証トークンは1時間のみ有効です。

以下を構成できます。

- 自動シークレットを作成してNetScalerエージェントを構成する

または

- 手動シークレットを作成してNetScalerエージェントを構成する

自動シークレットを作成してNETSCALER CONSOLEを構成する

Helmチャートを使用してエージェントを展開する
エージェントを展開するには、Kubernetesメインノードで次のコマンドを実行します。

`helm repo add citrix https://citrix.github.io/citrix-helm-charts`

`helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set token=<Token>`

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

エージェントが展開され、クラスターがNetScaler Consoleに登録されます。自動シークレットを使用してエージェントを作成すると、エージェントの資格情報を含むKubernetes Secretを作成できるエージェントとともに、`adm-agent-helper`も展開できるようになります。

このプロセスは、名前空間が`citrix-cpx=enabled`としてラベル付けされている場合に自動的に行われます。Kubernetesメインノードで次のコマンドを実行します。

```
kubectl label namespace <namespace> citrix-cpx=enabled
```

注

> `adm-agent-helper`をデプロイしない場合は、エージェントのログインシークレットを手動で作成できます。

NetScaler VPX/MPXをNetScaler Consoleに登録する

注

> NetScaler VPX/MPXをNetScaler Consoleに登録できるのは、追加のメリットのためだけです。

NetScaler VPX/MPXをNetScaler Consoleに登録するには、静的ルートを設定して、NetScaler VPXまたはMPXとクラスターノード間の接続を確立する必要があります。Citrix-node-controllerを設定している場合は、このプロセスを無視できます。

名前空間にNetScaler VPX/MPXのログイン資格情報を含むKubernetesシークレットを作成する必要があります。このプロセスが完了すると、エージェントのオンボーディングが開始されます。

```
kubectl create secret generic nslogin --from-literal=username=<username> --from-literal=password=<adc-password> -n <namespace>
```

NetScaler VPX/MPXの管理IPアドレスを環境変数として設定する必要があります: `adc.IP`。

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set adc.IP=<ADC ManagementIP>,adc.loginSecret=nslogin --set token=<Token>
```

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

注

管理HTTPポートadc.mgmtHTTPPortとHTTPSポートadc.mgmtHTTPSPort（それぞれ80と443）が開いていることを確認してください。

手動シークレットを作成してエージェントを構成する

NetScaler CPXは、NetScaler Consoleに登録するためにエージェントのログイン資格情報を必要とします。NetScaler CPXをデプロイする名前空間を手動で設定できます。

```
kubectl create secret generic admlogin --from-literal=username=nsroot --from-literal=password=<adm-agent-password> -n <namespace>
```

シークレットを作成したら、次のコマンドを使用してエージェントを構成できます。

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set admAgent.loginSecret=admlogin --set token=<Token>
```

NetScaler VPX/MPX を NetScaler Console に登録する

NetScaler VPX/MPX を NetScaler Console に登録するには、静的ルートを構成して、NetScaler VPX または MPX とクラスターノード間の接続を確立する必要があります。`Citrix-node-controller` を構成している場合は、このプロセスを無視できます。

静的ルートを構成した後、名前空間に NetScaler VPX/MPX のログイン資格情報を含む Kubernetes シークレットを作成する必要があります。このプロセスが完了すると、エージェントのオンボーディングが開始されます。

```
kubectl create secret generic nslogin --from-literal=username=<username> --from-literal=password=<adc-password> -n <namespace>
```

NetScaler VPX/MPX の管理 IP アドレスを環境変数として設定する必要があります: `adc.IP`。

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set adc.IP=<ADC ManagementIP>,adc.loginSecret=nslogin --set token=<Token>
```

注

管理 HTTP ポート adc.mgmtHTTPPort と HTTPS ポート adc.mgmtHTTPSPort がそれぞれ 80 と 443 で開いていることを確認してください。

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

上記の手順を構成すると、サービスグラフは 15 分以内に表示され始めます。NetScaler Console で、**Applications > Service Graph** に移動し、**Microservices** をクリックしてサービスグラフを表示します。

例:

- Service Mesh Lite でサービスグラフを生成するには、サービスグラフの例 を参照してください。
- Istio Service Mesh との Citrix 統合のサービスグラフを生成するには、NetScaler Observability と NetScaler Console を使用したサービスグラフ を参照してください。

サービスグラフの手動設定

サービスグラフは、次の方法で手動で設定できます。

- Kubernetesクラスターでエージェントをマイクロサービスとして構成する。
- クラスターの登録、インスタンスの追加、ライセンスの有効化、詳細なTCPおよびWebトランザクションなどの他のワークフローを完了する。

> **注**
>
> 既存のエージェントを使用する場合、またはハイパーバイザーを使用してオンプレミスのNetScalerエージェントを構成する場合は、サービスグラフを設定するためにサービスグラフの設定の手順に従ってください。

1. **アプリケーション > サービスグラフ**に移動し、**マイクロサービス**タブを選択します。

   マイクロサービスクラスターが構成されていないことを確認できます。構成オプションをクリックします。

2. **カスタム展開**を選択します。
3. 展開タイプを選択します。
4. アプリケーションタイプとして**マイクロサービス**を選択します。
5. **次へ**をクリックしてエージェントを設定します。
6. **エージェントマイクロサービスのダウンロード**ページで、次のパラメータを指定します。

   a. **アプリケーション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。

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

b. **パスワード** – CPXがエージェントを介してNetScaler Consoleにオンボードするために使用するパスワードを指定します。

c. **パスワードの確認** – 確認のため、同じパスワードを指定します。

注

デフォルトのパスワード (`nsroot`) を使用してはなりません。

d. **Submit** をクリックします。

7. **Download YAML File** または **Download Helm Chart** をクリックします。
8. Kubernetesメインモードで、ダウンロードしたYAMLファイルを保存し、次のコマンドを実行してエージェントを登録します。

`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。

9. **Register Agent** をクリックします。

ページが数秒間読み込まれ、登録されたエージェントが表示されます。

10. エージェントがリストに存在することを確認し、**Next** をクリックします。

11. クラスターを登録する必要があります。「**Add More Clusters**」をクリックして、次のパラメーターを指定します。

a. **名前** - 任意の名前を指定します。

b. **APIサーバーURL** - KubernetesメインノードからAPIサーバーURLの詳細を取得できます。

i. Kubernetesメインノードで、コマンド `kubectl cluster-info` を実行します。

ii. 「**Kubernetes main is running at.**」に表示されるURLを入力します。

c. **認証トークン** - 認証トークンを指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信アクセスを検証するために必要です。認証トークンを生成するには：

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

Kubernetesメインノードで：

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。

iii. クラスターロールをサービスアカウントにバインドするには、`kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` を実行します。

サービスアカウントは、クラスター全体のアクセス権を持つようになりました。

サービスアカウントの作成中にトークンが自動的に生成されます。

iv. トークンを表示するには、`kubectl describe sa <name>` を実行します。

v. シークレット文字列を取得するには、`kubectl describe secret <token-name>` を実行します。

☐

12. リストからエージェントを選択します。
13. **作成** をクリックします。
14. **クラスター** ページにクラスター情報が表示されます。**次へ** をクリックします。

☐

15. CPX および VPX インスタンスを設定し、**次へ** をクリックします。

☐

16. 詳細な Web および TCP トランザクションを有効にするには、**次へ** をクリックします。

☐

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

17. 設定が完了しました。**サービスグラフ** を選択し、**完了** をクリックします。

サービスグラフは、約15分で入力されます。**アプリケーション > サービスグラフ** に移動し、**マイクロサービス** タブを選択してサービスグラフを表示します。

サービスグラフのセットアップ

ソフトウェア要件

KUBERNETESディストリビューション	KUBERNETESバージョン	コンテナネットワークインターフェース (CNI)	CPXバージョン	CICバージョン	エージェントバージョン	
オープンソース	v1.16.3	フラネル、カリコ、またはカナル	13.0–47.103以降	1.6.1以降	13.0–49.x以降	

Kubernetesクラスターは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されています
シングルティアまたは統合イングリッジ	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

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

NetScaler Consoleでサービスグラフの設定を完了するには、Kubernetesクラスター用に構成したトポロジタイプをクリックし、記載されている手順を完了してください。

- シングルティアまたは統合イングレストポロジ
- デュアルティアまたはサービスメッシュライトトポロジ
- サービスメッシュトポロジ

注

デュアルティアおよびサービスメッシュライトトポロジのサービスグラフ設定手順は同じです。

シングルティアまたは統合イングレストポロジ

シングルティアまたは統合イングレストポロジを設定するには、以下の手順を完了していることを確認してください。詳細については、「シングルティアまたは統合イングレストポロジを設定するための詳細な手順」を参照してください。

- シングルティアまたは統合イングレストトポロジでKubernetesクラスターを構成済みであること。
- NetScaler ConsoleにVPX、MPX、SDX、BLXインスタンスを追加し、**Web Insight**を有効にしていること。
- NetScaler ConsoleにKubernetesクラスターを追加済みであること。

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

デュアルティアまたはサービスメッシュライトトポロジを設定するには、以下の手順を完了していることを確認してください。詳細については、「デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順」を参照してください。

- サポートされているトポロジのいずれかでKubernetesクラスターを構成済みであること。
- agentをインストールし、NetScaler ConsoleとKubernetesクラスター、またはデータセンターやクラウド内のマネージドインスタンス間の通信を有効にするように設定しました。

  エージェントをマイクロサービスとして展開することもできます。詳細については、Getting Startedの**NetScalerエージェントのインストールセクション**を参照してください。
- NetScaler ConsoleとNetScaler CPX間の通信を有効にするために、エージェント上でStatic routesを設定しました。

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

> **注**
>
> 同じクラスターにエージェントをマイクロサービスとして展開している場合は、この手順を無視できます。

- 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しました。
- NetScaler ConsoleへのCPXの登録を成功させるために、CPX YAMLファイルに必要なパラメータを追加しました。
- NetScaler ConsoleにVPX、MPX、SDX、またはBLXインスタンスを追加しました。
- NetScaler ConsoleにKubernetesクラスターを追加しました。
- サンプルマイクロサービスアプリケーションを展開しました。
- NetScaler CPXを展開し、CPXをNetScaler Consoleに登録しました（2層アーキテクチャにのみ適用）。
- エージェントがHTTPおよびTCPトランザクションを取得できるように、WebトランザクションおよびTCPトランザクション設定を**すべて**に設定しました。
- マイクロサービスにトラフィックを送信しました。

サービスメッシュトポロジ

サービスメッシュトポロジを設定するには、以下の手順を完了していることを確認してください。詳細については、サービスメッシュトポロジ設定の詳細手順を参照してください。

- Kubernetesクラスターバージョン `1.14.0` を、以下のいずれかのサービスメッシュトポロジで構成済み:
  - IstioのサイドカープロキシとしてのNetScaler CPX
  - Istioのイングレスゲートウェイとしての NetScaler
- `admissionregistration.k8s.io/v1beta1` APIを有効にしました。APIは以下を使用して確認できます。

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  次の出力は、APIが有効になっていることを示しています。

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Istio `istio v.1.3.0` をインストール済み。
- Helm version 3.x をインストール済み。

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

- (/ja-jp/netscaler-console-service/getting-started.html#install-an-agent-as-a-microservice) をインストールし、NetScaler ConsoleとKubernetesクラスター、またはデータセンターやクラウド内の管理対象インスタンス間の通信を有効にするように構成済み。

  エージェントをマイクロサービスとして展開することもできます。詳細については、Getting Started の「**NetScalerエージェントのインストール**」セクションを参照してください。
- NetScaler ConsoleとNetScaler CPX間の通信を有効にするため、エージェント上で (/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#configure-static-routes-in-the-agent) を構成済み。

  注

  同じクラスターにNetScalerエージェントをマイクロサービスとして展開している場合は、この手順を無視できます。
- サービスメッシュトポロジデータを入力するために、 (/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#configure-the-required-parameters) を構成済み。
- サンプルアプリケーション(/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#deploy-a-sample-application)を展開しました。
- NetScaler Console に Kubernetes クラスター(/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#add-kubernetes-cluster-in-citrix-adm)を追加しました。
- 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(/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#enable-web-transaction-and-tcp-transaction-settings)を **すべて** に設定しました。
- マイクロサービスにトラフィック(/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/sg-service-mesh-topology.html#send-traffic-to-microservices)を送信しました。

必要なセットアップ手順を完了すると、**Applications** > **Service Graph** および **Microservices** タブに表示されるサービスグラフを確認できます。詳細については、「サービスグラフの詳細(/ja-jp/netscaler-console-service/application-analytics-and-management/service-graph/service-graph-begin-details.html)」を参照してください。

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

サービスグラフで詳細を表示

NetScaler Console に Kubernetes クラスターを追加した後、サービスグラフにデータが入力されるまで約 10 分かかります。**Applications** > **Service Graph** に移動し、**Microservices** タブをクリックして、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	単層/統合イングレストポロジ

- **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表示されます。

サービスグラフダッシュボード

1 - コンポーネントサービスがどのように通信しているかを示す、アプリケーションのエンドツーエンドネットワークマップ

2 – 特定の期間のヒット数とエラーを示すグラフ

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のフィルターを適用

6 – 設定アイコン

7 – ズームインおよびズームアウト表示

8 – グラフ表示または表形式表示

選択した期間に基づいて、サービスグラフを表示できます。

サービスアイコン	説明
サービスグラフのエッジ検出(/en-us/netscaler-console-service/media/servicegraph-edge-detection.png)	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。

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

サービスアイコン	説明
サービスグラフのエラー(/en-us/netscaler-console-service/media/servicegraph-errors.png)	警告アイコンが付いたサービスは、そのサービスにエラーがあることを示します。
サービスグラフの遅延(/en-us/netscaler-console-service/media/servicegraph-latency.png)	ストップウォッチアイコンが付いたサービスは、そのサービスに遅延または応答時間の問題があることを示します。
サービスグラフの遅延(/en-us/netscaler-console-service/media/servicegraph-latency-errors.png)	ストップウォッチアイコンと警告アイコンの両方が付いたサービスは、そのサービスにエラーと遅延/応答時間の両方の問題があることを示します。

注

サービスに警告アイコンまたはストップウォッチアイコンがない場合、そのサービスに異常があるか、ヒット数のしきい値を超えていることを示します。

ヒット数を示すグラフから期間を選択し、詳細情報をさらにドリルダウンします。

注

NetScaler Consoleでアクティブなトランザクションが受信されない場合、NetScalerインスタンスによって負荷分散されているサービスのみを表示できます。サービスにマウスポインターを合わせると、すべてのメトリックが0として表示されます。

サービスグラフに、サービスが使用するプロトコルが表示されるようになりました。イメージに示すように、Kubernetesクラスターで次のサービスが実行されているとします。

注

Infrastructure > Orchestration > Kubernetes > Clustersで複数のクラスターを追加している場合、各クラスターに関連付けられたサービスを表示できます。

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

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)** - サービスに複数のメトリックで異常またはしきい値違反があります。デフォルトのしきい値の場合、重大ステータスは平均サービス応答時間 > 200 ms かつエラー数 > 0 を示します。
- **レビュー (オレンジ)** - サービスにいずれかのメトリックで異常またはしきい値違反があります。デフォルトのしきい値の場合、レビュー状態は平均サービス応答時間 > 200 ms またはエラー数 > 0 を示します。
- **良好 (緑)** - 異常なし、またはしきい値違反なしのサービス。デフォルトのしきい値の場合、良好なステータスはエラーがなく、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。

  異常の詳細については、ゴールデンシグナルメトリックを使用したサービスの監視を参照してください。

  しきい値の詳細については、サービスグラフでのしきい値の構成を参照してください。

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は次のとおりです。

- **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HTTPプロトコル上のSSLを使用していることを示します。
- **SSL、TCP** – サービスがTCPプロトコル上のSSL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、次の情報を確認できます。

- 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

管理者として、これらの主要メトリックを使用すると、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。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。

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

サービス応答時間のPxx値を表示

サービスにマウスカーソルを合わせると、応答時間のPxx値が表示されます。

PXX値 (/en-us/netscaler-console-service/media/pxx-response-time.png)

応答時間 (P99) – 選択した期間の要求の99%がP99値未満であることを示します。

サービスの詳細を表示するためにドリルダウンすると、選択した期間の応答時間の99パーセンタイルと99.9パーセンタイルも表示できます。

99パーセンタイル (/en-us/netscaler-console-service/media/p99-response-time.png)

管理者として、pxx値を使用すると、サービス応答時間をよりよく理解できます。詳細については、「サービス詳細の表示」を参照してください。

サービス詳細の表示

サービスをクリックすると、次のオプションが表示されます。

サービス詳細オプション (/en-us/netscaler-console-service/media/sg-details.png)

- **詳細の表示** - サービスがホストされている名前空間、ラベル、クラスターなどのサービス詳細を表示できます。詳細については、「サービス詳細の表示」を参照してください。
- **アプリダッシュボードで表示** - アプリスコア、Kubernetesサービス詳細、Pod詳細など、選択したアプリケーション詳細を表示できます。詳細については、「Kubernetesアプリケーションの詳細」を参照してください。
- **トランザクションログ** - HTTPおよびSSL over HTTPトランザクションの詳細を表示できます。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。
- **トレース情報** - サービスの分散トレースを表示できます。詳細については、「分散トレース」を参照してください。

クライアントメトリクスの表示

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クスを視覚化し、クライアントから発生する問題を分析できます。

メトリクスを表示するには、クライアント領域にマウスポインターを合わせます。

クライアントメトリクス(/en-us/netscaler-console-service/media/client-metrics.png)

- **ヒット数** - クライアントが受信した合計ヒット数を示します。
- **クライアントネットワーク遅延** - 平均クライアントネットワーク遅延を示します。

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

- **クライアント4xxエラー** - 合計クライアント4xxエラーを示します。
- **クライアントSSLエラー** - 合計クライアントSSLエラーを示します。

NetScaler ConsoleのIPブロック - クライアントがパブリックIPアドレスを使用している場合、NetScaler Consoleはクライアントの場所を認識できます。NetScaler Consoleには、クライアントIPアドレス範囲に基づいて場所を照合する組み込みの場所CSVファイルがあります。

NetScaler Consoleは、IPアドレスがNetScaler Consoleサーバーに追加されている場合にのみ、プライベートIPアドレスを持つクライアントの場所を認識できます。たとえば、クライアントIPアドレスが都市Aに関連付けられたプライベートIPアドレス範囲内にある場合、NetScaler Consoleはこのクライアントのトラフィックが都市Aから発信されていると認識します。

クライアントトランザクションの概要を表示

詳細なクライアントトランザクションの概要では、以下を表示できます。

- 応答時間 > 500ミリ秒
- 5xxエラー

クライアントの場所をクリックし、**トランザクションログ**を選択します。

トランザクションログ(/en-us/netscaler-console-service/media/client-transaction-summary.png)

詳細については、Web transaction analyticsを参照してください。

イングレスメトリクスを表示

Kubernetesクラスターで使用されているイングレスのタイプを表示できます。

- 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

単一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。

イングレスをクリックして、詳細をさらにドリルダウンします。詳細については、View ingress details for troubleshooting issuesを参照してください。

TCPおよびSSLメトリクスを表示

TCPおよびSSLメトリクスを使用して、次のことができます。

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

- サービス間のTCP接続の詳細を表示
- 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
- 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
- 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

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の上にマウスポインターを合わせると、TCPメトリックが表示されます。

- **TCP接続** – サービス間で確立された合計接続数
- **データ量** – サービスによって処理された合計データ量
- **TCPサーバーリセット** – サーバーから開始された合計TCPリセット数

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** – サーバーからの合計SSLエラーを示します。(例: SSL証明書不明)
- **SSLプロトコル** – サービスによって使用されるSSLプロトコルバージョンを示します
- **SSLクライアントエラー** – クライアントからの合計SSLエラーを示します。(例: SSLクライアント認証エラー)

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、レイテンシーが150ミリ秒未満のサービスを表示したい場合は、**サービス応答時間**の下にある棒グラフをクリックして結果を表示します。

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できる場合があります。

すべてクリア をクリックして、すべてのフィルターをクリアします。

または、検索テキストボックスを使用してサービス名を入力し、サービスグラフに結果を表示することもできます。

設定オプション

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 – カテゴリに基づいてサービスを表示するには、リストからオプションを選択します。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-console-service/media/services-views.png)

4 – サービスをどのように表示するかを選択できます。

5 - アクティブなサービスのみを表示するには、**アイドルサービスを非表示**オプションを選択します。

6 - **サービス情報**ラベルを変更できます。**フィルター**タブでは、ラベル（選択した期間とサービスからのアクティブなトランザクションに基づいて）を選択できます。

フィルター(/en-us/netscaler-console-service/media/settings-filter.png)

ラベルを選択した後、**フィルター**セクションの**サービス情報**タブで、選択したラベルにフィルターを適用して結果を絞り込むことができます。

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。

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

エラー	説明
TCPエラー(/en-us/netscaler-console-service/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-console-service/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。
	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**の場合に、任意のサービスで表示されます。
- 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。

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

NetScaler Consoleでは、Ingressとサービス間のトランザクションの詳細も表示できます。マウスポインターを合わせると、Ingressとサービス間の合計エラー数、平均サービス応答時間などの詳細が表示されます。

ヒット数 – サービスが受信したヒットの総数を示します。

サービス応答時間 – サービスがTime To First Byte (TTFB) に応答するまでにかか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プロトコル – SSLプロトコルバージョンを示します。

Ingress と **サービス** 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する」を参照してください。

サービスグラフでしきい値を構成する

管理者として、Kubernetesサービスにしきい値を構成できます。NetScaler Consoleは、サービスの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を削除することはできません。

新しいしきい値を構成するには：

1. **アプリケーション > サービスグラフ**で、**マイクロサービス**タブをクリックします。
2. 設定アイコンをクリックし、**しきい値**タブを選択します。
3. **新しいしきい値**をクリックして、新しいしきい値を構成します。

   しきい値を構成する(/en-us/netscaler-console-service/media/sg-new-threshold.png)

   新しいしきい値ページが表示されます。
4. 次のパラメータを構成します。

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

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、以下に対して**単一**または**二重**を選択します。

- 高い応答時間（平均、P99、P99.9）
- 高エラー
- 高ヒット

d. しきい値の値を指定します。

> **注**
>
> 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。

5. **保存**をクリックします。

しきい値の設定(/en-us/netscaler-console-service/media/sg-configure-threshold.png)

しきい値が正常に作成されました。しきい値の詳細は、**しきい値**ページで確認できます。

> **注**
>
> NetScaler Consoleは、選択されたメトリックに基づいてサービスの最終スコアとステータスを計算します。たとえば、しきい値設定で**高ヒット**のみを選択した場合、NetScaler Consoleはデフォルトのしきい値（応答時間 = 200ミリ秒、エラー数 = 0）と高ヒットを使用してサービススコアとステータスを計算します。

単一しきい値

すべてのメトリックまたは選択したメトリックに対して単一しきい値を構成すると、NetScaler Consoleは次のようになります。

- 各メトリックの現在の値を、各メトリックで構成されたしきい値と比較します。
- 各メトリックで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。

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

注

いずれかのメトリックがしきい値を超えていない場合、ペナルティはそれに応じて計算されます。

- 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

すべてのメトリックまたは選択したメトリックに対して二重しきい値を構成すると、NetScaler Console は次のようになります。

- 各メトリックの現在の値を、各メトリックで構成されたしきい値と比較します。
- 現在の値が次のいずれかであるかを確認します。
  - しきい値 1 未満
  - しきい値 1 としきい値 2 の間
  - しきい値 2 より大きい
- 各メトリックで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。

注

いずれかのメトリックがしきい値を超えていない場合、ペナルティはそれに応じて計算されます。

- 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-console-service/media/sg-details.png)

サービス詳細ページでは、以下を表示できます。

- サービスがホストされているクラスター名 (1)
- サービスのネームスペースとサービスラベル (2) (4)
- 選択したサービスに接続されているすべての関連する受信および送信サービス (3)

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

- 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します。**異常のあるメトリック**タブでは、特定の期間の異常を表示できます (5)。

  詳細については、「ゴールデンシグナルメトリックを使用したサービスの監視」を参照してください。
- 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-console-service/media/sg-details-more.png)

これらの主要メトリックの傾向を使用して、特定の期間におけるサービスのパフォーマンスを分析できます。

たとえば、サービスがすべてのリクエストに対してサービス応答時間 > 700 ms を示しているとします。管理者として、次のことができます。

- 特定の期間のサービス応答時間メトリックの傾向を分析する
- 問題をトラブルシューティングする
- サービス応答時間メトリックを再度確認し、応答時間が改善されたかどうかを分析します。

メトリックの詳細

メトリック	説明
ヒット数	サービスが受信したリクエストの総数
エラー	サービスからのHTTPエラーの総数
サービス応答時間	サービスがTime To First Byte (TTFB)に応答するまでにかかった平均応答時間。
データ量	サービスによって処理されたデータ総量
SSLフロントエンドエラー	サービスからのSSLフロントエンドエラーの総数。例: SSL CLIENTAUTH FAILURE
SSLバックエンドエラー	サービスからのSSLバックエンドエラーの合計。例：SSLクライアントエラー
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

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

メトリック	説明
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-console-service/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

「今すぐポーリング」オプションを使用してPodのステータスを取得する

今すぐポーリングオプションは、クラスターから最新のPodステータスを取得します。

今すぐポーリング(/en-us/netscaler-console-service/media/sg-poll-now.png)

ゴールデンシグナルメトリクスを使用してサービスを監視する

Kubernetesクラスターで実行されているサービスにおけるゴールデンシグナルメトリックとは、特定の期間における潜在的な異常を検出できる一連のメトリックを指します。Kubernetesクラスターに100個ものマイクロサービスがある場合、頻繁に問題が発生するサービスを特定するのは難しいかもしれません。NetScaler ConsoleグラフがKubernetesサービスの潜在的な異常を特定するのに役立つ、以下の3つの主要なメトリックがゴールデンシグナルメトリックです。

- ヒット数
- 応答時間 (平均) および応答時間 (P99)
- エラー

管理者として、これらのメトリックを使用すると、次のことができます。

- サービスステータスを特定する
  - **クリティカル** – 複数のメトリックでサービスに異常またはしきい値違反がある
  - **レビュー** – いずれかのメトリックでサービスに異常またはしきい値違反がある
  - **良好** – 異常またはしきい値違反がないサービス
- 各メトリックでいくつの異常が特定されたかを分析する

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

- 問題をトラブルシューティングし、大きな影響を回避する

異常を特定する

サービスをクリックして**詳細の表示**を選択すると、サービス詳細ページにすべてのメトリックの概要が表示されます。**異常のあるメトリック**タブをクリックして、異常の詳細を表示します。

各メトリックについて、グラフでは、期待される範囲を超えたときに検出された異常を表示できます。オプションをクリックして、グラフのビューをフィルタリングできます。

「グラフをフィルタリング」(/en-us/netscaler-console-service/media/anomalies.gif)

サービス応答時間 (P99) の異常を分析したいとします。

応答時間の下に、選択した期間の以下の詳細が表示されます。

「メトリクス P99」(/en-us/netscaler-console-service/media/metrics-p99.png)

- **99パーセンタイル** – 選択した期間のリクエストの99%が60ミリ秒未満であることを示します。
- **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。
- **異常** – 検出された異常の合計数を示します。

このグラフでは、選択した期間の予想範囲も表示できます。例によると、以下が表示されます。

- 応答時間の予想範囲は1ミリ秒から9ミリ秒です。
- サービスで2つの異常が検出されました（1つは60ミリ秒、もう1つは25ミリ秒）。これは、サービスの応答時間が予想範囲（1ミリ秒から9ミリ秒）を超えているためです。

問題のトラブルシューティングのためにイングレスの詳細を表示する

サービスグラフで、イングレスをクリックし、**View Details** 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。

Instance Details をクリックして詳細を表示します。

次の詳細が表示されます。

- **情報** - インスタンスタイプ、デプロイタイプ、バージョン、モデルなどのインスタンスの詳細。

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

- **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。**Licensed Features** 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。**View Enabled Modes** 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 – 選択した期間における現在のNetScalerインスタンススコアを示します。最終スコアは**100から合計ペナルティを引いた値**として計算されます。グラフには、選択した期間のスコア範囲が表示されます。

  2 – NetScalerインスタンスの現在のステータス（**Up**、**Down**、**Out of Service**など）を示します。

  3 – NetScalerインスタンスが稼働している期間を示します。

  4 – インスタンスで有効および無効になっているネットワークインターフェイスの合計数を示します。クリックすると、ネットワークインターフェイス名やステータス（有効または無効）などの詳細が表示されます。

  5 – リストから期間を選択して、インスタンスの詳細を表示します。

  6 – NetScalerインスタンスの合計問題数と問題カテゴリを表示します。

- **主要メトリック**

  各タブをクリックして詳細を表示します。各メトリックでは、選択した期間の平均値と差分値を表示できます。

  次の画像はHTTPS Req/Secの例で、選択された期間は過去1か月です。値**692**は過去1か月のHTTPS Req/Secの平均値であり、値**20**は差分値です。グラフでは、最初の値が**139**で、最後の値が**119**です。差分値は**139 – 119 = 20**です。

  選択した期間のインスタンスメトリックをグラフ形式で表示できます。

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

- **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。
- **スループット** – 選択した期間におけるインスタンスによって処理された平均ネットワークスループット。
- **HTTPS request/sec** – 選択した期間にインスタンスが受信したHTTPSリクエストの平均。
- **TCP connections** – 選択した期間にクライアントとサーバーによって確立されたTCP接続の平均。
- **SSL transactions** – 選択した期間にインスタンスによって処理されたSSLトランザクションの平均。

- **問題**

  NetScalerインスタンスで発生する以下の問題を表示できます。

問題カテゴリ	説明	問題
システムリソース	CPU、メモリ、ディスク使用量など、NetScalerシステムリソースに関連するすべての問題を表示します。	- 高いCPU使用率
		- 高いメモリ使用率
		- 高いディスク使用率
		- SSLカード障害
		- 電源障害
		- ディスクエラー
		- フラッシュエラー
		- NIC破棄

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

問題カテゴリ	説明	問題
SSL設定	NetScalerインスタンス上のSSL設定に関連するすべての問題を表示します。	- SSL証明書の期限切れ
		- 推奨されない発行者
		- 推奨されないアルゴリズム
		- 推奨されない鍵強度
設定の逸脱	NetScalerインスタンスに適用された設定ジョブに関連するすべての問題を表示します。	- 設定ドリフト
		- 実行中とテンプレートの比較
キャパシティの問題	NetScalerのキャパシティの問題を表示します。NetScaler Consoleは、NetScalerインスタンスから5分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンターの増分が存在する場合に表示します。問題は、以下の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

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

問題カテゴリ	説明	問題
ネットワーキング	インスタンスで発生する運用上の問題を表示します。	詳細については、「新しいインジケーターによる強化されたインフラストラクチャ分析」を参照してください。

各タブをクリックして、問題を分析し、トラブルシューティングを行います。たとえば、選択した期間にインスタンスに次のエラーが発生したとします。

- **Current**タブには、インスタンススコアに影響を与えている現在のNetScalerの運用上の問題が表示されます。
- **All**タブには、選択した期間に検出されたすべてのインフラ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する。
- 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する。
- 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する。
- 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する。

前提条件

サービスに関するトレース情報を表示するには、次のことを行う必要があります。

- 東西トラフィックを送信する際に、アプリケーションが次のトレースヘッダーを維持していることを確認してください。
- **1.7.23より前のCICビルド**の場合、CPX YAMLファイルを`NS_DISTRIBUTED_TRACING`として、値を`yes`として更新します。
- **1.7.23より後のCICビルド**の場合、ConfigMapを使用する必要があります。

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

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できます。ConfigMapを使用すると、ワークロードの構成を簡単に変更および管理でき、ポッド仕様に構成データを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。

```
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
```

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

```
    endpoint:
      server: <AgentIP> / <AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        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 Console は、指定された数のトレーストランザクションを表示します。

b. ConfigMap をデプロイするには、以下を使用します。

`kubectl create -f <configmap-yaml>.yaml`

c. CPX YAML ファイルを編集し、`envFrom` または `args` のいずれかを使用して、次の引数を指定します。

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

```
envFrom:

 - configMapRef:

     name: cic-configmap
```

または

ConfigMap YAML 設定は CIC にデプロイされます。

d. いずれかの変数の値を変更する場合は、ConfigMap の値を編集します。この例では、他のすべての変数が `false` から `true` に変更されています。

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG: |

    distributed_tracing:

      enable: 'true'

      samplingrate: 100

    endpoint:
```

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

```
      server: <AgentIP> / <AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        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`

サービストレースの詳細を表示

サービスグラフでサービスをクリックし、**トレース情報**を選択します。

トレース情報(/en-us/netscaler-console-service/media/trace-info.png)

選択したサービスのトレース概要ページが表示されます。

トレース概要(/en-us/netscaler-console-service/media/trace-summary.png)

トレース概要には以下が表示されます。

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

- 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ヶ月、カスタム時間などの期間を選択できる期間リスト (2)。
- 特定の期間の結果を表示するためにドラッグして選択できるタイムライン詳細グラフ (3)。
- 各メトリックからオプションを選択できるフィルターパネル (4)。
- 選択したサービスのトランザクション詳細 (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。選択したサービスのトランザクション詳細を次のように表示できます。

- 開始時刻
- 終了時刻
- SSLメトリック
- 相互依存サービスとの通信（各サービスのエラーおよび応答時間を含む）。

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、**トレースの詳細を表示** をクリックしてください。

トレースの詳細(/en-us/netscaler-console-service/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-console-service/media/trace-transactions.png)

1 – トランザクションの開始時刻、応答時間、合計サービス数、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-console-service/media/trace-click-transaction.png)

`product-catalogue-service` と `catalogue-store-service` 間のトランザクション詳細では、HTTP応答が500であることが示されています。これらの詳細により、管理者として、エラー

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

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-console-service/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。
- **アプリケーション応答時間**：アプリケーションの平均応答時間
- **データ転送時間**：サービスとの間で転送が発生する可能性のあるデータ転送サイズとレート。
- **ロケーション**：クライアントのロケーション
- **ブラウザ**：クライアントが使用するブラウザの種類。例：Chrome、Firefox。
- **クライアントOS**：ブラウザのユーザーエージェントの詳細に基づくクライアントOS。
- **デバイス**：ブラウザのユーザーエージェントの詳細に基づくデバイス。例：タブレット、モバイル。
- **リクエストタイプ**：トランザクションのリクエストタイプ。例：GET。
- **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。
- **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**：高、中、低などのSSL証明書キーサイズに基づく暗号強度。
- **SSLキー強度**：SSL暗号強度は、SSL証明書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**：フロントエンドのSSLハンドシェイクエラーメッセージ。例：SSL CLIENTAUTH FAILURE

サービスグラフの部分的またはデータなしの診断詳細を表示

必要なサービスグラフの構成を完了し、NetScaler ConsoleにKubernetesクラスターを追加すると、サービスグラフにデータが入力され始めます。いくつかのシナリオでは、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場合があります。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

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

- 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仮想サーバーが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 Consoleで、**Applications** > **Service Graph** に移動し、**Microservices** タブをクリックします。

データなしの診断

サービスグラフにデータが表示されない場合、次の診断メッセージが表示されます。

> 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-console-service/media/more-details.png)

- **問題の種類** – 問題が構成、分析構成、またはライセンスから発生しているかどうかを示します。
- **メッセージ** – 問題の原因を示します。
- **アクション** – 問題のトラブルシューティングのために実行する必要があるアクションを示します。

部分的なデータに関する診断

サービスグラフが部分的なデータのみで表示される場合は、**診断の表示**ボタンをクリックして診断情報を表示します。

次の例は、TCPトランザクションが無効になっていることを示しています。

部分的なデータ(/en-us/netscaler-console-service/media/partial-data.png)

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

この例では、**設定 > 分析設定**に移動して、**TCPトランザクション設定**を**すべて**に有効にする必要があります。

トラブルシューティング

管理者として、これらの診断メッセージを使用して、これらの問題を検証し、トラブルシューティングを試みることができます。トラブルシューティング後、NetScaler Consoleは定期的に自動で診断チェックを実行します。診断チェックが完了すると、サービスグラフの部分的なデータまたはデータなしの問題が解決されます。

また、**診断の実行**をクリックし、**CPXインスタンス**を選択して、**診断の実行**をクリックすることもできます。

トラブルシューティング(/en-us/netscaler-console-service/media/troubleshooting.png)

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

3層Webアプリケーションのサービスグラフ

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。

アプリケーションビュー

アプリケーション構成の概要が表示されます。このビューでは、クライアント、NetScaler、Webアプリケーション間の通信を視覚化できます。

GSLBアプリケーションの場合、クライアント、データセンター、NetScaler、およびサービス間の通信を視覚化できます。

ネットワーク機能ビュー

アプリケーションに関連付けられている仮想サーバーを表示します。このビューでは、NetScalerが以下と通信しているかどうかを視覚化できます。

- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバー
- アプリケーションにアクセスするための負荷分散仮想サーバー
- アプリケーションにアクセスするためのコンテンツスイッチング仮想サーバーと負荷分散仮想サーバーの両方

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

GSLBアプリケーションの場合、データセンターとNetScalerとともに詳細が表示されます。

アクティブなトランザクションがない場合のサービスグラフビュー

NetScalerとWebアプリケーション間でアクティブなトランザクションが発生しない場合、サービスグラフはアプリケーションの基本構成のみを表示します（クライアントとNetScalerなし）。

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。

メトリックの分析

各サービスにマウスポインターを合わせると、**アプリケーションビュー**または**ネットワーク機能ビュー**でメトリックの詳細を表示できます。

クライアントメトリクス

クライアントにマウスポインターを合わせると、クライアントメトリクスが表示されます。

クライアントメトリクス(/en-us/netscaler-console-service/media/ga-sg-clientmetrics.png)

- **ヒット数** - クライアントが受信したリクエストの合計。
- **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。
- **データ量** - クライアントによって処理されたデータの合計を示します。

ネットワーク機能メトリクス

ロードバランシングまたはコンテンツスイッチングサービスにマウスポインターを合わせると、メトリクスの詳細が表示されます。

ネットワーク機能メトリクス(/en-us/netscaler-console-service/media/network-function-metric-now.png)

- **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。
- **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。

© 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。

サービスメトリクス

サービス（Webアプリケーション）にマウスポインターを合わせると、メトリクスが表示されます。

サービスメトリクス(/en-us/netscaler-console-service/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)

NetScalerにマウスポインターを合わせると、メトリックが表示されます。

- ホスト名と現在のNetScaler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
- **NetScaler処理時間** – NetScalerインスタンスによる平均処理時間を示します

注

NetScalerにホスト名が割り当てられていない場合:

- ホスト名の代わりにNetScalerのIPアドレスが表示されます。
- メトリックには、NetScalerのIPアドレス情報は表示されません。

© 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

アプリケーション > **サービスグラフ** に移動し、**グローバル** をクリックします。

グローバルサービスグラフ(/en-us/netscaler-console-service/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ディスクリートアプリケーション

> **注**
>
> NetScalerインスタンスにディスクリートアプリケーションがない場合、NetScalerインスタンスからディスクリート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ックの表示

クライアントリージョンにマウスカーソルを合わせると、メトリックを表示できます。

クライアントメトリック(/en-us/netscaler-console-service/media/ga-sg-clientmetrics.png)

- **ヒット数** - クライアントが受信した合計リクエスト数。
- **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。
- **データ量** - クライアントによって処理された合計データ量を示します。

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、そのデータセンターにグループ化されたNetScalerインスタンスの合計数

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

- 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

  インスタンスグループ(/en-us/netscaler-console-service/media/adc-group.png)

その他のNetScalerインスタンス をクリックして、それぞれのステータス（Critical、Review、Good、Not Applicable）タブを選択し、すべてのNetScalerインスタンスを表示します。

その他のインスタンス(/en-us/netscaler-console-service/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。

インスタンスの詳細(/en-us/netscaler-console-service/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（Up、down、out-of-serviceなど）を示します。
- **最大寄与** – 現在のNetScalerスコアに影響を与える主要な問題を示します。
- **SSLの問題** – NetScalerインスタンスからのSSL問題の総数を示します。エラー数をクリックしてドリルダウンし、SSLエラーの詳細を表示します。

NetScalerインスタンスをクリックすると、インスタンススコア、主要メトリック、NetScalerインスタンスに関連する問題などのインスタンス詳細が表示されます。詳細については、「Infrastructure Analyticsでインスタンスの詳細を表示する」を参照してください。

個別のアプリケーションを表示

サービスグラフには、スコアの低い上位4つの個別のアプリケーションが表示されます。

次の個別のアプリケーションがあるとします。

アプリ名	NETSCALER	アプリスコア	アプリステータス
App1	10.102.29.50	35 (クリティカル)	稼働中
App2	10.102.29.90	100 (良好)	ダウン
App 3	10.102.32.40	49 (レビュー)	アップ

© 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
App4	10.102.113.208	92 (良好)	ダウン
App5	10.102.25.25	86 (良好)	稼働中
App6	10.102.29.41	77 (良好)	稼働中
App7	10.102.29.102	41 (要確認)	稼働中

このシナリオでは、App1、App3、App6、App7 をサービスグラフ内のスコアが低い上位 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**および**マイクロサービス**アプリケーションについても、スコアが低い上位 4 つのアプリケーションを表示できます。

サービスにマウスポインターを合わせると、メトリック情報が表示されます。

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** – アプリケーションの現在のステータス（稼働中または停止中など）を示します
- **問題** – アプリケーションに適用される問題の総数を示します
- **上位の問題** – アプリケーション全体のスコアに影響を与える上位の問題を示します

その他をクリックして、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。

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
- **重大** – アプリのスコアが0～40未満
- **レビュー** – アプリのスコアが40～75未満
- **良好** – アプリのスコアが75より大きい
- **該当なし** – アプリがどの仮想サーバーにもバインドされていない

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.

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。メトリックの詳細を表示するには、サービスにマウスポインターを合わせます。

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総数
- **サービス応答時間** – サービスから取得された平均応答時間。

  （応答時間 = クライアントRTT + リクエストの最終バイト – リクエストの最初のバイト）
- **エラー** – 4xx、5xxなどのエラーの総数
- **データ量** – サービスによって処理されたデータの総量
- **名前空間** – サービスの名前空間
- **クラスター名** – サービスがホストされているクラスター名
- **SSLサーバーエラー** – サービスからのSSLエラーの総数

サービスをクリックすると、選択したサービスのKubernetesサービスグラフが、サービスの名前空間とクラスター名のフィルターが適用された状態で表示されます。

Kubernetesサービス(/en-us/netscaler-console-service/media/k8s-service.png)

詳細をクリックして、すべてのサービスを含むKubernetesサービスグラフを表示します。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-console-service/media/k8s-all.png)

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、次のような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。

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

- 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-console-service/media/search-bar-gsg.png)

たとえば、特定のNetScalerインスタンスを表示したい場合は、検索バーから**インスタンス**を選択し、インスタンスのIPアドレスを選択します。グローバルサービスグラフには、選択したインスタンスとそれに関連するアプリケーション、データセンター、クライアントの場所が表示されます。

検索結果(/en-us/netscaler-console-service/media/search-results-gsg.png)

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

StyleBooks

StyleBooksは、アプリケーションの複雑なNetScaler構成を管理するタスクを簡素化します。StyleBookは、NetScaler構成を作成および管理するために使用できるテンプレートです。

StyleBookを使用すると、次のことができます。

- NetScalerの特定の機能を構成する。
- 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。

StyleBooksは、DevOpsチームが実践するInfrastructure-as-codeの原則によく適合し、構成は宣言的でバージョン管理されています。構成は繰り返し使用され、全体として展開されます。StyleBooksには次の利点があります。

- **宣言的**: StyleBooksは、命令型ではなく宣言型の構文で記述されます。StyleBooksを使用すると、特定のNetScalerインスタンスで構成を実現するための段階的な手順ではなく、構成の結果または「望ましい状態」を記述することに集中できます。NetScaler Consoleは、NetScaler上の既存の状態と指定した望ましい状態との差分を計算し、インフラストラクチャに必要な編集を行います。StyleBooksはYAMLで記述された宣言型構文を使用するため、StyleBookのコンポーネントは任意の順序で指定でき、NetScaler Consoleは計算された依存関係に基づいて正しい順序を決定します。
- **アトミック**: StyleBooksを使用して構成を展開する場合、完全な構成が展開されるか、まったく展開されないかのいずれかであり、これによりインフラストラクチャは常に一貫した状態に保たれます。
- **バージョン管理**: StyleBookには、システム内の他のStyleBookと一意に区別する名前、名前空間、およびバージョン番号があります。StyleBookを変更するには、この一意性を維持するためにバージョン番号（または名前または名前空間）の更新が必要です。バージョン更新により、同じStyleBookの複数のバージョンを維持することもできます。
- **構成可能**: StyleBookが定義されると、そのStyleBookは他のStyleBookを構築するための単位として使用できます。構成の一般的なパターンを繰り返すことを避けることができます。また、組織内で標準的な構成要素を確立することもできます。StyleBooksはバージョン管理されているため、既存のStyleBooksへの変更は新しいStyleBooksを生み出し、その結果、依存するStyleBooksが意図せずに破損することはありません。

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

- **アプリケーション中心**: StyleBooksは、完全なアプリケーションのNetScaler構成を定義するために使用できます。アプリケーションの構成は、パラメータを使用することで抽象化できます。したがって、StyleBookから構成を作成するユーザーは、いくつかのパラメータを入力するだけで、複雑なNetScaler構成を作成できるシンプルなインターフェイスを操作できます。StyleBooksから作成された構成は、インフラストラクチャに縛られません。したがって、単一の構成を1つまたは複数のNetScalerインスタンスに展開したり、インスタンス間で移動したりできます。
- **自動生成UI**: NetScaler Console GUIを使用して構成を行う際、NetScaler ConsoleはStyleBookのパラメータを入力するためのUIフォームを自動生成します。StyleBookの作成者は、新しいGUI言語を学習したり、UIページやフォームを個別に作成したりする必要はありません。
- **API駆動**: すべての構成操作は、NetScaler Console GUIまたはREST APIを使用してサポートされます。APIは同期モードまたは非同期モードで使用できます。構成タスクに加えて、StyleBooks APIを使用すると、実行時に任意のStyleBookのスキーマ（パラメータ記述）を検出することもできます。

1つのStyleBookを使用して、複数の構成を作成できます。各構成はconfig packとして保存されます。たとえば、一般的なHTTPロードバランシングアプリケーション構成を定義するStyleBookがあるとします。ロードバランシングエンティティの値を持つ構成を作成し、NetScalerインスタンスで実行できます。この構成はconfig packとして保存されます。同じStyleBookを使用して、異なる値を持つ別の構成を作成し、同じインスタンスまたは異なるインスタンスで実行できます。この構成のために新しいconfig packが作成されます。config packは、NetScaler Consoleと、構成が実行される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ために、NetScaler Consoleに付属のデフォルトのStyleBooksを使用することも、独自のStyleBooksを設計してNetScaler Consoleにインポートすることもできます。StyleBooksを使用して構成を作成するには、NetScaler Console GUIを使用するか、APIを使用します。

このドキュメントには、次のセクションが含まれています。

- 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
- カスタムStyleBook
- スタイルブックのAPI
- StyleBookの文法

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

StyleBookのカテゴリ

NetScaler Consoleには、デフォルトとカスタムの2つのStyleBookカテゴリがあります。これらはパブリックまたはプライベートのいずれかになります。NetScaler Consoleでは、システムに存在するすべてのStyleBookと、それらがどのように相互に接続されているかを表示できます。

このドキュメントでは、さまざまな種類のStyleBookと、NetScaler ConsoleからStyleBookに対して実行できる次のアクションについて説明します。

- 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に基づいて新しいStyleBookを作成します。
- NetScaler ConsoleのデフォルトStyleBookを非表示にします。
- NetScaler Consoleからカスタム StyleBookを削除します。
- StyleBookにタグを追加します。

デフォルトStyleBookとカスタムStyleBook

- **デフォルトStyleBook**は、NetScaler Consoleに付属しているStyleBookであり、NetScalerインスタンスに展開できる構成を作成できます。デフォルトStyleBookを削除することはできませんが、NetScaler Console GUIから非表示にすることはできます。
- **カスタムStyleBook**は、NetScaler Consoleにインポートした独自のStyleBookです。

デフォルトStyleBookとカスタムStyleBookはどちらも、パブリックまたはプライベートのいずれかになります。

パブリックStyleBookとプライベートStyleBook

設定パックを作成できるStyleBookは、**パブリック**StyleBookとして分類できます。つまり、NetScaler Console GUIおよびAPIから構成を作成するために、すべて直接使用できます。

しかし、一部のStyleBookは、他のStyleBookの構成要素として使用されます。このようなStyleBookは**プライベート**としてマークされます。プライベートStyleBookは、NetScaler Console GUIから設定パックを直接作成するために使用することはできません。ただし、これらのStyleBookをNetScaler Consoleに表示して確認することはできます。カスタムStyleBookのいずれかを**プライベート**としてマークするには、StyleBookのプライベート属性を**true**に設定します。プライベートStyleBookは、NetScaler Console APIを使用して設定パックを作成するために引き続き使用できます。

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

プライベートとしてマークされたStyleBookの例

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

private: true
```

StyleBookの表示

NetScaler Consoleでは、デフォルトとプライベートの両方のStyleBookの数が増加しています。アクセスしたい特定のStyleBookを検索したい場合があります。また、両方の種類のStyleBookを個別に表示したい場合もあります。

NetScaler Consoleで、**Applications > Configuration > 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。

デフォルトのパブリックStyleBook(/en-us/netscaler-console-service/media/mas-stylebooks-default-and-public-icon.png)

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。

プライベートアイコン(/en-us/netscaler-console-service/media/mas-stylebooks-default-and-private-icon.png)

プライベートStyleBookの定義と依存関係を表示することはできますが、GUIを使用してプライベートStyleBookから設定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

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

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、共通の設定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。

デフォルトのパブリックアイコン(/en-us/netscaler-console-service/media/mas-stylebooks-default-and-custom-icon.png)

カスタムのプライベートStyleBookには、このアイコンが表示されます。

デフォルトのプライベートアイコン(/en-us/netscaler-console-service/media/mas-stylebooks-private-and-custom-icon.png)

ページの右上には、表示するStyleBookの種類を選択するオプションがあります。オプションは「すべて」、「パブリック」、「プライベート」の3つです。いずれかのオプションをクリックします。

パブリックとプライベートでStyleBookをフィルタリング(/en-us/netscaler-console-service/media/nmas-stylebooks-sorting-icon-new.png)

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。

StyleBookを検索(/en-us/netscaler-console-service/media/nmas-stylebooks-searching-icon-new.png)

カスタムStyleBookをダウンロード

NetScaler ConsoleからカスタムStyleBookをダウンロードするには、**Applications > Configuration > Confg Packs**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する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。

StyleBookをダウンロード(/en-us/netscaler-console-service/media/mas-download-custom-stylebooks-new.png)

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

注

NetScaler Console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。そのためには、StyleBookパネルの**View Definition**および**View Dependencies**リンクをクリックします。

カスタムStyleBookを更新

NetScaler Console GUIからカスタムStyleBookの定義を更新できます。そのため、バージョンを変更せずにStyleBookを変更できます。StyleBookバンドルからインポートされた定義を更新することもできます。

重要

NetScaler Console GUIからStyleBook定義を更新する前に、StyleBook定義に依存するStyleBookがないことを確認してください。

設定パックを持つStyleBook定義を更新できます。StyleBook定義が下位互換性があることを確認してください。そのため、すべてのパラメータは更新されたStyleBookに保持され、新しく追加されたパラメータはオプションとして表示されます。

1. **Applications > Configuration > StyleBooks**に移動します。
2. **Custom StyleBooks**タブを選択します。
3. 更新するStyleBookで**定義を更新**を選択します。
4. 必要に応じて定義を更新し、**更新**をクリックします。

5. ページを更新して、最新の変更を確認します。

カスタムStyleBookを削除する

削除ボタンをクリックして、カスタムStyleBookを削除することもできます。ポップアップウィンドウが表示され、NetScaler ConsoleからStyleBookを削除するかどうかを確認するメッセージが表示されます。StyleBookが他のカスタムStyleBookを使用している場合は、チェックボックスをオンにして、それらのStyleBookを削除することを選択できます。

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

注：

NetScaler Consoleに依存するStyleBookがある場合は、カスタムStyleBookを削除しないでください。この操作により、既存のStyleBookが破損する可能性があります。

StyleBookの依存関係を表示する

StyleBookの重要かつ強力な機能の1つは、他のStyleBookの構成要素として使用できることです。

次のことができます。

- **StyleBookを別のStyleBookにインポートする** - インポートされたStyleBookはタイプとして宣言され、2番目のStyleBookのコンポーネントまたはパラメータによって使用されます。NetScaler Consoleの既存のデフォルトStyleBookを表示して、StyleBookが別のStyleBookの上にどのように構築できるかを確認してください。
- **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する** - この表現は、他のStyleBookを構成要素として使用して構築された複雑なStyleBookに役立ちます。依存関係グラフを使用すると、StyleBook間の関係と依存関係を確認できます。

注：

他のStyleBookで使用されているStyleBookは、既存のStyleBookを破損させる可能性があるため、削除できません。依存関係グラフ表示を使用して、どのStyleBookがStyleBookの削除を妨げているかを特定します。

StyleBookの依存関係を表示するには

NetScaler Consoleで、**Applications > Configuration > StyleBooks** に移動します。StyleBooksページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして目的のStyleBookを見つけます。**View Dependencies** をクリックして、依存するStyleBookを表示します。

順方向の依存関係

Forward Dependencies タブでは、お使いのStyleBookが使用しているさまざまなデフォルトのStyleBookを表示できます。矢印をたどって、StyleBookが使用しているStyleBookを見つけます。いずれかの矢印にマウスを合わせると、その矢印と相互に接続されているStyleBookが強調表示されます。StyleBook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.

順方向の依存関係(/en-us/netscaler-console-service/media/nmas-stylebooks-forward-dependencies.png)

逆方向の依存関係

Reverse Dependencies タブでは、お使いのStyleBookを使用しているStyleBookをグラフィカルに表示できます。矢印をたどると、表示されているすべてのStyleBookがお使いのStyleBookを指していることがわかります。一部のStyleBookは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。

逆方向の依存関係(/en-us/netscaler-console-service/media/nmas-stylebooks-reverse-dependencies.png)

設定パックに対するNetScaler構成の監査

StyleBook設定パックによって行われた変更を現在のNetScaler構成と比較できます。この比較により、次のことができます。

- StyleBook設定パックとNetScaler構成間の設定ドリフトを検出します。
- 設定パックによって行われた変更が表示されない、NetScaler上の変更済みおよび削除済みオブジェクトを特定します。

設定パックの変更をNetScalerインスタンス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 > 構成 > 設定パック** に移動します。
2. 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。

注記：

NetScalerインスタンスに展開されているStyleBook構成パックを更新する際、展開された状態と異なる場合があります。その場合、構成パックの更新は失敗します。StyleBookエンジンは、これらの差異を自動的に調整し、構成パックを更新します。

構成パックのサポートバンドルをダウンロードする

構成パックのサポートバンドルは、Citrixテクニカルサポートチームが構成パックの問題を表示、分析、トラブルシューティングするのに役立ちます。サポートバンドルをダウンロードするには、次の手順を実行します。

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

1. **> >** の順に移動します。
2. サポートバンドルをダウンロードする構成パックを選択します。
3. で、 をクリックします。

   バンドルはZipまたはTGZファイル形式で圧縮できます。
4. オプションで、バンドルファイルを暗号化するためのパスフレーズを指定します。
5. をクリックします。

StyleBookのタグを作成する

NetScaler Consoleの任意のStyleBookにタグを追加できます。タグは、さまざまな基準を使用してStyleBookをグループ化できるキーと値のペアです。NetScaler ConsoleでStyleBookを検索またはフィルタリングする際に、これらのタグを使用できます。

StyleBookにタグを追加するには：

1. **Applications > Configuration > StyleBooks**に移動します。
2. タグを追加したいStyleBookで、**Tags**を選択します。

   StyleBookのタグ(/en-us/netscaler-console-service/media/adm-tags-stylebooks-new.png)

   すべての種類のStyleBookにタグを追加できます。
3. StyleBookのフィルタリングに役立つ、必要な**Key**と**Value**情報を指定します。

   例：キー=team、値=bizdata

   StyleBookのタグを作成する(/en-us/netscaler-console-service/media/adm-create-tags-stylebook.png)

   さらにタグを追加するには、**+**をクリックします。
4. **Create**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**Tags**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-console-service/media/use-tags-stylebook.png)

以下は、タグを持つStyleBookの検索例です。`key=team`および`value=bizdata`：

タグの例(/en-us/netscaler-console-service/media/example-adm-tag.png)

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

StyleBookタグをその設定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設定パックを検索できます。

設定パックを作成する際は、**タグの関連付け**セクションで以下のいずれかのオプションを使用します。

- **現在および将来のすべてのStyleBookタグを設定に関連付ける** – このオプションは、すべてのStyleBookタグを設定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確実に自動的に関連付けます。
- **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、設定パックに関連付けることができます。

StyleBookタグを設定パックに関連付ける(/en-us/netscaler-console-service/media/associate-tags-stylebook-configuration-pack.png)

StyleBookをクローンする

管理者は、StyleBookとその依存StyleBookの複製を作成できます。その後、このバンドルを`parameters`および`components`セクションの更新などのカスタマイズに使用できます。

StyleBookをクローンするには：

1. **アプリケーション > 設定 > StyleBooks**に移動します。
2. 複製したいデフォルトまたはカスタムのStyleBookで、**クローン**を選択します。

   StyleBookをクローンする(/en-us/netscaler-console-service/media/clone-stylebook.png)
3. **StyleBookのクローン**ページで、StyleBookおよび依存StyleBookのネームスペースとバージョンを入力します。推奨されるネームスペースとバージョンを選択することもできます。

   StyleBookをクローンする(/en-us/netscaler-console-service/media/clone-stylebook-dependencies.png)

   注：

   クローンされたStyleBookとその依存StyleBookは、既存のStyleBookと区別するために異なるネームスペースとバージョンを持つ必要があります。クローンされたStyleBookには、予約済みのNetScaler Consoleネームスペースを使用することはできません。
4. **クローン**」をクリックします。クローンされたStyleBookパッケージがNetScaler Consoleにインポートされ、「**StyleBooks**」ページに表示されます。

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

外部リポジトリからStyleBookをインポートして同期する

開発にCI/CDプロセスを使用しているシナリオ、またはすべてのアプリケーションソースコードとデプロイメントアーティファクトをGitHub/GitLabで管理しているシナリオを考えてみましょう。

GitHub/GitLabリポジトリでは、NetScaler構成をデプロイし、これらのStyleBookを管理するために、いくつかのStyleBookを保守している場合があります。これらのStyleBookをNetScaler Consoleにアップロードする必要があります。この機能を使用すると、GitHub/GitLabにあるStyleBookをNetScaler Consoleに直接インポートできます。GitHub/GitLabから手動でコピーしてNetScaler Consoleにアップロードしたり、NetScaler ConsoleとGitHub/GitLabの両方でファイルを手動で同期したりする必要はありません。また、GitHub/GitLabから構成パックをインポートして同期することもできます。

StyleBookと構成パックをインポートするには、NetScaler ConsoleでGitHub/GitLabリポジトリを表すリポジトリを定義します。GitHub/GitLabリポジトリのURLと、GitHub/GitLabで作成したユーザー名およびAPIまたは個人アクセストークン（PAトークン）を指定します。つまり、GitHub/GitLabで有効なアカウントを持つ承認されたユーザーのみがStyleBookをインポートおよび同期できます。

次の種類のリポジトリをインポートおよび同期できます。

- **公開アクセス可能なリポジトリ** - 一般に公開されており、インターネット経由でアクセスできるリポジトリ。
- **オンプレミスまたはプライベートなGitLab/GitHubリポジトリ** - プライベートにホストされており、通常は企業のイントラネット内でのみアクセスできるリポジトリ。これらのリポジトリの場合、登録プロセス中にNetScalerエージェントを選択する必要があります。NetScalerエージェントは、企業のイントラネット内のリポジトリにアクセスするためのプロキシとして機能します。

リポジトリを作成した後、NetScaler ConsoleをGitHub/GitLabリポジトリと同期できます。NetScaler ConsoleはGitHub/GitLabに接続し、そのリポジトリで見つかったStyleBookと構成パックをインポートします。その後、NetScaler ConsoleはStyleBookを検証し、NetScaler ConsoleのStyleBookリストに追加します。検証に失敗したStyleBookはNetScaler Consoleに追加されません。StyleBookのエラーを特定して修正できます。その後、更新されたバージョンをGitHub/GitLabリポジトリにコミットします。後で、それらをNetScaler Consoleに再度インポートまたは同期を試すことができます。

リポジトリの作成中に次のエラーが発生した場合、それは、NetScaler Consoleが、不足しているまたは認識されていない認証局（CA）証明書のために、リポジトリのSSL証明書を検証できないことを示しています。

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

`certificate verify failed: unable to get local issuer certificate`

この問題を解決するには、リポジトリへのアクセスに使用されるNetScaler Consoleエージェントに、必要なCA証明書を手動で追加できます。必要なCA証明書を追加することで、外部リポジトリへの安全な接続が適切に検証されるようになります。

リポジトリへのアクセスに使用されるNetScaler Consoleエージェントにログインし、CA証明書を信頼された証明書バンドル`/var/mps/ca_certs/cacert.pem`に追加します。

重要

- StyleBookファイルは、GitHub/GitLabリポジトリの任意のブランチからインポートおよび同期できます。
- 依存するStyleBookが関連付けられているStyleBookもインポートおよび同期できます。これらの依存StyleBookは、GitHub/GitLabリポジトリにあるか、すでにNetScaler Consoleに存在している可能性があります。
- GitHub/GitLabリポジトリからのStyleBookの同期は、NetScaler Consoleの管理画面またはAPIから手動で開始する必要があります。つまり、現在、StyleBookの取り込みと同期は、GitHub/GitLab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。
- インポートする構成パックファイルはJSON形式である必要があります。また、構成ファイルの内容はエクスポートされた構成形式に従う必要があります。GitHub/GitLabリポジトリでは、構成パックに関連付けられたファイルは`configpacks`フォルダーにある必要があります。

GitHub/GitLabリポジトリの任意のフォルダーからNetScaler ConsoleにStyleBookファイルをインポートできます。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. ルートディレクトリの下に`configpacks`という名前のフォルダーを作成します。構成に関連するすべてのファイルがこのフォルダーにあることを確認してください。
2. `configpacks`フォルダーに、構成パックのペイロードを含むJSONファイルを作成します。このペイロードは、構成パックを同期するために使用されます。以下はペイロードの例です。

```
{

    "config_key": "unique-key-for-configpack",
```

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

```
    "parameters": {
        "param-name1": "param-value1",
        "param-name": "param-value2",
        "param-namen": "param-valuen"
    },
    "stylebook": {
        "namespace": "some namespace",
        "name": "somename",
        "version": "spme-version"
    }
}
```

- `config_key` - NetScaler Consoleで構成パックを識別するための一意のIDまたは名前。config_keyを指定しない場合、NetScaler Consoleは構成パックの作成時にIDを自動生成します。

  指定されたIDがNetScaler Console GUIで見つかった場合、同期アクションはNetScaler Console GUIの構成パックを更新します。それ以外の場合は、指定されたIDで構成パックを作成します。
- `parameters` - 構成パックを作成または更新するために必要なすべてのパラメーターが含まれています。
- `stylebook` - JSONファイル内の必須プロパティです。構成パックを関連付けたい名前空間、バージョン、およびStyleBook名が含まれています。

3. `configpacks`フォルダーには、証明書、署名ファイル、XMLファイルなど、構成パックに関連するすべてのファイルを保持します。

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

リポジトリを追加

1. NetScaler Consoleで、**Applications > Configuration > Repositories** に移動します。**Add** をクリックします。
2. **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/GitLabのリポジトリ名と同じでも、異なるものでも構いません。
   - **リポジトリURL** - GitHub/GitLabリポジトリのURLを入力します。

     GitHub/GitLabエンタープライズURLを指定できます。これにより、GitHub/GitLabエンタープライズアカウントからStyleBookとconfig packをインポートまたは同期できます。
   - **プライベートURLですか？** - リポジトリがオンプレミスまたはプライベートのGitLab/GitHubリポジトリである場合は、このチェックボックスをオンにしてから、**エージェント** を選択します。
   - **ユーザー名** - GitHub/GitLabアカウントまたはエンタープライズアカウントへのアクセスに使用するユーザー名を入力します。
   - **API/PAトークン** - このトークンは、GitHub/GitLabリポジトリにアクセスするために使用されます。GitHub/GitLabリポジトリのAPI/PAトークンの作成方法については、個人アクセストークンの作成に関するGitHub/GitLabドキュメントを参照してください。

   GitHubリポジトリを追加(/en-us/netscaler-console-service/media/stylebooks-git-import-1.png)

   GitLabリポジトリを追加(/en-us/netscaler-console-service/media/stylebooks-gitlab-import.png)
3. **作成**をクリックします。

   リポジトリがNetScaler Consoleに作成されます。

リポジトリオプション

リポジトリの追加オプ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、APIトークンを編集できます。
- **削除** - そのGitHub/GitLabリポジトリから以前にインポートされた、NetScaler Consoleに存在するすべてのStyleBookとともにリポジトリを削除できます。

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

注

関連付けられたconfig packを持つStyleBookがある場合、NetScaler Consoleからリポジトリを削除することはできません。まず、これらのStyleBookのすべてのconfig packを削除します。その後、NetScaler Consoleからリポジトリを削除して、そのリポジトリからStyleBookをクリーンアップできます。

- **リセット** - リポジトリエントリを実際に削除することなく、そのリポジトリから同期されたNetScaler Console内のすべてのStyleBookを削除できます。
- **ファイルの一覧表示** - GitHub/GitLabリポジトリから取得された、NetScaler Consoleに存在するすべてのStyleBookのリストを表示できます。

GitHub/GitLabからStyleBookと設定パックをインポートする手順

前提条件を完了したら、GitHub/GitLabリポジトリからStyleBookと設定パックをインポートする手順に従ってください。

1. オプション：まだ追加していない場合は、リポジトリを追加します。
2. **リポジトリ**ページでリポジトリを選択します。
3. **同期**をクリックします。

デフォルトのStyleBookを使用する

NetScaler Consoleには、一連のデフォルトのStyleBookが用意されています。デフォルトのStyleBookを使用する場合は、StyleBook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 Console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、インスタンスで構成を実行します。

NetScalerの機能

この表は、負荷分散、コンテンツスイッチング、およびGSLBの仮想サーバーを構成するのに役立つStyleBookを示しています。

スタイルブック名	説明	バージョン
`lb`	シンプルな負荷分散仮想サーバーを構成します。「[負荷分散]」を参照してください。(/	1.1, 2.0

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

スタイルブック名	説明	バージョン
	ja-jp/citrix-adc/current-release/load-balancing.html).	
`lb-mon`	モニター付きの負荷分散仮想サーバーを構成します。「[負荷分散設定でモニターを構成する]」を参照してください。(/ja-jp/citrix-adc/current-release/load-balancing/load-balancing-configure-monitors.html).	1.0, 2.0
`cs-lb-mon`	モニター付きのコンテンツスイッチング仮想サーバーを構成します。詳細については、「[コンテンツスイッチング]」を参照してください。(/ja-jp/citrix-adc/current-release/content-switching.html).	1.0, 1.1
`lb-mon-full`	NetScalerインスタンスでモニター付きの負荷分散仮想サーバーを構成します。また、rewrite、responder、compression、SSL暗号などのNetScaler機能を構成します。	1.0
`cs-lb-mon-full`	NetScalerインスタンスでモニター付きのコンテンツスイッチング仮想サーバーを構成します。また、rewrite、responder、compressionなどのNetScaler機能を構成します。	1.0
`gslb`	GSLBセットアップで、異なるサイトのNetScalerインスタンスを1つ以上構成します。開始する前に、NetScalerインスタンスでSNIP IPアド	1.0

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

スタイルブック名	説明	バージョン
	レスを構成します。このStyleBookは、SNIP IPアドレスをサイトIPアドレスとして使用します。	
`multicloud-glb`	NetScalerインスタンスのGLBを構成します。これらのインスタンスは、パブリッククラウドおよびオンプレミスデータセンターにGLBノードとして展開されます。このStyleBookを使用して、階層型展開でGLBノードを構成できます。	1.1

ウェブアプリケーションファイアウォール機能

この表は、Web Application Firewall (WAF) 機能のデフォルトのStyleBookを示しています。

スタイルブック名	説明	バージョン
`waf-basic`	アプリケーションファイアウォールポリシーを使用して、基本的なWebアプリケーションを構成します。	1.2
`waf-adv`	アプリケーションファイアウォールポリシーを使用して、高度なWebアプリケーションを構成します。	1.2
`waf-default-130`と`waf-default-131`	NetScalerインスタンスのWAFとIPレピュテーションポリシーを構成します。	1.2
`lb-appfw`	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とともにロードバランシング構成を展開します。	1.0

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

スタイルブック名	説明	バージョン
`appfw-import-object`	アプリケーションファイアウォールオブジェクトを作成またはアップロードします。	1.1
`appfw-general-settings`	アプリケーションファイアウォールのグローバル設定を構成します。これらの設定は、NetScalerインスタンス内のすべてのアプリケーションに適用されます。	1.0
`apic-http-lb`	Cisco APIC を介して HTTP ロードバランサーアプリケーションを作成します。	1.0
`api-waf-profile`	NetScaler Console で WAF プロファイルを作成します。このプロファイルを使用すると、API リソースに WAF ポリシーを構成できます。	1.0

アプリケーションセキュリティ機能

この表は、アプリケーションセキュリティ機能のデフォルトのStyleBookを示しています。

スタイルブック名	説明	バージョン
`api-proxy`	NetScalerインスタンスにAPIプロキシを作成します。同じポリシータイプで複数のプロキシを作成できます。	1.1
`appsec-for-gateway`	開始する前に、カスタムのボットシグネチャを作成します。WAFとボットを使用して認証ポリシーを構成し、Gatewayログインページを保護します。この認証ポリシーを認証仮想サーバーにバインドします。	1.0

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

スタイルブック名	説明	バージョン
`appsec-for-gateway-with-insights`	開始する前に、カスタムのボットシグネチャを作成します。WAFとボットを使用して認証ポリシーを構成し、セキュリティインサイトでGatewayログインページを保護します。この認証ポリシーを認証仮想サーバーにバインドします。	1.0
`appvserver-contentrule-networkfunction-bind`	NetScalerインスタンスからのアプリケーショントラフィックに独自の `contentRule` 構成を適用します。	1.0
`appsec-owasptop10-protection`	WAFとボットポリシーを使用して保護構成を作成します。このStyleBookは、NetScaler構成をOWASPトップ10の脆弱性にマッピングします。	1.0

ボット管理機能

この表は、ボット管理機能のデフォルトのStyleBookを示しています。

スタイルブック名	説明	バージョン
`api-bot-profile`	NetScaler Consoleでボットプロファイルを作成します。このプロファイルを使用すると、APIリソースにボットポリシーを構成できます。	1.0
`bot-signature`	NetScalerインスタンスのボットシグネチャを作成します。	1.2

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

スタイルブック名	説明	バージョン
`bot-management`	ボットポリシーを使用してWebアプリケーション構成を定義します。	1.2
`bot-general-settings`	NetScalerインスタンスのボット管理チェックのグローバル設定を構成します。詳細については、「ボット管理」を参照してください。	1.2

NetScalerネットワーク構成

この表は、NetScalerネットワーク構成のデフォルトのStyleBookを示しています。

スタイルブック名	説明	バージョン
`adc_globalparam_configuration`	NetScalerインスタンスのグローバルパラメータを設定します。	1.0
`snmp_configuration`	NetScalerインスタンスにSNMP構成を展開します。Simple Network Management Protocol (SNMP) アプリケーションは、NetScaler ConsoleでNetScalerイベントをログに記録するのに役立ちます。詳細については、「SNMP構成」を参照してください。	1.0
`adv_network_configuration`	VXLAN、クラスターなどの高度なネットワーク構成を展開します。詳細については、ネットワーキングを参照してください。	1.0
`storefront`	Citrix StoreFront 用にNetScaler インスタンスを構成します。	1.0

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

スタイルブック名	説明	バージョン
`ntp_configuration`	NetScaler インスタンスでネットワークタイムプロトコル (NTP) リソースを構成します。	1.0
`network_param_configuration`	AppAlg、ARP、インバウンド NAT などのネットワークパラメータを構成します。	1.0
`network_configuration`	基本的なネットワークコンポーネントを展開します。詳細については、ネットワーキングを参照してください。	1.0
`cs-netfunc`	NetScalerインスタンスのコンテンツスイッチング仮想サーバーの高度なネットワーク機能を構成します。	1.0

次のステップ?

デフォルトのStyleBookから構成パックを作成するには、構成パックの作成の手順に従ってください。

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 Console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。

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とともにロードバランシング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：

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

1. NetScaler Consoleで、**アプリケーション** > **構成** > **StyleBooks** に移動します。StyleBooksページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、アプリケーションファイアウォールポリシーとIPレピュテーションポリシーを含むHTTP/SSLロードバランシングStyleBookを見つけます。`lb-appfw` のように名前を入力してStyleBookを検索することもできます。**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付きの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。

   アプリケーションファイアウォール設定でロードバランシング構成を作成する(/en-us/netscaler-console-service/media/waf-stylebook-1.png)

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-console-service/media/waf-stylebook-2.png)

4. オプションで、ロードバランシング仮想サーバーのトラフィックを認証するための認証サーバーを設定することもできます。

   オプション、高度なロードバランサー仮想サーバー(/en-us/netscaler-console-service/media/waf-stylebook-3.png)

5. サーバーIPとポートセクションで「+」をクリックして、アプリケーションサーバーとそれらにアクセスできる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-console-service/media/waf-stylebook-4.png)

6. アプリケーションサーバーのFQDN名を作成することもできます。

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

アプリケーションサーバーのFQDN名を作成します(/en-us/netscaler-console-service/media/waf-stylebook-5.png)

7. SSL証明書の詳細を指定することもできます。

   アプリケーションサーバーにSSL証明書の詳細を指定します(/en-us/netscaler-console-service/media/waf-stylebook-6.png)

8. ターゲットのNetScalerインスタンスでモニターを作成することもできます。

   ターゲットインスタンスでモニターを作成します(/en-us/netscaler-console-service/media/waf-stylebook-7.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したい場合は、アプリケーションファイアウォールポリシー規則がtrueであることを確認してください。そうでない場合は、アプリケーションファイアウォール設定を適用するリクエストのサブセットを選択するためにNetScalerポリシー規則を指定します。次に、適用する必要があ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-console-service/media/waf-stylebook-8.png)

10. オプションで、アプリケーションファイアウォールプロファイル設定チェックボックスを有効にすることで、詳細なアプリケーションファイアウォールプロファイル設定を構成できます。
11. オプションで、アプリケーションファイアウォール署名を構成したい場合は、仮想サーバーが展開されるNetScalerインスタンス上に作成された署名オブジェクトの名前を入力します。

    注

    このStyleBookを使用して署名オブジェクトを作成することはできません。

12. 次に、StartURL設定、DenyURL設定などの他のアプリケーションファイアウォールプロファイル設定も構成できます。

    アプリケーションファイアウォールと構成設定の詳細については、「Application Firewall」を参照してください。

13. **ターゲットインスタンス**セクションで、アプリケーションファイアウォールとともにロードバランシング仮想サーバーを展開するNetScalerインスタンスを選択します。

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

> **注**
>
> このウィンドウで、更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを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。

14. 不要なリクエストを送信しているIPアドレスを特定するために、**IPレピュテーションチェック**を有効にすることもできます。IPレピュテーションリストを使用して、評判の悪いIPからのリクエストを事前に拒否できます。
15. **作成**をクリックして、選択したNetScalerインスタンスに構成を作成します。

> **ヒント**
>
> インスタンスで実際の構成を実行する前に、ターゲットインスタンスで作成する必要がある構成オブジェクトを確認するために、**ドライラン**を選択することをお勧めします。

構成が正常に作成されると、StyleBookは必要なロードバランシング仮想サーバー、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、それらをロードバランシング仮想サーバーにバインドします。

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。

WAFによってインスタンスに作成されたオブジェクト(/en-us/netscaler-console-service/media/waf-stylebook-12.png)

16. NetScaler Consoleで作成されたConfigPackを表示するには、**Applications** > **Configurations**に移動します。

WAF構成パック(/en-us/netscaler-console-service/media/waf-stylebook-13.png)

SNMP 設定スタイルブック

シンプルネットワーク管理プロトコル (SNMP) アプリケーションは、NetScaler Console で NetScalerイベントをログに記録するのに役立ちます。このアプリケーションはNetScaler Consoleで実行され、NetScalerインスタンス上のSNMPエージェントにクエリを実行します。エージェントは、ネットワーク管理アプリケーションによって要求されたデータを管理情報ベース (MIB) で検索し、そのデータをアプリケーションに送信します。

インスタンスで設定変更が発生すると、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。NetScaler

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

Consoleはトラップ宛先として設定されます。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、要求されたデータを管理情報ベース (MIB) で検索し、そのデータをSNMPマネージャーに送信します。

StyleBookを使用してNetScalerインスタンスにSNMP設定を展開するには、次の手順を実行します。

1. NetScaler Consoleで、**Applications > Configuration > StyleBooks** に移動します。名前を `snmp_configuration` と入力して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イスページとして開き、このStyleBookで定義されているすべてのパラメーターの値を入力できます。
2. 次のパラメーターを指定します。

   - **SNMP MIB設定** - 次のインスタンス情報を指定します。
     - **管理者の連絡先**: 管理者のメールアドレス。
     - **NetScaler名**: NetScalerインスタンスの名前。
     - **NetScalerの場所**: インスタンスの物理的な場所。
     - **カスタム識別番号**: NetScalerのカスタム識別番号。この番号はインスタンスの識別に役立ちます。
     - **オーナーノード**: このMIBを設定するクラスターノードID。このフィールドは、CLIPでSNMP MIBを設定するために必須です。

   - **SNMPコミュニティ設定** - 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。この文字列は、GET、GET NEXT、ALL、GET BULKなどの任意のSNMPクエリタイプに関連付けることができます。

     「SNMPコミュニティ設定」(/en-us/netscaler-console-service/media/snmp-comunity-string.png)
   - **SNMPエンジンID設定** - SNMPv3エンジンには一意の識別子 (ID) があります。このIDは、SNMPv3ユーザーとSNMPv3エンジンの間の通信で使用されます。このIDは、最低10文字の16進値です。この設定では、MIB設定で指定する `Ownernode` を指定します。

     「SNMPエンジンID」(/en-us/netscaler-console-service/media/snmp-engine-id.png)
   - **SNMPオプション設定** - SNMPマネージャーのSNMPオプションを有効または無効にできます。

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

- **SNMP Setリクエスト**: このオプションを有効にすると、SNMPマネージャーがMIBオブジェクトに値を書き込めるようになります。
- **SNMPトラップロギング**: このオプションはSNMPトラップイベントをログに記録します。
- **SNMPトラップロギングレベル**: このオプションは、SNMPトラップログの監査ログレベルを送信します。
- **パーティション名の送信**: このオプションはパーティション名を送信します。

「SNMPオプション」(/en-us/netscaler-console-service/media/snmp-options.png)

- **SNMPマネージャー設定** - NetScalerインスタンスを照会するSNMPマネージャー。マネージャーはSNMP V1、V2、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、インスタンスは指定された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。
  - **IPアドレス**: SNMPマネージャーのIPアドレス。
  - **ネットマスク**: IPv4ネットワークアドレスに関連付けられたサブネットマスク。
  - **ドメイン解決の再試行**: 最後のDNSクエリがSNMPマネージャーのホスト名を解決できなかった場合、NetScalerインスタンスは、別のDNSクエリを送信する前に、指定された間隔だけ待機します。

  「SNMPマネージャー」(/en-us/netscaler-console-service/media/snmp-manager-configuration.png)
- **SNMPアラーム設定** - エンタープライズ固有のトラップメッセージを生成するためにSNMPアラームを追加します。NetScalerインスタンスは、タイプ (クラス) がSPECIFICのトラップリスナーにのみトラップメッセージを送信します。SNMPアラームは、イベントベースまたはしきい値ベースのいずれかです。
  - **トラップ名**: SNMPアラームの名前。
  - **状態**: NetScalerインスタンスは、有効になっているSNMPアラームに対してのみトラップメッセージを生成します。
  - **ロギング**: ロギングを有効にすると、NetScalerインスタンスはこのアラームに対して生成されたすべてのトラップメッセージをログに記録します。
  - **高しきい値**: この値は、このアラームに関連付けられた属性の最大制限です。属性がこの値に達するか超えると、NetScalerインスタンスはSNMPトラップメッセージを生成します。

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

- **通常しきい値**: この値は、このアラームに関連付けられた属性の最小制限です。属性がこの値に達するか下回ると、NetScalerインスタンスはSNMPトラップメッセージを生成します。
- **時間 (秒)**: 指定された条件が満たされたときに、NetScalerインスタンスがSNMPトラップメッセージを生成する間隔。
- **重大度**: このアラームによって生成されるトラップメッセージの重大度レベル。このフィールドは、インスタンスに重大度レベルに基づいてトラップメッセージを送信させたい場合に役立ちます。

- **SNMPトラップ構成** - この構成はSNMPトラップリスナーを追加します。NetScalerインスタンスは、異常な状態を報告するためにトラップメッセージを生成します。トラップメッセージはトラップリスナーに送信され、管理者がインスタンスを監視し、問題に迅速に対応するのに役立ちます。

  - **トラップクラス**: インスタンスがトラップリスナーに送信するトラップメッセージの種類。
  - **トラップ宛先**: トラップリスナーのIPv4またはIPv6アドレス。インスタンスはSNMPトラップメッセージをこのIPアドレスに送信します。
  - **バージョン**: SNMPバージョン。このバージョンはトラップリスナーのバージョンと一致している必要があります。そうでない場合、リスナーはトラップメッセージを破棄します。
  - **UDP宛先ポート**: トラップリスナーがトラップメッセージを受信するUDPポート。この値はトラップリスナーの値と一致している必要があります。そうでない場合、リスナーはトラップメッセージを破棄します。
  - **コミュニティ名**: トラップメッセージとともに文字列が送信されます。トラップリスナーはこの文字列を認証に使用します。
  - **送信元IP**: 送信元IPアドレス。NetScalerインスタンスのIPv4またはIPv6アドレス。
  - **深刻度**: トラップメッセージの深刻度レベル。NetScalerインスタンスは、指定された深刻度レベル以上のトラップメッセージを送信します。
  - **トラフィックドメイン**: トラフィックドメインを一意に識別する整数値。
  - **すべてのパーティション**: このオプションが有効になっている場合、インスタンスはすべてのパーティションのトラップメッセージを宛先IPアドレスに送信します。

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

- **SNMPビュー構成** - SNMPビューは、SNMPv3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。

  - **ビュー名**: SNMPv3ビューの名前。

    インスタンスは、サブツリーパラメータ設定によって区別される、同じ名前の複数のSNMPv3ビューを持つことができます。最大1000個のSNMPv3ビューを追加できます。

  - **サブツリー**: このSNMPv3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。

- **SNMPグループ構成** - インスタンス上のSNMPv3ユーザーグループ。これらのグループは、SNMPv3ユーザーの論理的な集合体です。SNMPv3グループは、アクセス制御を実装し、ユーザーのセキュリティレベルを定義するために使用されます。NetScalerインスタンスに最大1000個のSNMPv3グループを追加できます。

- **SNMPユーザー構成** - NetScalerインスタンスにSNMPクエリを送信できるSNMPv3ユーザーを追加します。最大1000個のSNMPv3ユーザーを追加できます。

  - **名前**: SNMPv3ユーザーの名前。
  - **グループ**: SNMPv3ユーザーにバインドする構成済みSNMPv3グループの名前。このグループに設定されたアクセス権（バインドされたSNMPv3ビュー）とセキュリティレベルがこのユーザーに割り当てられます。
  - **Authype**: NetScalerインスタンスにアクセスするSNMPv3ユーザーを認証するために使用されるアルゴリズム。SNMPマネージャーでSNMPv3ユーザーを設定する際には、同じ認証アルゴリズムを指定する必要があります。
  - **Authpassword**: 認証用のパスワードです。このパスワードは、指定された認証アルゴリズムタイプを使用します。
  - **Privtype**: SNMPv3ユーザーとNetScalerインスタンス間の通信を暗号化するアルゴリズム。
  - **privpasswd**: **Privtype**で指定された暗号化アルゴリズムの暗号化キー。

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

- **SNMPユーザーのトラップバインディング設定** - SNMPv3は、SNMPユーザーの資格情報を使用して、認証や暗号化などのセキュリティ機能を提供します。SNMPマネージャーは、その設定にSNMPユーザーに割り当てられたパスワードが含まれている場合にのみ、SNMPv3トラップメッセージを受信できます。

3. **ターゲットインスタンス**で、設定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に設定を展開できます。

4. **タグ関連付け**で、現在および将来のすべてのStyleBookタグを設定に関連付けます。

   このオプションは、すべてのStyleBookタグを構成パックに関連付けます。また、将来StyleBookに追加する可能性のある新しいタグも確実に連携させます。

5. **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。

6. **作成**をクリックします。

   設定パックは、**StyleBook > Configurations** ページに表示されます。

NetScalerネットワーク構成StyleBook

NetScalerインスタンスにさまざまなネットワークコンポーネントを展開する場合、NetScaler Console StyleBookを使用できます。NetScalerネットワークコンポーネントを作成するには、以下のStyleBookを使用します。

- `network_configuration`: 基本的なネットワークコンポーネント用。
- `adv_network_configuration`: VXLAN、クラスターなどの高度な構成用。

NetScalerネットワークコンポーネントの詳細については、「ネットワーク」を参照してください。

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

基本的なネットワークコンポーネントを展開する

基本的なネットワークコンポーネントには、インターフェイス、チャネル、VLAN、NSIP、アドレス解決プロトコル (ARP)、またはブリッジグループ構成があります。これらのコンポーネントのいずれかを展開するには、次の手順を実行します。

1. NetScaler Consoleで、**アプリケーション > 構成 > StyleBooks** に移動します。`network_configuration`として名前を入力してStyleBookを検索します。
2. **構成の作成** をクリックします。
3. 必要に応じて、以下の構成を追加します。

> **注**
>
> 各セクションの (+) アイコンをクリックして構成を追加します。

- **インターフェイス構成** - 構成内のインターフェイスの数は、NetScalerインスタンスのモデルによって異なります。インターフェイスの詳細については、「インターフェイス」を参照してください。インターフェイスを構成するために必要なフィールドを指定します。
- **チャネル構成** - リンクアグリゲーションを構成すると、NetScalerインスタンスと他の接続デバイス間の通信チャネルの容量と可用性が向上します。集約されたリンクは「チャネル」とも呼ばれます。リンクアグリゲーションは、複数のポートからのデータを単一の高速リンクに結合します。詳細については、「リンクアグリゲーションの構成」を参照してください。
- **チャネルインターフェイスバインディング構成** - 構成をバインドするインターフェイスとチャネルIDを指定します。
- **VLAN構成** - VLANを設定し、IPサブネットにバインドできます。NetScalerは、これらのVLAN間でIP転送を実行します（これらのサブネット上のホストのデフォルトルーターとして構成されている場合）。詳細については、「VLANについて」を参照してください。VLANを構成するための詳細を指定します。
- **NS IP構成** - NSIPアドレスは、管理目的でNetScalerインスタンスにアクセスするためのIPアドレスです。インスタンスは1つのNSIPのみを持つことができ、これは管理IPアドレスとも呼ばれます。詳細については、「NSIPアドレスの構成」を参照してください。
- **NS IP6構成** - NetScalerインスタンスにIPv6アドレスをNSIPとして構成することもできます。
- **VLANインターフェースバインディングの構成** - ネットワークインターフェースをVLANにバインドすると、そのネットワークインターフェースはデフォルトVLANから削除されま

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

す。ネットワークインターフェースが複数のVLANの一部である必要がある場合は、タグ付きメンバーとしてVLANにバインドできます。

- **VLAN NS IPバインディングの構成** - NetScaler IPアドレス (NSIP) をVLANにバインドできます。IPアドレスがVLANに関連付けられると、そのサブネット内のすべてのIPアドレスが自動的にVLANに関連付けられます。
- **IPv4のルート構成** - NetScalerインスタンスのルーティングテーブルにルートエントリを追加したいネットワークIPアドレス (IPv4) を追加します。
- **IPv6のルート構成** - NetScalerインスタンスのルーティングテーブルにルートエントリを追加したいネットワークIPアドレス (IPv6) を追加します。
- **ARP構成** - ARPテーブルに静的ARPエントリを追加したり、静的ARPエントリを削除したりできます。詳細については、「静的ARP」を参照してください。
- **ND6変数構成** - 近隣探索 (ND) は、IPv6の最も重要なプロトコルの1つです。これは、アドレス解決プロトコル (ARP)、インターネット制御メッセージプロトコル (ICMP)、およびルーター探索の機能を組み合わせたメッセージベースのプロトコルです。NDにより、ノードは自身のリンク層アドレスをアドバタイズし、隣接ノードのMACアドレスまたはリンク層アドレスを取得できます。詳細については、「近隣探索」を参照してください。

  NetScalerインスタンスのND6変数を構成できます。
- **IPv6の近隣探索構成** - IPv6アドレスのNDを構成できます。
- **ブリッジグループ構成** - ブリッジグループ機能はVLANと同じように機能します。複数のVLANを単一のブリッジグループにバインドでき、同じブリッジグループにバインドされたすべてのVLANは単一のブロードキャストドメインを形成します。詳細については、「ブリッジグループの構成」を参照してください。
- **ブリッジグループ NS IPv46バインディング構成** - NetScaler IP (NSIP) アドレスをブリッジグループにバインドします。
- **ブリッジグループ VLANバインディング構成** - VLANをブリッジグループにバインドします。

4. **ターゲットインスタンス**で、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. 「**タグ関連付け**」で、現在および将来のすべてのStyleBookタグを構成に関連付けます。

   このオプションは、すべてのStyleBookタグを構成パックに関連付けます。また、将来StyleBookに追加する可能性のある新しいタグも確実にS関連付けます。
6. 「**ドライラン**」をクリックします。

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

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。

7. 「**作成**」をクリックします。

構成パックは、「**StyleBook > 構成**」ページに表示されます。

高度なネットワークコンポーネントを展開する

高度なネットワークコンポーネントには、VXLAN、VRID、ブリッジテーブル、フェイルオーバーインターフェースセット (FIS)、INAT、RNAT構成などがあります。このような高度なネットワークコンポーネントを展開するには、次の手順を実行します。

1. NetScaler Consoleで、「**アプリケーション > 構成 > StyleBooks**」に移動します。名前を `adv_network_configuration` と入力してStyleBookを検索します。
2. 「**構成の作成**」をクリックします。
3. 必要に応じて、次の構成を追加します。

> **注**
>
> 各セクションの (+) アイコンをクリックして構成を追加します。

- **VXLAN構成** - VXLANは、VLANよりも高いスケーラビリティと柔軟性を提供します。詳細については、VXLANを参照してください。
- **VXLAN VLAN MAP構成** - NetScalerインスタンス上にマッピングテーブルを作成します。このテーブルは、VXLAN IDを対応するVLAN IDにマッピングします。
- **VRID構成** - 仮想MAC (VMAC) を識別するIPv4アドレスを追加します。他のVRIDオプションとバインディング情報も構成できます。
- **VRID6構成** - 仮想MAC (VMAC) を識別するIPv6アドレスを追加します。他のVRID6オプションとバインディング情報も構成できます。
- **BridgeTable構成** - NetScalerインスタンスは、宛先MACアドレスとVLAN IDのブリッジテーブルルックアップに基づいてフレームをブリッジします。ブリッジテーブルを監視するために必要な詳細を指定します。
- **FIS構成** - FISはインターフェイスの論理グループです。NetScaler HA構成では、FISを使用することで、インターフェイスをグループ化して、1つのインターフェイスが故障しても他の機能しているインターフェイスが利用可能になるようにすることで、フェイルオーバーを防ぐことができます。FISはNetScalerクラスターのノードに対しても構成できます。詳

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

細については、「フェイルオーバーインターフェイスセットの構成」を参照してください。

- **ForwardingSessionの構成** - フォワーディングセッションルールは、特定のネットワークから発信または宛先となり、NetScalerインスタンスによって転送されるトラフィックのフォワーディングセッションエントリを作成します。IPv4トラフィックとIPv6トラフィックの両方に対してフォワーディングセッションルールを作成できます。「フォワーディングセッションルールの構成」を参照してください。
- **INAT構成** - クライアントがインバウンドネットワークアドレス変換 (INAT) 用に構成されたNetScalerインスタンスにパケットを送信すると、インスタンスはパケットのパブリック宛先IPアドレスをプライベート宛先IPアドレスに変換します。そして、インスタンスはそのアドレスのサーバーにパケットを転送します。「インバウンドネットワークアドレス変換」を参照してください。
- **NAT64構成** - ステートフルNAT64は、NetScalerアプライアンスでセッション情報を維持しながら、IPv6からIPv4へのパケット変換を介してIPv6クライアントとIPv4サーバー間の通信を可能にし、その逆も可能です。「ステートフルNAT64変換」を参照してください。
- **RNAT構成** - リバースネットワークアドレス変換 (RNAT) では、NetScalerアプライアンスはサーバーによって生成されたパケットの送信元IPアドレスをパブリックNAT IPアドレスに置き換えます。「RNAT」を参照してください。
- **RNAT6構成** - IPv6パケットのリバースネットワークアドレス変換 (RNAT) ルールはRNAT6と呼ばれます。「RNAT6の構成」を参照してください。
- **IPSet構成** - IPセットは、NetScalerインスタンス上でサブネットIPアドレス (SNIP) または仮想IPアドレス (VIP) として構成されるIPアドレスのセットです。IPセットを作成するために必要な詳細を指定します。
- **IPTunnel構成** - IPトンネルとそのバインディングを作成するための詳細を指定します。「IPトンネル」を参照してください。
- **IP6トンネル構成** - IPv6アドレスの場合、IPトンネルとそのバインディングを作成するための詳細を指定します。
- **Linkset構成** - リンクセットは、同じブロードキャストドメインに属するクラスターノードのインターフェイスのグループです。「リンクセットの構成」を参照してください。
- **MAP-T基本マッピングルール構成** - マッピングアドレスとポートの変換 (MAP-T)。これは、顧客宅内機器 (CE) および境界ルーター (ISPコアネットワーク内) で二重変換 (IPv4からIPv6、およびその逆) を実行するメカニズムです。基本的なマッピングルールを追加するための詳細を指定します。「マッピングアドレスとポートの変換」を参照してください。

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

- **MAP-Tデフォルトマッピングルール構成** - デフォルトのマッピングルールを追加するための詳細を指定します。
- **MAP-Tマップドメイン構成** - マップドメインを追加するための詳細を指定します。
- **NetProfile構成** - ネットプロファイルを追加し、オーバーライド `lsn` を構成します。
- **NetBridge構成** - VXLAN-VLANマップをネットワークブリッジにバインドします。
- **ルーターアドバタイズメント構成用のオンリンクIPv6グローバルプレフィックス** - IPv6クラスター構成の場合、グローバルプレフィックスとルーターアドバタイズメントを構成します。「クラスターのIPv6対応ロゴのサポート」を参照してください。

4. **ターゲットインスタンス**で、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. **タグ関連付け**で、現在および将来のすべてのStyleBookタグを構成に関連付けます。

   このオプションは、すべてのStyleBookタグを構成パックに関連付けます。また、将来StyleBookに追加する可能性のある新しいタグも関連付けられるようにします。
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インスタンスから作成、変更、または削除されるオブジェクトが表示されます。
7. **作成**をクリックします。

構成パックは、**StyleBook > 構成**ページに表示されます。

Prometheus アナリティクス StyleBook

NetScalerでアナリティクスプロファイルを作成し、スキーマファイルを指定することで、NetScalerからPrometheusにメトリクスをエクスポートできます。StyleBookでは、`Prometheus TimeSeries Analytics Configuration` StyleBookを使用して、すべての管理対象インスタンスに構成を実行できます。

前提条件

管理対象のNetScalerインスタンスが**13.1 build 39-27以降**であることを確認してください。

`Prometheus TimeSeries Analytics Configuration` StyleBookを使用して構成するには：

1. **Applications** > **Configurations** > **StyleBooks** に移動し、名前を `Prometheus TimeSeries Analytics Configuration` と入力してStyleBookを検索し、**Create Configuration** をクリックします。
2. **Configpack の詳細**」で：

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

a. アナリティクスプロファイル名を指定します。詳細については、「Configure metrics collector」を参照してください。

b. **カウンタースキーマファイル：**

- デフォルトのスキーマで続行する場合は、この手順をスキップできます。
- カスタムスキーマで続行する場合は、パラメータで変更したスキーマファイルをアップロードします。NetScalerでは、サポートされているすべてのカウンターを含む参照ファイル `reference_schema.json` がパス `/var/metrics_conf/` の下にあります。FTPクライアントを使用して、ファイルをローカルにファイルをコピーできます。

3. **Target Instances** で、構成を実行するインスタンスまたはインスタンスグループを選択します。
4. **Tag Assosiation** で、現在および将来のすべてのStyleBookタグを構成に関連付けます。

   このオプションは、すべてのStyleBookタグを構成パックに関連付けます。また、将来StyleBookに追加する可能性のある新しいタグも関連付けられるようにします。

   注：

   NetScaler®インスタンスから作成、変更、または削除される結果を表示するには、「**ドライラン**」をクリックします。

5. 構成を実行するには、「**作成**」をクリックします。

StyleBooks Configuration Builder を使用した NetScaler アプリケーション構成の移行

StyleBooks Configuration Builder は、既存の NetScaler 構成を StyleBooks に移行するために使用されます。この機能は、アプリケーション構成の移行を、ある NetScaler インスタンスから別のインスタンスまたは Autoscale グループへ自動化します。

Configuration Builder は、NetScaler 構成のあらゆるバリアントに使用できる構造化されたアプリケーション StyleBook を提供します。この機能は、StyleBooks の文法や構成要素に関する深い知識がなくても StyleBooks を使い始めるのに役立ちます。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 NetScaler インスタンスで同じ NetScaler 構成を反映する構成パックも作成します。この構成パックを使用すると、ある NetScaler インスタンスからの初期

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

NetScaler 構成を別の NetScaler 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い場合でも、Configuration Builder は NetScaler 構成を StyleBook および構成パックに変換します。この構成パックは、後で NetScaler 構成を他の NetScaler インスタンスに移行するために使用できます。

  ターゲットインスタンスが Autoscale™ グループの場合、構成パックは **Network > AutoScale Group** ページに表示されます。**Configuration** タブの下です。
- **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 は選択したアプリケーションの CLI コマンドのセットを抽出します。これらの CLI コマンドはソース構成から抽出されます。また、入力が必要となる可能性のある展開属性と構成属性も識別します。

- **IP アドレス/ポート** - 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。
- **構成ファイル/シークレット** - これらの属性は、ソース構成で指定されたパスワードまたは証明書である場合があります。

必要な情報を指定した後、ターゲット NetScaler インスタンスでアプリケーション構成の移行または複製を開始します。

アプリケーションの作成と移行後、`adc_nitro_application` StyleBook を使用して NetScaler Console に構成パックが作成されます。この StyleBook は NetScaler NITRO リソースに基づいて作成されます。この構成パックは、ターゲット NetScaler インスタンス上のアプリケーション構成を表します。作成された構成パックを表示するには、**Applications > Configuration > Confg Packs** に移動します。

移行された構成間での構成エンティティの共有

Config Migrationユーティリティを使用して構成を移行する際に、構成エンティティを再利用できます。その後の移行では、既存の構成エンティティが正常に再利用されます。以前は、一部の構成エンティティを共有する2つの構成を移行する際に、「**Resource already exists**」というエラーで構成の移行が失敗していました。このオプションにより、複数の構成で構成エンティティが使用されるシナリオで、それらの再利用が可能になり、移行ワークフローが効率化されます。

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

サポートされているNetScaler機能

StyleBook Configuration Builderは、ソース構成内の以下の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
- 負荷分散
- 監視
- SSLオフロード
- レート制限
- 書き換え
- レスポンダー
- Webアプリケーションファイアウォール (WAF)
- ボット管理
- 圧縮制御

NetScalerアプリケーション構成を移行するためのStyleBookの作成

NetScaler Console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. **アプリケーション > 設定 > 設定パック** に移動します。
2. **Migrate NetScaler 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 a NetScaler**: このオプションは、選択したNetScaler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元の **Source NetScaler Instance** を指定します。

    アプリケーション構成をAutoscaleグループに移行するには、ソース構成に以下の情報が含まれていないことを確認してください。

    - `IPset`
    - デバイスプロファイル

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

- プロトコル
- ポート

6. アプリケーション構成を移行または複製する先の **Target NetScaler Instance** を指定します。

   アプリケーション構成をAutoscaleグループに移行するには、リストからAutoscaleグループを選択します。

7. **アプリケーションの定義** で、,

   a. 「**アプリケーション名**」で、アプリケーションの名前を指定します。

      ターゲットインスタンスがAutoscaleグループである場合は、次のAutoscaleパラメータを指定します。

      - 「**アクセスタイプ**」 - NetScaler Consoleのオートスケーリングソリューションは、外部アプリケーションと内部アプリケーションの両方に使用できます。必要なアプリケーションアクセスタイプを選択します。
      - 「**ドメイン名**」 - アプリケーションのドメイン名を指定します。このオプションは、ユーザー定義FQDNタイプを選択した場合にのみ適用されます。
      - 「**ドメインのゾーン**」 - リストからアプリケーションのゾーン名を選択します。このオプションは、ユーザー定義FQDNタイプを選択した場合にのみ適用されます。

        このドメイン名とゾーン名は、Azureの仮想サーバーにリダイレクトされます。たとえば、`app.example.com`でアプリケーションをホストしている場合、`app`がドメイン名で、`example.com`がゾーン名です。

   b. 移行する仮想サーバーを選択します。

   c. 「**次へ**」をクリックします。

8. 「**同等のCLIコマンド**」で、コマンドを確認し、「**次へ**」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のものです。

   「

注:

」.

必要に応じて、構成を追加または編集することもできます。

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

9. 「**展開属性**」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、フロー図の仮想サーバー、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。

   展開属性を編集する(/en-us/netscaler-console-service/media/edit-deployment-attributes.png)

   注:

   ターゲットインスタンスがAutoscaleグループの場合、フロントエンドIPアドレスの編集は無効になります。

   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る場合。
   - CLIコマンドを使用して構成をインポートする場合。

10. **構成属性**で、必要な詳細を指定し、**次へ**をクリックします。

    このタブには、パスワードと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、ターゲットインスタンスで、見つからない構成またはサポートされていない構成を個別に適用する必要があります。そして、**次へ**をクリックします。

11. **移行**で、**移行**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。

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

- ソースに`servicegroup`とモニターバインディングが次のように設定されている場合:

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  次のエラーが表示されます:

  ```
  CLI Command conversion failed: 100 - No such command [{ "errorcode":
  1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
  ```

  このエラーは、NetScaler がサービスグループとモニター間のバインディングを無効な形式で保存するため発生します。この問題は、NetScaler 12.1.52.15 ビルド以降で修正されています。

ビジネスアプリケーション StyleBook

NetScaler Console は、特定のビジネスアプリケーション向けに NetScaler の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、以下のトピックを参照してください。

- SSO Google Apps スタイルブック
- SSO Office 365 スタイルブック
- Microsoft Skype for Business スタイルブック
- Microsoft Exchange スタイルブック
- Microsoft SharePoint スタイルブック
- Microsoft ADFS プロキシ スタイルブック
- Oracle e-ビジネス スタイルブック

SSO Google Apps スタイルブック

Google Appsは、Googleが開発したクラウドコンピューティング、生産性向上、コラボレーションツール、ソフトウェア、製品のコレクションです。シングルサインオン (SSO) を使用すると、ユーザーはエンタープライズ資格情報を使用してすべてのサービスに一度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め、すべてのエンタープライズクラウドアプリケーションにアクセスできます。

NetScaler Console SSO Google Apps StyleBookを使用すると、NetScalerインスタンスを介してGoogle AppsのSSOを有効にできます。このStyleBookは、NetScalerインスタンスを、Google Appsにアクセスするユーザーを認証するためのSAML IDプロバイダーとして構成します。

© 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:

次の表に、この統合を正常に機能させ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、これより新しいバージョンもサポートしています。

製品	最小要件バージョン
NetScaler	リリース11.0、Advanced/Premiumライセンス

以下の手順は、認証要求をNetScalerが監視するIPアドレスにルーティングするために、適切な外部および内部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。

SSO GoogleアプリStyleBook構成の展開:

以下のタスクは、ビジネスネットワークにMicrosoft SSO Google Apps StyleBookを展開するのに役立ちます。

SSO GoogleアプリStyleBookを展開するには

1. NetScaler Consoleで、**Applications** > **Configurations** > **StyleBooks** に移動します。StyleBooksページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、**SSO Google Apps StyleBook** を見つけます。**Create Configuration** をクリックします。
2. StyleBookは、このStyleBookで定義されているすべてのパラメータの値を入力できるユーザーインターフェイスページとして開きます。
3. 以下のパラメータの値を入力します:

    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NetScaler AAA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NetScaler AAA仮想サーバーによって使用されるSAML IdPプロファイルとポリシーを作成することにより、NetScalerインスタンスをSAML IDプロバイダーとして構成できます。

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://<Citrix_ADC_VIP>/saml/login`

b. **SAMLサービスプロバイダー（SP）ID**。（オプション）NetScaler IDプロバイダーは、このIDと一致する発行者名からのSAML認証要求を受け入れます。

c. **アサーションコンシューマーサービスURL**。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、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます:

i. SAMLバインディングプロファイル（デフォルトは「POST」プロファイルです）。

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」）。

iii. SAMLリクエスト/レスポンスのハッシュをダイジェストする方法（デフォルトは「SHA-1」）。

iv. 暗号化アルゴリズム（デフォルトはAES256）およびその他の設定。

注

これらの設定はGoogle Appsをサポートするためにテスト済みであるため、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以下の詳細を入力します。ドメインユーザーが会社のメールアドレスを使用してNetScalerインスタンスにログオンできるようにするには、以下を設定する必要があります。

a. **LDAP (Active Directory) ベース**。認証を許可するActive Directory (AD) 内で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) Bind DN Password**。認証用のドメインアカウントのパスワードを入力します。

d. このセクションで入力する必要があるその他のフィールドは次のとおりです。

i. ユーザー認証のためにNetScalerが接続するLDAPサーバーのIPアドレス

ii. LDAPサーバーのFQDN名

> **注**
>
> 上記の2つのうち、少なくとも1つを指定する必要があります - LDAPサーバーのIPアドレスまたはFQDN名。

iii. ユーザー認証のためにNetScalerが接続するLDAPサーバーポート (デフォルトは389です)。

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になっています) に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、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 Consoleのディレクトリから SSL証明書ファイルを選択します。

   c. **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 Console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. 「詳細証明書設定」チェックボックスを有効にして、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力することもできます。

7. オプションで、上記で入力したSAML IdP証明書がNetScalerにCA公開証明書をインストールする必要がある場合は、「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、「SAML SP SSL証明書」を選択して、Google Apps (SAML SP) からの認証要求を検証するために使用されるGoogle SSL証明書 (公開キー) を指定できます。

9. 「**ターゲットインスタンス**」をクリックし、このGoogle Apps SSO構成を展開するNetScalerインスタンスを選択します。「**作成**」をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

注

また、更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを、このウィンドウの利用可能なインスタンスリストに追加することもできます。

また、,

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

ヒント

SSO Office 365 スタイルブック

Microsoft Office 365は、Microsoftがサブスクリプションベースで提供する、クラウドベースの生産性およびコラボレーションアプリケーションのスイートです。これには、Exchange、SharePoint、Office、Skype for BusinessなどのMicrosoftの人気のあるサーバーベースのアプリケーションが含まれます。シングルサインオン (SSO) により、ユーザーはすべてのエンタープライズクラウドアプリケーションにアクセスできます。

- 管理コンソールにサインインする管理者を含む
- 企業の資格情報を使用して、すべてのMicrosoft Office 365サービスに1回サインオンします。

SSO Office 365 StyleBookを使用すると、NetScalerインスタンスを介してMicrosoft Office 365のSSOを有効にできます。これで、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認証を構成できます。

このStyleBookを使用してNetScalerインスタンスでMicrosoft Office 365のSSOを有効にするには、次の手順が必要です。

1. 認証仮想サーバーの構成
2. SAML IdPポリシーとプロファイルの構成
3. ポリシーとプロファイルを認証仮想サーバーにバインドする
4. インスタンス上でLDAP認証サーバーとポリシーを構成する
5. インスタンス上で構成された認証仮想サーバーにLDAP認証サーバーとポリシーをバインドします。

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が表に示されています。統合プロセスは、それらのより高い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	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済みであることを前提としています。これらのエントリは、認証要求をNetScalerが監視するIPアドレスにルーティングするために不可欠です。

以下の手順は、ビジネスネットワークでSSO Office 365 StyleBookを実装するのに役立ちます。

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

SSO Microsoft Office 365 StyleBookを展開するには

1. NetScaler Consoleで、**Applications > Configuration > StyleBooks**に移動します。**StyleBooks**ページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、**SSO Office 365 StyleBook**を見つけます。**Create Configuration**をクリックします。
2. StyleBookは、このStyleBookで定義されているすべてのパラメータの値を入力できるユーザーインターフェイスページとして開きます。
3. 次のパラメータの値を入力します。

   a. **アプリケーション名**。ネットワークに展開するSSO Microsoft Office 365構成の名前。

   b. **認証仮想IPアドレス**。Microsoft Office 365 SAML IdPポリシーがバインドされているNetScaler 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からそれぞれのファイルを選択します。PEM形式で暗号化されたプライベートキーをロードするために、プライベートキーのパスワードを入力することもできます。

   ☐
6. 「**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。
7. 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、オプションで「**SSL CA Certificate for the authentication virtual** IP」チェックボックスを選択できます。上記の「**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。
8. 「**LDAP Settings for SSO Office 365**」セクションで、Office 365ユーザーを認証するために以下の詳細を入力します。ドメインユーザーが会社のメールアドレスを使用してNetScalerインスタンスにログオンできるようにするには、以下を設定します。

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

a. **LDAP (Active Directory) ベース**。認証を許可するために、ユーザーアカウントがActive Directory (AD) 内に存在するドメインのベースドメイン名を入力します。例: `dc=netscaler,dc=com`

b. **LDAP (Active Directory) 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）。LDAPSは636を使用します。

iv. LDAPホスト名。検証が有効になっている場合（デフォルトでは無効）、ホスト名はLDAP証明書の検証に使用されます。

v. LDAPログイン名属性。ログイン名を抽出するために使用されるデフォルトの属性は「sAMAccountName」です。

vi. その他のオプションのLDAP設定。

☐

9. **SAML IdP Certificate** 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。

a. **Certificate Name**。SSL 証明書の名前を入力します。

b. **Certificate File**。ローカルシステムのディレクトリから SSL 証明書ファイルを選択します。

c. **CertKey Format**。ドロップダウンリストボックスから、証明書と秘密鍵ファイルの形式を選択します。サポートされている形式は .pem および .der 拡張子です。

d. **Certificate Key Name**。証明書の秘密鍵の名前を入力します。

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

e. **Certificate Key File**。ローカルシステムから、証明書の秘密鍵を含むファイルを選択します。

f. **Private Key Password**: 秘密鍵ファイルを保護するパスフレーズを入力します。

Advanced Certificate Settings チェックボックスを有効にすることもできます。ここでは、証明書の有効期限通知期間、証明書の有効期限モニターの有効化または無効化などの詳細を入力できます。

10. オプションで、上記で入力した SAML IdP 証明書が 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 Certificate** を選択できます。上記の **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。

11. **SAML SP Certificate** セクションで、Office 365 SSL 公開証明書の以下の詳細を入力します。この証明書は、NetScaler インスタンスが受信 SAML 認証要求を検証するために使用されます。

a. **Certificate Name**。SSL 証明書の名前を入力します。

b. **Certificate File**。ローカルシステムのディレクトリから SSL 証明書ファイルを選択します。

c. **CertKey Format**。ドロップダウンリストボックスから、証明書と秘密鍵ファイルの形式を選択します。サポートされている形式は .pem および .der 拡張子です。

「**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。

SAML SP証明書(/en-us/netscaler-console-service/media/nmas-sso-office-365-5.png)

12. 「**SAML IdP設定**」セクションでは、ステップ3で作成されたNetScaler AAA仮想サーバーで使用される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_VIP_Address\>/saml/login`

b. **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"`

c. **署名アルゴリズム**: SAMLリクエスト/レスポンスを検証/署名するための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.

d. **ダイジェストメソッド**。SAMLリクエスト/レスポンスのハッシュをダイジェストする方法を選択します (デフォルトは「SHA256」)。

e. **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。

f. **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。

g. **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。

h. このセクションには、他にも入力できるオプションフィールドがあります。たとえば、次のオプションを設定できます。

   i. **SAML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。

   ii. **SAML属性フレンドリ名**。SAMLアサーションで送信されるユーザー属性のフレンドリ名。

   iii. **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 (mail) をSAML認証属性として指定します。

   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ています。

   ヒント

   Citrixでは、これらの設定はMicrosoft Office 365アプリをサポートするためにテストされているため、デフォルト設定を維持することをお勧めします。

13. **ターゲットインスタンス**をクリックし、このMicrosoft Office 365 SSO構成を展開するNetScalerインスタンスを選択します。**作成**をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。

© 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Advanced Editionの2つのバージョンがあります。主な違いは、Advanced 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デプロイし、SQLサーバーをミラーリングする必要があります。

Advanced Editionのデプロイメントでは、異なる役割を持つ複数のサーバーを作成できます。

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アプリケーションにおいて、フロントエンドサーバーはネットワークの中核となるサーバーです。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会議のためのリンクとサービスを提供します。Skype for Business 2015 Enterprise Editionをデプロイする場合、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とともに、フロントエンドプールで負荷分散された少なくとも2つのフロントエンドサーバーで構成されます。

エッジサーバー:

Skype for Business向けにエッジサーバーをデプロイする必要があるのは、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

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

内部ユーザーとやり取りする必要がある場合です。これらの外部ユーザーは、認証されたリモートユーザー、匿名のリモートユーザー、フェデレーションパートナー、またはその他のモバイルクライアントである可能性があります。

Skype for Business Edge Serverには、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、リモート接続を許可し、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Web会議
- A/V会議パケットを処理し、オーディオとビデオ、アプリ共有、ファイル転送を外部ユーザーに拡張する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、セキュリティが向上します。

ディレクターは、複数のプールが存在する場合に最も役立ちます。これは、エンドポイントを認証するための単一の連絡先を提供するためです。また、リモートユーザーの場合、ディレクターはEdgeプールとFront-End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。

エンタープライズでの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。

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

© 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
	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 Consoleで、**Applications** > **Configuration** に移動し、**Create New** をクリックします。**Choose StyleBook** ページには、NetScaler Consoleで使用できるすべてのStyleBookが表示されます。下にスクロールして、**Microsoft Skype for Business 2015 StyleBook** を選択します。StyleBookはユーザーインターフェイスページとして開き、このStyleBookで定義されているすべてのパラメーターの値を入力できます。
2. 「**Edge Server**」セクションで、ネットワーク内のすべてのEdge Serverの仮想IP (VIP) アドレスと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 Server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 Server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 Server 2台と内部Edge Server 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アドレスを入力します。
4. 「**Director Server**」セクションで、Skype for Businessアプリケーション用に作成されるDirectorサーバーの仮想IPアドレス (VIP) を入力します。また、ネットワーク内のすべてのSkype for Business DirectorサーバーのIPアドレスを入力します。高可用性のため、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。

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。

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

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。
自動検出内部ポート	4443	HTTPS	HTTPS（リバースプロキシから）および自動検出サインインのためのHTTPSフロントエンドプール間通信。
RPCポート	135	DCOMおよびリモートプロシージャコール (RPC)	ユーザーの移動、ユーザーレプリケーターの同期、アドレス帳の同期などのDCOMベースの操作に使用されます。
SIPポート	5061	TCP (TLS)	すべての内部SIP通信にフロントエンドサーバーによって使用されます。
SIPフォーカスポート	444	HTTPS、TCP	フォーカス（Skype会議の状態を管理するコンポーネント）と個々のサーバー間のHTTPS通信に使用されます。
SIPグループポート	5071	TCP	応答グループアプリケーションの受信

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

ラベル	ポート	プロトコル	説明
			SIPリクエストに使用されます。
SIPアプリケーション共有ポート	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 Conf Announcement Port`	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 CallPark 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 通話受付ポート	448	TCP	Skype for Business サーバー帯域幅ポリシーサービスによる通話受付制御に使用されます。
SIPコールアドミッションTURNポート	5080	TCP	帯域幅ポリシーサービスによるオーディオ/ビデオエッジTURNトラフィックのコールアドミッション制御に使用されます。

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

ラベル	ポート	プロトコル	説明
SIPオーディオテストポート	5076	TCP	オーディオテストサービスへの着信SIPリクエストに使用されます。
HTTPS外部ポート	443	HTTPS	リモートユーザーアクセス、内部Web会議へのアクセス、および内部メディアとA/Vセッションへのアクセス用のSTUN/TCPインバウンドおよびアウトバウンドメディア通信のための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用のSIP/TLS通信、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用のSIP/MTLS通信の外部ポートに使用されます。
SIP内部リモートアクセスポート	5061	TCP	リモートユーザーアクセスまたはフェデレーション用のSIP/

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

ラベル	ポート	プロトコル	説明
			MTLS通信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の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に流れるIM通信のSIP/MTLS認証用の内部ポートに使用されます。
HTTPポート	80	TCP	ディレクターからWebファームのFQDNへの初期通信に使用されます。
HTTPSポート	443	HTTPS	ディレクターからWebファームのFQDNへの通信に使用されます。
自動検出内部ポート	4443	HTTPS	HTTPS（リバースプロキシから）およびHTTPSディレクターのプール間通信に、自動検出サインインのために使用されます。

© 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。

1. 「**ターゲットインスタンス**」セクションで、3つのSkype for Businessサーバーを展開する3つの異なるNetScalerインスタンスを選択します。

   注

   更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを、このウィンドウの利用可能なインスタンスリストに追加することもできます。

2. 「**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。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、メッセージングサービスを提供する上で重要なエンタープライズアプリケーションです。

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

Microsoft Exchange StyleBookを使用して構成されるNetScaler機能

Microsoft Exchange 2016 StyleBookは、Microsoft Exchange 2016サーバー向けに以下のNetScaler機能を有効にし、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アクセスとクエリの正しい負荷分散仮想サーバーへのリダイレクトを可能にするコンテンツスイッチング
- 書き換え - 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サーバーの展開を模式的に示しています。

Microsoft Exchangeサーバーの展開(/en-us/netscaler-console-service/media/stylebook-exchange-topology-diagram-new.jpg)

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。
- SIPポートがMicrosoft Exchange 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。

Microsoft Exchange スタイルブックの構成

NetScaler構成を展開するために、ビジネスエンタープライズでMicrosoft Exchange StyleBookを構成します。

Microsoft Exchangeアプリケーションを構成するには

1. NetScaler Consoleで、**Applications > Configuration > StyleBooks** に移動します。
2. **Microsoft Exchange 2016 StyleBook** を検索し、**Create Configuration** をクリックします。

   StyleBookは、このStyleBookで定義されているすべてのパラメータ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表示されます。

3. 次のパラメーターの詳細を入力します。

   - **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

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

- **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サーバーIP** - ネットワーク内のすべてのExchangeサーバーのIPアドレス。

  さらにIPアドレスを追加する場合は、プラス (+) アイコンをクリックします。通常、ネットワークには2台のExchangeサーバーが構成されています。

4. **Exchange証明書**セクションで、Exchange証明書をNetScaler Consoleにアップロードします。証明書ファイルとキーファイルの両方の名前を入力し、ローカルストレージからアップロードします。キーファイルを暗号化するための秘密鍵パスワードを提供することもできます。

   注

   証明書ファイルが「.pem」または「.der」形式であることを確認してください。NetScaler Consoleは、他の形式のファイルを拒否します。

   証明書の有効期限の詳細や高度な設定を指定する場合は、**Advanced Certificate Settings** を選択します。

5. **Exchange Active Directory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アプライアンス上で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。
   - **アクティブディレクトリベース文字列** - アクティブディレクトリ内の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ているLDAPグループ属性名。例: LDAPのグループ属性には「memberOf」など。

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

- **Active Directory Sub-Attribute Name** - LDAPサーバーで構成されているLDAPサブ属性名。例: LDAPのサブ属性には「cn」など。
- **アクティブディレクトリ認証ドメイン** - 認証に使用されるAD/LDAPドメイン名。例: ctxnssfb.com。

6. **ターゲットインスタンス**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. **作成**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、最初に**ドライラン**を選択して、実際の構成をインスタンスで実行する前に、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1台、負荷分散仮想サーバー5台、およびLDAP認証仮想サーバー1台にバインドされたLDAPポリシー1つが作成されます。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、高度に構成可能で、すべての主要なブラウザでサポートされています。

Microsoft SharePoint 2016 StyleBook を使用して、ネットワーク内の Microsoft SharePoint 2016 エンタープライズアプリケーションを最適化および保護する NetScaler 構成を展開できます。

前提条件

- マイクロソフト シェアポイント 2016
- NetScaler Console、バージョン 12.0 以降
- NetScaler、バージョン 10.5 以降

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

Microsoft SharePoint 2016 StyleBook によって構成される NetScaler 機能

Microsoft SharePoint 2016 StyleBook を使用して、Microsoft SharePoint 2016 の以下の NetScaler 機能を有効にして構成できます。

- 負荷分散
- コンテンツスイッチング
- レスポンダー
- リライト
- 圧縮
- 統合キャッシュ

ロードバランシング

NetScalerのロードバランシングは、バックエンドのSharePointサーバーにリクエストを均等に分散します。バックエンドサーバーのインテリジェントな監視により、誤動作しているサーバーにリクエストが送信されるのを防ぎます。

SharePoint StyleBookは、ドキュメント、画像、オーディオ、ビデオ、その他のファイルタイプなど、特定の種類のコンテンツに対するリクエストのロードバランシング専用の12個のロードバランシング仮想サーバーを構成します。

NetScaler Console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を選択し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に設定されていることに注意してください。

コンテンツスイッチング

コンテンツスイッチング機能は、要求されたSharePointコンテンツの特定のタイプ（例えば、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、そのタイプのコンテンツを処理できる最適なロードバランシング仮想サーバーに誘導します。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。例えば、ビデオにはテキストドキュメントとは異なる圧縮ポリシーやキャッシュポリシーを使用したい場合があります。

レスポンダー

NetScalerインスタンスのレスポンダー機能は、HTTPからHTTPSへユーザーを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

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

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。例えば、リライトは、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、圧縮します。このプロセスにより、データ伝送時間が改善され、クライアントのネットワーク帯域幅要件が削減され、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遅延の削減、およびサーバーパフォーマンスの向上があります。

統合キャッシュ

NetScalerのインメモリキャッシュは、SharePointオブジェクトを保存して、頻繁に要求されるコンテンツをユーザーに迅速に配信できます。キャッシュされたコンテンツには、ダウンロードされたドキュメント、オーディオ、ビデオ、および画像ファイルが含まれます。

次の図は、NetScaler Consoleを使用してSharePoint StyleBook構成を展開するNetScalerインスタンスによってフロントエンドされたネットワークにおけるSharePointサーバーの展開を図式的に示しています。

SharePointサーバーの展開(/en-us/netscaler-console-service/media/stylebook-sharepoint-topology-new.jpg)

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

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 Consoleで、**Applications** > **Administration** > **Configuration** に移動し、**Create New** をクリックします。

   Choose StyleBook ページには、NetScaler Consoleで使用可能なすべてのStyleBookが表示されます。
2. 下にスクロールして、**Microsoft SharePoint 2016 StyleBook** を選択します。

   注

   NetScaler Consoleで、**Applications** > **Configurations** > **StyleBooks** に移動します。下にスクロールして、**Microsoft SharePoint 2016 StyleBook** を見つけます。**Microsoft SharePoint 2016 StyleBook** パネルで、**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 Application Name**。ネットワークに展開するSharePoint構成の名前。
   b. **SharePoint Virtual IP**。NetScalerインスタンスがMicrosoft SharePointアプリケーションのクライアント要求を受信する仮想IPアドレス。
   c. **SharePoint仮想ポート**。ユーザーがSharePointアプリケーションにアクセスするために使用するTCPポート。
   d. **SharePointフロントエンドプロトコル**。ドロップダウンリストからSharePointフロントエンドプロトコルを選択します。利用可能なオプションはHTTPまたはSSLです。

      注

      SSLを選択した場合は、このStyleBookのSharePoint詳細設定セクションで「リライト設定」パラメーター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。

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

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それぞれのファイルを選択します。

4. オプションで**詳細証明書設定**をクリックして、SSL証明書の有効期限監視を有効または無効にします。証明書の有効期限監視を有効にする場合は、証明書の有効期限が切れるまでの日数を設定すると、その日数後にNetScaler Consoleがアラームを発行します。OCSPチェックをオプション機能または必須機能にするオプションもあります。

5. SharePointの**詳細設定**セクションでは、NetScalerインスタンスで構成されるNetScaler機能を有効にできます。ロードバランシングとコンテンツスイッチング機能はデフォルトでインスタンスに構成されますが、レスポンダー設定、リライト設定、圧縮設定、統合キャッシング設定など、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 Consoleで最近検出されたNetScalerインスタンスを、このウィンドウで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。

ターゲットインスタンス(/en-us/netscaler-console-service/media/nmas-sharepoint-ssl-support-service-4.png)

注

Citrix は、実際の構成を実行する前に、ターゲットインスタンスに作成される構成オブジェクトを確認するために**ドライラン**を選択することを推奨します。

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

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

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 Console 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。**Applications** > **Administration** > **Configuration** に移動し、**View Objects Created** をクリックします。次の図は、「NetScaler Console から SharePoint StyleBook 構成を展開する」の例で指定された 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。

インスタンスに作成されたSharePointオブジェクト(/en-us/netscaler-console-service/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ベースの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。クラウドベースのリソースの一例として、Office 365があります。ADFSプロキシサーバーの目的は、インターネットからアクセスできないADFSサーバーへの要求を受信して転送することです。ADFSプロキシはリバースプロキシであり、通常、組織の境界ネットワーク（DMZ）に配置されます。ADFSプロキシは、リモートユーザーの接続性とアプリケーションアクセスにおいて重要な役割を果たします。

NetScalerは、セキュアな接続性、認証、およびフェデレーションIDの処理を可能にする正確なテクノロジーを備えています。NetScalerをADFSプロキシとして使用することで、DMZに追加のコンポーネントをデプロイする必要がなくなります。

NetScaler ConsoleのMicrosoft ADFSプロキシStyleBookを使用すると、NetScalerインスタンス上にADFSプロキシサーバーを構成できます。

次の図は、NetScalerインスタンスをエンタープライズDMZ内のADFSプロキシサーバーとして展開する様子を示しています。

NetScalerインスタンスをADFSプロキシとして展開する(/en-us/netscaler-console-service/media/nmas-adfs-proxy-stylebooks-1.png)

NetScalerをADFSプロキシとして使用する利点

1. ロードバランシングとADFSプロキシの両方のニーズに対応
2. 内部および外部ユーザーアクセスの両方のシナリオをサポート
3. 豊富な事前認証方法をサポート

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

4. ユーザーにシングルサインオンエクスペリエンスを提供
5. アクティブプロトコルとパッシブプロトコルの両方をサポート
    a. アクティブプロトコルアプリの例：Microsoft Outlook、Microsoft Skype for Business
    b. パッシブプロトコルアプリの例：Microsoft Outlook Web App、Webブラウザ
6. DMZベースの展開向けに強化されたデバイス
7. 追加のNetScalerコア機能を使用することで価値を付加します
    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、Office 365にトークンを送信してクライアントアクセスを提供します。

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、後に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ようにNetScalerを設定する方法について説明します。

構成の詳細

以下の表に、この統合を正常に展開するために必要な最小ソフトウェアバージョンを示します。

製品	最小要件バージョン
NetScaler	11.0、Advanced/Premiumライセンス

© 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。

NetScaler Console から Microsoft ADFS プロキシ StyleBook 構成を展開する

以下の手順は、ビジネスネットワークで Microsoft ADFS プロキシ StyleBook を実装する際に役立ちます。

Microsoft ADFS プロキシ StyleBook を展開するには

1. NetScaler Console で、**Applications > Configuration > StyleBooks** に移動します。**StyleBooks** ページには、NetScaler Console で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 プロキシ StyleBook** を見つけます。**Create Configuration** をクリックします。 StyleBook はユーザーインターフェイスページとして開き、この StyleBook で定義されているすべてのパラメーターの値を入力できます。
3. 次のパラメーターの値を入力します。

   a. **ADFS プロキシ展開名**。ネットワークに展開される ADFS プロキシ構成の名前を選択します。

   b. **ADFS サーバーの FQDN または IP**。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 プロキシパブリック 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。

   ADFS パラメーターを指定する (/en-us/netscaler-console-service/media/nmas-adfs-proxy-stylebooks-2.png)
4. **ADFS プロキシ証明書**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該当するファイルを選択します。.pem 形式の暗号化された秘密キーをロードするために、秘密キーパスワードを入力することもできます。

   ADFS プロキシ証明書を指定する (/en-us/netscaler-console-service/media/nmas-adfs-proxy-stylebooks-3.png)

   「**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。

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

5. オプションで、SSL証明書がNetScalerにCA公開証明書をインストールする必要がある場合は、「**SSL CA Certificate**」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、以下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 Proxy Active Authentication VIP**。アクティブクライアントが認証のためにリダイレクトされるNetScalerインスタンス上の仮想認証サーバーの仮想IPアドレスを入力します。
   b. **Service Account Username**。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. **Service Account Password**。NetScalerがユーザーをActive Directoryに認証するために使用するパスワードを入力します。

8. 対応するオプションを有効にし、LDAP設定を構成することで、パッシブクライアントの認証を設定します。

   注

   パッシブクライアントのサポートを設定することはオプションです。

   パッシブクライアントの認証を有効にするには、以下の詳細を入力します。

   a. **LDAP (Active Directory) Base**。認証を許可するために、Active Directory (AD) 内で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`」

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

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名を入力します。」.

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**。ユーザー名を「sAMAccountName」として入力します。」

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サーバー用のDNS VIPを構成することもできます。」.

「

」

10. 「**ターゲットインスタンス**をクリックし、このMicrosoft ADFSプロキシ構成を展開するNetScalerインスタンスを選択します。**作成**をクリックして構成を作成し、選択したNetScalerインスタンスに構成を展開します。」.

「

」

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

注

Citrixでは、実際の構成を実行する前に、**ドライラン**を選択することをお勧めします。まず、StyleBookによってターゲットのNetScalerインスタンスに作成される構成オブジェクトを表示できます。その後、**作成**をクリックして、選択したインスタンスに構成を展開できます。

作成されたオブジェクト

NetScalerインスタンスにADFSプロキシ構成が展開されると、いくつかの構成オブジェクトが作成されます。次の図は、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 スタイルブック

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。

- 企業資源計画 (ERP)
- 顧客関係管理 (CRM)
- サプライチェーン管理 (SCM)

これらのコンピュータアプリケーションは、Oracleによって開発または買収されたものです。Oracle E-Business Suite 12.2 StyleBookを使用すると、選択したNetScalerインスタンスに構成を展開できます。

このStyleBookは、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 Consoleで、**アプリケーション > 構成 > StyleBooks**に移動します。**StyleBooks**ページには、NetScaler Consoleで利用可能なすべてのStyleBookが表示されます。下にスクロールして、**Oracle E-Business Suite 12.2**を選択します。検索オプションを使用してStyleBookを検索することもできます。
2. StyleBookパネルで**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。ここにはHTTPとHTTPS/SSLの2つのオプションがあります。ポート番号を入力することもできます。
5. 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。**+**をクリックして、さらにサーバーIPアドレスを追加します。
6. **SSL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のNetScalerインスタンスを選択し、**作成**をクリックします。

   Oracle構成パック(/en-us/netscaler-console-service/media/nmas-oracle-e-business-stylebook.png)

   ヒント

   更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスをこのウィンドウで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NetScaler Consoleでのみ利用可能です。

カスタムStyleBookの作成と使用

展開用の独自のStyleBookを作成し、NetScaler Consoleにインポートして、構成オブジェクトを作成できます。APIを使用して、StyleBookから構成を作成することもできます。

このドキュメントには、次の情報が含まれています。

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

開始する前に

StyleBookの作成を開始する前に、次の知識があることを確認してください。

- NITRO API。詳細については、NITRO APIドキュメントを参照してください。
- YAML

StyleBookファイルはYAML形式を使用します。YAML形式の詳細については、YAML構文を参照してください。

StyleBookを作成する際に注意すべきYAMLガイドラインのリストを次に示します。

- YAMLは大文字と小文字を区別します。
- 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）がある場合にのみ、文字列を引用符で囲んでください。数値を文字列として解釈したい場合は、数値を引用符で囲むか、StyleBookのstr()組み込み関数を使用してください。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off、TRUE/true/truthy/FALSE/False/false/falselyのようなリテラルはブール値と見なされ、それぞれtrueとfalseに相当します。これらを文字列として解釈するには、引用符で囲んでください。例：
  - "YES"
  - 「いいえ」
  - 「真」
  - 「False」など。

注

NetScaler Console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推奨しています。

詳細については、NITRO APIドキュメントを参照してください。

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

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。一般的な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から参照したい他のStyleBookを宣言します。StyleBookを作成するには、NetScaler NITRO構成StyleBookまたは他のStyleBookをインポートする必要があります。これは必須セクションです。
- **パラメーター**: このセクションでは、構成を作成するためにStyleBookで必要となるパラメーターを定義します。StyleBookが受け取る入力を記述します。これはオプションのセクションです。
- **コンポーネント**: このセクションでは、特定の構成のためにStyleBookによって作成されるエンティティ（構成オブジェクト）を定義します。このセクションはStyleBookの核と見なされます。コンポーネントは通常、パラメーターセクションで提供される入力を使用して、StyleBookによって生成される構成を調整します。これはオプションのセクションです。StyleBookには、パラメーターセクション、コンポーネントセクション、またはその両方を含めることができます。パラメーターセクションのみを持つStyleBookは、他のStyleBookで使用できるパラメーターのリストを定義するのに役立ちます。これにより、StyleBookのセット全体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内の属性の値を指定したい場合に使用できます。
- **出力**: パラメーターセクションがStyleBookの入力を定義するのに対し、このオプションのセクションはその出力を定義します。このオプションの出力セクションでは、このStyleBookから構成を作成するユーザーや、このStyleBookをインポートする他のStyleBookに公開したいコンポーネントを指定できます。ユーザーやインポートする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るようになります。
- **操作**: StyleBookには、StyleBookの一部である仮想サーバーでNetScaler ConsoleのAnalyticsを有効にするためのオプションセクションを含めることができます。

次の図は、StyleBookの簡単な概要を示しています。

StyleBookの概要(/en-us/netscaler-console-service/media/stylebook-outline.png)

以下の例は、StyleBookの文法と構造、および複雑さのレベルを上げてStyleBookを作成する方法を学ぶのに役立ちます。

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

- 負荷分散仮想サーバーを作成するためのStyleBook(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks/create-load-balancing-virtual-server.html)
- 基本的な負荷分散構成を作成するためのStyleBook(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks/create-basic-load-balancing-configuration.html)
- 複合StyleBookを作成する(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks/create-composite-stylebook.html)
- GUI属性を使用してStyleBookをカスタマイズする(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks/use-gui-attributes.html)

構成パックの作成と編集

NetScaler Consoleでは、StyleBookから構成パックを作成できます。構成パックは、作成元のStyleBookに紐付けられます。構成パックへの更新は、紐付けられているStyleBookを通じて行われます。

構成パックの作成

StyleBookから構成パックを作成するには、次の手順を実行します。

1. **アプリケーション > 設定 > 設定パック** に移動します。
2. **Add** をクリックします。
3. **Choose StyleBooks** で、構成パックを作成するStyleBookを選択します。

   このページでは、StyleBookがデフォルト、エンタープライズ、カスタムStyleBookに分類されています。それぞれのタブを選択して、必要なStyleBookを見つけます。
4. オプションで、構成パックに一意の **Config Key** を指定します。このキーは、この構成パックの **Display Key** として表示されます。

   - 既存の **Config Key** を指定した場合、NetScaler Consoleは構成パックを作成できません。
   - **Config Key** を指定しない場合、NetScaler Consoleは自動的に **Configpack ID** を割り当てます。ただし、この値は **Display Key** として表示されません。
   - **Config Key** を指定せず、いずれかのStyleBookパラメーターに `key` 属性が設定されている場合、そのパラメーター値が **Display Key** として表示されます。詳細については、「Parameters」を参照してください。
5. 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によって異なります。

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

6. **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。

   注記:

   必要な数のターゲットインスタンスを指定することで、複数のNetScalerに構成を展開できます。

7. **ドライラン**をクリックします。

   オブジェクトページには、NetScalerインスタンスで作成、変更、または削除されるオブジェクトが表示されます。

8. **作成**をクリックします

   構成パックは、**StyleBook > 構成**ページに表示されます。

既存の構成パックを編集する場合は、構成パックを選択して**編集**をクリックします。

StyleBookの外部で作成された構成を再利用し、ConfigPack間で構成を共有する

特定の運用上のニーズやレガシーな設定により、Stylebookの外部でNetScaler®構成を作成したことがあるかもしれません。これらの既存の構成をStylebook構成パックの一部として統合および管理できるようになり、より柔軟で一元的な管理が可能になります。

たとえば、この機能が導入される前は、NetScalerにすでにSSLプロファイルが構成されており、StyleBookの構成パック操作が同じ名前のSSLプロファイルを作成しようとすると、「リソースがすでに存在します」というエラーで構成パック操作が失敗していました。この機能が有効になったことで、構成パック操作は成功し、同じ名前の既存のSSLプロファイルを新しい構成パックで再利用できるようになりました。

同様に、ネットワーク設定、セキュリティポリシー、アプリケーション構成の一部などのリソースが複数のアプリケーションまたは構成で必要となるシナリオに直面することもあります。この機能により、複数の構成パック間で構成を共有できます。

この機能を有効にするには、次の手順に従います。

1. **アプリケーション > 構成 > Stylebooks**に移動します。
2. **Stylebooks**ページで、新しい構成パックの作成に使用するStylebook、または編集中の構成パックに関連付けられているStylebookを選択します。
3. **アクションの選択**で、**設定の構成**をクリックします。

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

4. 次のいずれかまたは両方のオプションを選択して、設定を調整します。

   - 構成の作成時にNetScaler上の既存のリソースを再利用できるようにするには、**構成の作成時にNetScaler上の既存のリソースの再利用を許可する**オプションを選択します。
   - 構成の削除時にNetScaler上の再利用されたリソースを保持するには、**構成の削除時にNetScaler上の再利用されたリソースを保持しますか？**オプションを選択します。このオプションは、それらを参照する最後の構成パックが削除された場合でも、StyleBookの外部でNetScaler上に元々作成されたリソースを保持し、それらの継続的な可用性を保証します。

5. **OK** をクリックします。

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既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。

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StyleBook **example-lb** の例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するには、新しいStyleBookが必要です。そのためには、基本的なロードバランサー構成とともにモニターを構成する機能を含む **example-lb-mon** StyleBookを作成します。

StyleBookを作成したら、既存の構成パックCP1を更新してモニターを追加します。構成パックを更新するには、次の手順を実行します。

1. **アプリケーション > 設定 > 設定パック** に移動します。
2. 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。

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

構成パックの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。そうでない場合、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。

注:

StyleBook Compatibilityページには、パラメータの違いが表示されます。このページは、StyleBookを変更するか、既存のStyleBookを継続するかを決定するのに役立ちます。StyleBookを変更する場合は、変更内容を確認してから**Next**をクリックします。

新しいStyleBookに新しいパラメータが追加された場合、StyleBookの変更後、それらのパラメータの値を手動で指定する必要があります。

この例では、**example-lb** StyleBookの構成ページに表示されるパラメータは次のとおりです。

ロードバランシング構成パックの例](/en-us/netscaler-console-service/media/nmas-migrate-configpack-3.png)

新しい**example-lb-mon** StyleBookの構成ページに表示されるパラメータは次のとおりです。

構成パック移行後のパラメータの例](/en-us/netscaler-console-service/media/nmas-migrate-configpack-4.png)

この場合、新しいStyleBookは既存のパラメータを変更していないため、StyleBookは基本的なロードバランサー構成の古い値を保持します。そして、新しいパラメータのみを追加します。モニターパラメータについては、必要な値を手動で指定してください。

6. **ターゲットインスタンス**で、選択したインスタンスを確認し、必要に応じてリストを更新します。
7. **Dry Run**をクリックします。

   オブジェクトページには、NetScalerインスタンスで作成、変更、または削除されるオブジェクトが表示されます。
8. 「**OK**」をクリックします。

   「**StyleBook > Configurations**」ページで、「**StyleBook Name**」列に、選択した構成パックの新しいStyleBook名が表示されます。この場合、「**example-lb-mon**」と表示されます。

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

複数の構成パックを持つStyleBookを変更する

複数の構成パックを持つ既存のStyleBookを変更する場合は、次の手順を実行します。

1. NetScaler Consoleに新しいStyleBookをインポートします。

   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。

   「**Change StyleBook**」を選択できるのは、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です。

   選択した構成パックの場合、次の条件が満たされたときに、NetScaler Consoleは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、「**Configurations**」ページで「**Configurations in Progress/Failed**」を選択します。

3. すべての構成パックが新しいStyleBookに紐付けられたら、NetScaler Consoleから古いStyleBookを削除します。

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NetScaler Console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。

設定のエクスポート

設定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. **アプリケーション > 設定 > 設定パック** に移動します。
2. エクスポートする設定パックを選択します。
3. **Select Action** で、**Export Configuration** を選択します。

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

エクスポート設定オプション(/en-us/netscaler-console-service/media/export-configuration-pack.png)

4. **Export Configuration** ペインで、以下を指定します。

   - **設定が展開されているターゲットインスタンス情報**: 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。
   - **設定に関連付けられたStyleBook**: このオプションを選択すると、StyleBookがエクスポートバンドルに含まれます。
   - **エクスポート設定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、設定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。

   設定パックのエクスポート(/en-us/netscaler-console-service/media/export-configuration-options.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。

設定のインポート

ローカルコンピューターから別のNetScaler Console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. **アプリケーション > 構成 > 設定パック**」に移動します。
2. **Import Configuration** を選択します。
3. コンピューターからインポートファイルバンドルを選択します。
4. エクスポート時に指定したパスフレーズを使用します。
5. オプションで、詳細オプションで「**すべての設定オブジェクトがNetScalerに既に存在する場合にのみ、新しい構成の作成を許可する**」を選択します。

   このオプションは、NetScalerインスタンスにすでに作成されているオブジェクトを変更しません。

   2つのNetScaler Consoleサーバーに同じNetScalerインスタンスを追加したとします。そして、あるNetScaler Consoleサーバーから別のサーバーに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、NetScaler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。

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

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. **Import** をクリックします。

構成パックをインポートすると、NetScaler Consoleは次のことを検証します。

- **関連付けられたStyleBook**: 関連付けられたStyleBookがNetScaler Consoleにない場合、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。記載されているNetScalerインスタンスがNetScaler Consoleに存在しない場合、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NetScaler Console**: 同じNetScaler Console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。

構成パックを下書きとして保存する

構成パックの**下書きとして保存**オプションを使用すると、構成の変更を下書きとして保存できます。この機能により、変更をNetScalerインスタンスにすぐに展開することなく保存できます。

構成パックを下書きとして保存するには、次の手順に従います。

1. **アプリケーション > 設定 > 設定パック** に移動します。
2. **Configurations**ページで、**Add**をクリックします。
3. 目的のスタイルブックを選択し、**Select**をクリックします。
4. **Create Configuration**ページで、**Save as Draft**をクリックします。

構成パックが下書きとして保存されると、構成の変更はNetScalerインスタンスに直接展開されません。代わりに、構成パックは**Pending Configurations**の下の**Draft Configurations**タブに下書きとして保存されます。

Draft Configurationsタブで、構成パックを選択して次の操作を実行します。

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

- 下書きの構成を編集します。
- 構成をNetScalerインスタンスに展開します。
- 下書きを削除します。

ドラフト構成(/en-us/netscaler-console-service/media/draft-config.png)

保存したドラフトをいつ展開するかをスケジュールすることもできます。

詳細については、「設定パックのスケジュールを作成する」(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks/edit-configpack.html#create-a-schedule-for-a-config-pack)を参照してください。

設定パックのスケジュールを作成する

設定パックを作成すると、設定パックはデフォルトでNetScalerインスタンスに自動的に展開されます。この機能を使用すると、設定パックの展開をスケジュールできます。

設定パックのスケジュールを作成するには、次の手順に従います。

1. **アプリケーション > 設定 > 設定パック** に移動します。
2. **Configurations** ページで、**Add** をクリックします。
3. StyleBook を選択し、**Select** をクリックします。
4. **Create Configuration** ページの **Execution** で、**Execution Mode** リストから **Later** を選択します。
5. スケジュールする希望の日時を選択し、**Submit** をクリックします。

実行モード(/en-us/netscaler-console-service/media/execution-mode.png)

スケジュールされたすべての構成は、**Pending Configurations** の下の **Scheduled configurations** タブに保存されます。作成されたスケジュールを選択して、構成パラメータを編集したり、スケジュールを展開またはキャンセルしたりできます。

注:

スケジュールされた設定パックを展開すると、スケジュールがキャンセルされ、構成がすぐに実行されます。

スケジュール済み構成(/en-us/netscaler-console-service/media/scheduled-config.png)

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

展開済みの構成パックの場合

展開済みの構成パックを編集および削除するためのスケジュールを作成することもできます。

構成パックの編集操作をスケジュールする

展開済みの構成パックを編集するためのスケジュールを作成するには、次の手順に従います。

1. 「**Applications > Configuration > Config Packs**」の順に移動します。
2. **Configurations** ページで、StyleBook を選択し、**Edit** をクリックします。
3. **Edit Configuration** ページで、構成パックを編集します。
4. **Execution Mode** リストで、**Later** を選択します。
5. スケジュールする希望の時間と日付を選択し、**Submit** をクリックします。

構成パックの削除操作をスケジュールする

展開済みの構成パックを削除するためのスケジュールを作成するには、次の手順に従います。

1. 「**Applications > Configuration > Config Packs**」の順に移動します。
2. **Configurations** ページで、StyleBook を選択し、**Delete** をクリックします。
3. **Execution Mode** リストで、**Later** を選択します。
4. スケジュール設定に必要な日時を選択し、**OK**をクリックします。

設定パックのスケジュールを削除(/en-us/netscaler-console-service/media/delete-config-pack.png)

設定パックからターゲットインスタンスをデタッチする

設定パックからターゲットインスタンスをデタッチするには、次の手順を実行します。

1. **アプリケーション > 設定 > 設定パック**に移動します。
2. 削除するターゲットインスタンスを含む設定パックを選択します。
3. **Select Action**で、**Detach Targets**を選択します。
4. **Detach Targets**ペインで、設定パックから削除するターゲットインスタンスを選択します。

   ターゲットのデタッチ(/en-us/netscaler-console-service/media/stylebooks-detach-target.png)
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、重複する設定パックの作成を確認するメッセージが表示されます。

StyleBookを作成する

example-lb StyleBookの全内容を参考として以下に示します。

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

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

example-lb-mon StyleBookの全内容を参考として以下に示します。

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

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

  -

    namespace: com.citrix.adc.commontypes

    prefix: cmtypes

    version: "1.0"

parameters-default-sources:

  - stlb::lb
```

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

```
parameters:

  -

    name: monitors

    label: "List of Monitors"

    description: "List of Monitors to monitor Application Servers"

    type: cmtypes::monitor[]

substitutions:

  mon-name(appname, monname): $appname + "-mon-" + $monname

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon
```

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

```
    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

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各パラメータは、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で構成されます。この例では、ヘッダーセクションは次のように記述されています。

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

```
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"
```

ヘッダーセクションには、以下の詳細が含まれます。

- **name**: このStyleBookの名前。
- **description**: このStyleBookが何をするかを定義する説明。この説明はNetScaler Consoleに表示されます。
- **display-name**: NetScaler Consoleに表示されるStyleBookの記述的な名前。
- **namespace**: 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。
- **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 Consoleでは、名前、名前空間、およびバージョンの組み合わせが同じ2つのStyleBookを持つことはできません。ただし、同じ名前とバージョンで異なる名前空間を持つ2つのStyleBook、または同じ名前空間とバージョンで異なる名前を持つ2つの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、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でもバージョン番号を更新してください。

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

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:

 -

  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に基づいている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には、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）でNITRO 10.5名前空間をインポートすることを推奨します。

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

他のStyleBookをインポートするStyleBookは、インポートするStyleBookと同じかそれ以上のNITROバージョンに基づいている必要があります。たとえば、NITROバージョン10.5に基づいているStyleBookは、11.1に基づいている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に基づいているStyleBookは、11.1より前の任意のバージョンに基づいている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バージョンを取得します。そして、そのバージョン以降のNetScalerを構成するために使用されます。

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のユーザーに指定してもらいたい入力内容を決定する必要があります。この例では、仮想サーバーの名前、そのIPアドレス、および負荷分散方法をユーザー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

  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"
```

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

```
  type: ipaddress
  required: true
-
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION
```

注

パラメータのラベルを指定しない場合、NetScaler Console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 Console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つのパラメーターを宣言しました。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** は、これらのパラメーターが取りうる値の型を指します。たとえば、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 のパラメーターは、以下のいずれかの組み込み型にすることができます。
- **string**: 文字の配列です。長さが指定されていない場合、文字列値は任意の数の文字を取ることができます。ただし、min-length および max-length 属性を使用することで、文字列型の長さを制限できます。

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

- **number**: 整数です。min-value および 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 のいずれかです。また、すべてのリテラルは YAML によってブール値と見なされることに注意してください (例: Yes または No)。
- **ipaddress**: 有効な IPv4 または IPv6 アドレスを表す文字列です。
- **tcp-port**: TCP または UDP ポートを表す、0 から 65535 までの数値です。
- **password**: 不透明な/秘密の文字列値です。NetScaler Console がこのパラメーターの値を表示する場合、アスタリスク (*****) で表示されます。
- **certfile**: 証明書ファイルです。
- **keyfile**: 証明書秘密鍵ファイルです。
- **file**: この型のパラメーターは、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必要があります。
- **object**: 複数の要素で構成され、これらの各要素がパラメーターです。この型は、複数の関連するパラメーターを1つの親パラメーターの下にグループ化するために使用できます。
- **required**: パラメーターが必須かオプションかを示します。true に設定されている場合、そのパラメーターは必須であり、この StyleBook を使用して構成を作成する際に、ユーザーはこのパラメーターの値を指定する必要があります。デフォルトでは、すべてのパラメーターはオプションです。この例では、**name** と **ip** は必須パラメーターですが、**lb-alg** はオプションパラメーターであり、そのデフォルト値は「ROUNDROBIN」です。

オプションパラメーターにデフォルト値を割り当てるには、**default** 属性を使用します。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。たとえば、**lb-alg** パラメーターの場合、デフォルト値は ROUNDROBIN です。

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するには、**allowed-values** 属性を使用します。この例では、**lb-alg** パラメーターに ROUNDROBIN と LEASTCONNECTION の2つの値を指定しました。

StyleBookをインポートして使用すると、NetScaler Consoleにこれら3つのパラメータを含むフォームが表示されます。名前とIPに表示されるフィールドには、文字列と`ipaddress`型の値を入力でき、`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。

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

注

組み込み型に加えて、パラメータは別のStyleBookをその型として持つことができます。これは、他のStyleBookで定義されたパラメータを再利用する方法です。

コンポーネント

このStyleBookの最後のセクションはコンポーネントセクションと呼ばれ、StyleBookの中で最も重要なセクションと見なされます。このセクションでは、StyleBookによって作成される構成オブジェクトを定義します。

この例では、コンポーネントセクションを次のように記述する必要があります。

```
components:

 -

  name: lbvserver-comp

  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler lbvserver configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

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、名前、タイプ、プロパティです。コンポーネントのタイプは、このコンポーネントが提供するプロパティを決定します。コンポーネントには次の2種類があります。

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

- **組み込み型**: このタイプはシステムによって提供され、定義する必要はありません。たとえば、NITROエンティティタイプ`lbvserver`または`servicegroup`などです。この例では、組み込みコンポーネントタイプを使用しています。
- **複合型**: このタイプは、作成してNetScaler ConsoleにインポートしたStyleBook、またはNetScaler Consoleに付属しているデフォルトのStyleBookです。複合StyleBookの作成で複合StyleBookについて詳しく学ぶことができます。

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**タイプ（組み込みのNITROタイプ）です。「ns」は、import-stylebooksセクションで指定した名前空間netscaler.nitro.configおよびバージョン10.5を参照するプレフィックスであり、`lbvserver`はこの名前空間内の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。

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`とポートに静的な値を指定していますが、名前、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

慣例により、プレフィックス「ns」は「import-stylebooks」セクションでNetScaler NITRO名前空間を指定するために常に使用されます。必須ではありませんが、Citrixは一貫性のために独自のStyleBookで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、それらをすべてまとめて、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。

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

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

 -

  namespace: com.citrix.adc.stylebooks

  version: "1.0"

  prefix: stlb



parameters:

 -

  name: name

  label: "Application Name"
```

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

```
   description: "Give a name to the application configuration."
   type: string
   required: true
  -
   name: vip-ipaddress
   label: "Load Balancer IP Address"
   description: "The Application VIP that clients access"
   type: ipaddress
   required: true
  -
   name: lb-alg
   label: LB Algorithm
   description: Load Balancing Algorithm
   type: string
   default: ROUNDROBIN
   allowed-values:
    - ROUNDROBIN
    - LEAST-CONNECTION


components:
 -
   name: lbvserver-comp
```

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

```
  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler lbvserver configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

StyleBookを使用して構成を作成するには、NetScaler Consoleにインポートしてから使用する必要があります。詳細については、「ユーザー定義StyleBookの使用方法」を参照してください。

このStyleBookを他のStyleBookにインポートすることもできます（import-stylebooksコンストラクトを使用）。または、次のセクションで説明するように、このStyleBookを修正して、より多くのパラメータとコンポーネントを含めることもできます。

基本的なロードバランシング構成を作成するためのStyleBook

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を含むロードバランシング構成を作成するStyleBookを設計します。StyleBookは、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。

基本的なロードバランシング構成を作成するには、ロードバランシング仮想サーバーを作成するためのStyleBookで作成したサンプルStyleBook **lb-vserver** を使用し、**basic-lb-config.yaml** として保存します。

ヘッダー

このStyleBookを構築するには、ヘッダーセクションを更新します。このセクションは、ロードバランシング仮想サーバーを作成するためのStyleBookで作成したヘッダーセクションと似ています。

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

name の値を basic-lb-config に変更します。**description** と **display-name** を更新して、StyleBook を説明します。**namespace** と **version** の値を変更する必要はありません。名前を変更したため、このStyleBookの一意の識別子がシステムに作成されます。

```
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"
```

StyleBookのインポート

import-stylebooksセクションは変更されません。これは、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。

```
import-stylebooks:

 -

 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

パラメータ

パラメータセクションを更新して、さらに2つのパラメータを追加します。

パラメータは、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します。最初の3つのパラメータ `name`、`ip`、および `lb-alg` は変更されません。

```
parameters:

 -
```

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

```
  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true

 -

  name: 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

 -
```

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

```
  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true

 -

  name: svc-port

  type: tcp-port

  label: Server Port

  description: The TCP port open on the application servers to receive
requests.

  default: 80
```

アプリケーションのバックエンドサーバーのIPアドレスのリストを受け入れるために、パラメータ **svc-servers** が追加されます。**svc-servers** は、**required: true** で示されるように必須パラメータです。

2番目のパラメータ **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限り、デフォルトのポート番号は80です。

コンポーネント

また、コンポーネントセクションを更新して、2つの新しいパラメータを使用し、完全なロードバランシング構成を構築するように、より多く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
```

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

```
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg


components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP


  components:
    -
      name: lbvserver-svg-binding-comp
      type: ns::lbvserver_servicegroup_binding
      properties:
          name: $parent.parent.properties.name
```

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

```
        servicegroupname: $parent.properties.name

  -

    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv

    properties:

       ip: $srv

       port: str($parameters.svc-port)

       servicegroupname: $parent.properties.name
```

この例では、元のコンポーネント **lbvserver-comp** (前の例から) に、**svcg-comp** という子コンポーネントがあります。**svcg-comp** コンポーネントには、さらに2つの子コンポーネントが含まれています。コンポーネントを別のコンポーネント内にネストすると、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` の属性に指定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ていますが、**name** 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ているパラメータ **name** を、**$parameters.name + "-svcgrp"** という表記を使用して参照します。ここで、「**-svcgrp**」はユーザー定義の名前に付加（連結）されます。

コンポーネント **svcg-comp** には、**lbvserver-svg-binding-comp** と **members-svcg-comp** の2つの子コンポーネントがあります。

最初の子コンポーネントである **lbvserver-svg-binding-comp** は、その親コンポーネントによって作成されたサービスグループと、親の親コンポーネントによって作成された負荷分散仮想サーバー (`lbvserver`) と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

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

（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。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と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。バインディング構成オブジェクトの作成は、StyleBookの **repeat** 構造を使用して、パラメータ **svc-servers** で指定されたサーバーリストを反復処理することによって実現されます。反復処理中に、このStyleBookコンポーネントは、サービスグループ内の各サービス（**repeat-item** 構造では `srv` と呼ばれます）に対して **servicegroup_servicegroupmember_binding** 型のNITRO構成オブジェクトを作成し、各NITRO構成オブジェクトの **ip** 属性を対応するサーバーのIPアドレスに設定します。

一般に、コンポーネントで **repeat** および **repeat-item** 構造を使用すると、そのコンポーネントが同じタイプの複数の構成オブジェクトを構築できるようになります。**repeat-item** 構造に変数名（例: `srv`）を割り当てて、反復処理中の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または子コンポーネントのプロパティで **`$<varname>`** として参照されます（例: $srv）。

上記の例では、コンポーネントのネストが構成の構築を容易にしています。次の例に示すように、ネストせずに構成を構築することもできます。

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP

   ipv46: $parameters.ip

   port: 80

   lbmethod: $parameters.lb-alg
```

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

```
-
 name: svcg-comp
 type: ns::servicegroup
 properties:
   servicegroupname: $parameters.name + "-svcgrp"
   servicetype: HTTP
-
 name: lbvserver-svg-binding-comp
 type: ns::lbvserver_servicegroup_binding
 properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.servicegroupname
-
 name: members-svcg-comp
 type: ns::servicegroup_servicegroupmember_binding
 repeat: $parameters.svc-servers
 repeat-item: srv
 properties:
  ip: $srv
  port: 80
  servicegroupname: $components.svcg-comp.properties.servicegroupname
```

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

ここでは、コンポーネントはネストされていませんが、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。

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` 文字列を接尾辞として付けることです。

出力

このセクションでは、StyleBookが構成を作成した後にユーザー（または他のStyleBook）に公開するものを指定する必要があります。たとえば、このStyleBookによって作成された `lbvserver` および `servicegroup` 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
```

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

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、このStyleBookをインポートするStyleBookはより柔軟になります。この機能は、複合StyleBookを作成する場合に役立ちます。

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が推奨されます (例えば、名前だけではなく、**$components.lbvserver-comp.properties.name**ではなく、**$components.lbvserver-comp**全体を公開します)。また、特定の出力が何を表しているかを説明する記述を出力に追加してください。

StyleBookを構築する

このStyleBookの必要なセクションをすべて定義したので、それらをすべて組み合わせて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、StyleBook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ます。

ファイル**basic-lb-config.yaml**の全コンテンツ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
```

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

```
  version: "10.5"

  prefix: ns

parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true

 -

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:
```

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

```
      - ROUNDROBIN

      - LEASTCONNECTION

    default: ROUNDROBIN

  -

    name: svc-servers

    type: ipaddress[]

    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true

  -

    name: svc-port

    type: tcp-port

    label: Server Port

    description: The TCP port open on the application servers to receive
requests.

    default: 80



components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:
```

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

```
    name: $parameters.name + "-lb"
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
  -
   name: svcg-comp
   type: ns::servicegroup
   properties:
     servicegroupname: $parameters.name + "-svcgrp"
     servicetype: HTTP
  -
   name: lbvserver-svg-binding-comp
   type: ns::lbvserver_servicegroup_binding
   properties:
    name: $components.lbvserver-comp.properties.name
    servicegroupname: $components.svcg-comp.properties.servicegroupname
  -
   name: members-svcg-comp
   type: ns::servicegroup_servicegroupmember_binding
   repeat: $parameters.svc-servers
   repeat-item: srv
```

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

```
  properties:

   ip: $srv

   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname



outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

StyleBookを使用して構成を作成するには、NetScaler Consoleにインポートしてから使用する必要があります。詳細については、「ユーザー定義StyleBookの使用方法」を参照してください。

このStyleBookを他のStyleBookにインポートし、次のセクションで説明されてい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。

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

たとえば、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

   version: "10.5"

   prefix: ns

  -

   namespace: com.example.stylebooks

   version: "0.1"

   prefix: stlb

parameters:

  -
```

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

```
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true


  -
    name: response-code
    type: string[]
    label: List of Response Codes
```

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

```
    description: List of Response Codes - Provide a list of response codes
in integer.



components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config

    description: This component's type is another StyleBook that builds
the NetScaler lbvserver, servicegroups and services configuration objects.

    properties:

     name: $parameters.name

     ip: $parameters.ip

     svc-servers: $parameters.svc-servers

  -

     name: monit-comp

     type: ns::lbmonitor

     description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.

     properties:

       monitorname: $parameters.name + "-mon"

       type: HTTP

       respcode: $parameters.response-code

       httprequest: "'GET /'"
```

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

```
        lrtm: ENABLED

        secure: "YES"



      components:

         -

           name: monit-svcgrp-bind-comp

           type: ns::servicegroup_lbmonitor_binding

           properties:

             servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname

             monitor_name: $parent.properties.monitorname
```

import-stylebooksセクションでは、basic-lb-config StyleBookをその名前空間とバージョンを使用してインポートします。これはプレフィックス`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、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、これらすべてをコンポーネントとして実行するStyleBookをインポートし、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`servicegroup`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`servicegroup`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、それ以外ではアクセスできなかっ

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

たインポートされたStyleBook内のコンポーネントにアクセスするために、outputsセクションをどのように使用できるかを示す例です。

次に、StyleBookの内容をテキストエディターにコピーして貼り付け、ファイルを**composite-example.yaml**として保存します。NetScaler Consoleにファイルをインポートする前に、YAMLコンテンツを検証してください。その後、NetScaler Consoleにインポートし、このStyleBookを使用して1つまたは複数の構成を作成します。

Citrixでは、StyleBookに組み込まれているYAMLバリデーターを使用してYAMLコンテンツを検証およびインポートすることをお勧めします。

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 Consoleに表示されるときにフィールドが直感的になります。

パラメータにツールチップ付きのラベルを追加する

label属性を使用して、パラメータに説明的な名前を追加できます。description属性を使用して、このパラメータにツールチップを追加します。

例:

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.

type: ipaddress

required: true
```

パラメータの折りたたみ可能なペインを設定する

オブジェクト型のパラメータがある場合、**gui**属性を使用してレイアウトを定義できます。

例-1:

```
name: svcg-advanced

label: Advanced Application Server Settings
```

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

```
type: object

required: false

gui:

 collapse_pane: true

 columns: 2
```

この例では、レイアウトは折りたたみ可能なオブジェクトであり、フィールドは2つの列に表示されます。

`type: object[]` (オブジェクトのリスト) 型のパラメータの概要ビューを、内部パラメータを列として表すテーブルとして表示することもできます。概要ビューに内部パラメータを含めるか除外するには、`gui` セクションで `summary_display` 属性を次のように使用します。

例-2:

```
name: settings

label: Settings

type: object[]

parameters:

  -

    name: name

    label: Name

    description: Name of this setting

    type: string

    gui:

      summary_display: true
```

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

ユーザーオプションをラジオボタンとして設定する

`layout` および `allowed-values` 属性を使用して、ユーザーオプションをラジオボタンとしてリストできます。これにより、ユーザーが構成パックを作成する際に、パラメータ値がラジオボタンとして表示されます。

デフォルトでは、gui属性が指定されていない場合、パラメータ値はドロップダウンメニューとして表示されます。

```
-

    name: block-by-category-action

    label: Action

    description: Set an action if the bot is detected.

    type: string

    default: RESET

    gui:

        layout: radio

    allowed-values:

        - NONE

        - DROP

        - REDIRECT

        - RESET

        - MITIGATION
```

この例では、アクションを設定するためのユーザーオプションがラジオボタンとして表示されます。そして、**RESET**オプションがデフォルトで選択されています。

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

カスタムStyleBookのインポート

StyleBookを構築したら、NetScaler Consoleにインポートして使用します。NetScaler Consoleでは、単一のStyleBookをYAML形式でインポートしたり、多数の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したりできます。NetScaler Consoleシステムは、インポート時にStyleBookを検証します。これで、StyleBookは構成の作成に使用できるようになります。

NetScaler Consoleには、StyleBookのYAMLコンテンツを作成するために使用できる組み込みのYAMLエディターも搭載されています。YAMLエディターを使用すると、NetScaler Console 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に別のツールを使用する必要はありません。コンテンツはYAML標準に対して検証され、逸脱がある場合は強調表示されます。その後、コンテンツを修正し、StyleBookをNetScaler Consoleにインポートできます。組み込みのYAMLエディターは、独自のStyleBookを作成する際に2つの利点を提供します。

- **色分け**。エディターは、YAMLガイドラインに従って解析されたStyleBookコンテンツを表示します。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、StyleBookをNetScaler Consoleに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記述できます。

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字脱字は検証しません。

StyleBookの説明とヘッダーでHTML書式設定タグを使用する

StyleBook定義では、ヘッダーフィールドを含め、テキストにHTML書式設定タグを使用できます。ヘッダーの一部として画像を含めることもできます。ヘッダーフィールドのHTMLコンテンツは、構成を作成または更新する際に、構成ページの最上部に表示されます。この機能により、StyleBookのインフォグラフィックを追加して、StyleBookの構成を理解するのに役立てることができます。ヘッダーに画像を使用する場合は、`<img>`タグでbase64エンコードされた画像形式を使用してください。

HTMLコンテンツで画像を使用するには、次の例に示すように、画像はインラインである必要があります。オンラインツールを使用して、画像をbase64エンコード形式に変換できます。

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

```
name: cs-example

namespace: com.example.stylebooks

version: "1.2"

display-name: Content Switching Configuration

description: Example of a very simple content switching config that
creates and binds an lb to a cs

header:  <img id="b64img" src="…" />

     <h3>Operations performed by this StyleBook:</h3>

     <ul>

      <li style="list-style-type: circle"> Creates a Server </li>

      <li style="list-style-type: circle"> Creates a Service Group </li>

       <li style="list-style-type: circle"> Creates a LBVServer </li>

      <li style="list-style-type: circle"> Creates a CS Policy and Action
</li>

     </ul>

schema-version: "1.0"
```

StyleBookをインポートするには

1. NetScaler Consoleで、**Applications** > **Configuration** > **StyleBooks**に移動し、**Import New StyleBook**をクリックします。
2. 次のいずれかのオプションをクリックして、StyleBookをインポートします。
   - **File** - 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。

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

注：

この例では、StyleBook to Create a Load Balancing Virtual Serverで作成した`lb-vserver.yml` StyleBookをインポートします。

- **バンドル** - NetScaler Consoleでは、YAML形式のStyleBookを多数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。

NetScaler Consoleにインポートされ たStyleBookは、StyleBooks GUIにデフォルトのアイコンで表示されます。これらのデフォルトアイコンは、独自の画像でカスタマイズできます。

そのためには、次の手順を実行します。

- StyleBook YAMLファイルがあるフォルダーの下に、`resources`という名前のフォルダーを作成します。
- アイコンを`resources`フォルダーにアップロードします。

注:

`resources`フォルダーの名前を他の名前に変更することはできません。

- アイコンファイルとそれに対応するStyleBookファイルの名前が同じ場合、アイコンはStyleBookに自動的にマッピングされます。
- アイコンファイルとそれに対応するStyleBookファイル（例：exchange.yamlとexch.png）が一致しない場合は、`resources`フォルダーに「icon_mapping.json」という名前のJSONファイルを次のように作成します。

```
<StyleBook file name> : <icon file name>

<StyleBook file1 name> : <icon file1 name>

<StyleBook file2 name> : <icon file2 name>
```

以下はStyleBookバンドルの例です。

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

`resources`フォルダーには必要なアイコンが含まれています。

リソースフォルダー内のアイコン(/en-us/netscaler-console-service/media/stylebook-resources-folder.png)

この例では、`sharepoint.yaml`ファイルと`skype.yaml`ファイルは、それぞれ`sharepoint.jpeg`と`skype.png`に自動的にマッピングされます。

`exchange.yaml`を`exch.png`にマッピングするには、`icon_mapping.json`ファイルで次のように指定します。

```
{

"exchange.yaml":"exch.png"

}
```

StyleBookバンドルにアイコンがない場合、デフォルトのアイコンが表示されます。

- **Raw** - YAMLエディターでStyleBookのコンテンツを作成します。

  StyleBookのコンテンツを検証して、StyleBookの文法エラーを確認できます。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、「How to Create Your Own StyleBooks」を参照してください。

  注:

  お気に入りのエディターでStyleBookを作成し、そのコンテンツをYAMLエディターにコピー＆ペーストして、検証およびインポートすることもできます。

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

- **Sync Repository** - GitHubでStyleBookを作成および管理している場合は、このオプションを使用して、NetScaler Consoleがリポジトリ内の新規または更新されたStyleBookを検出できるようにします。NetScaler Consoleと同期するリポジトリを選択します。

3. オプション: StyleBookのアイコンを選択します。

   Applications > Configuration > StyleBooks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. **Create**をクリックします。

   NetScaler Consoleは、StyleBookの文法に従って、すべての構文エラーと意味エラーについてStyleBookを検証します。エラーがある場合、StyleBookはNetScaler Consoleにインポートされません。

   エラーがない場合、StyleBookは正常にインポートされ、**StyleBooks**ページに表示されます。StyleBookのヘッダーセクションで定義した表示名でStyleBookを識別できます。

   注:

   ファイルのバンドルをインポートする場合、NetScaler Consoleは圧縮されたフォルダを解凍し、すべてのStyleBookを検証します。 1つのStyleBookファイル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. **Create Configuration**リンクをクリックして、このStyleBookから構成を作成します。

   StyleBookページが開き、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。

6. パラメータ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**LoadBalancing Algorithm**を選択します。デフォルトでは、**ROUNDROBIN**が選択されています。

7. **Target Instances**で、構成をデプロイするNetScalerインスタンスのIPアドレスを選択します。

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

構成を複数のNetScalerに展開することもできます。その際は、必要な数のターゲットインスタンスを指定します。

注:

NetScaler Consoleで最近検出されたすべてのNetScalerインスタンスを**ターゲットインスタンス**に追加するには、**StyleBooks**ページに移動し、ページの右側にある更新アイコンをクリックします。

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。

   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。

   後で、**作成**をクリックして、選択したNetScalerインスタンスに構成を展開します。

構成が正常に展開されると、新しい構成パックが**構成**ページに表示されます。

ファイルをアップロードするためのStyleBookを作成する

NetScaler Console StyleBookを使用すると、NetScaler Console GUIまたはAPIを使用して、ローカルファイルシステムからNetScalerインスタンスにあらゆる種類のファイルをアップロードする際に、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
```

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

```
version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

-

 namespace: netscaler.nitro.config

 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
Console

 type: file

 required: true



components:

-
```

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

```
 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 Consoleにインポートして、地理位置情報ファイルをアップロードするために使用できます。

このStyleBookでは、ファイルがNetScaler Consoleにすでに存在している必要があります（たとえば、SCPのようなユーティリティを使用してNetScaler Consoleにすでにコピーしている場合など）。 NetScaler Consoleファイルシステムに最初にコピーせずに、NetScaler Consoleを介してNetScalerにファイルをアップロードしたい場合は、2つの「string」パラメータを持つStyleBookを作成できます。1つはNetScalerで使用するファイル名を指定するためのもので、もう1つはファイルの内容を指定するためのものです。これらの2つのパラメータを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"
```

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

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the NetScaler
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
```

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

```
-

 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を作成する

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、選択したNetScalerインスタンス上の構成を作成します。

ファイルをアップロードするための構成を作成するには：

1. NetScaler Consoleで、**Applications** > **Configuration** に移動し、**Create New** をクリックします。「Choose StyleBook」ページには、NetScaler Consoleで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. 「**場所ファイル**」セクションで、ファイルの名前または場所を入力します。

   「

   注

   」

   NetScaler Consoleでは、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FTPを使用して、ファイルをNetScaler Console ファイルシステムにコピーします。

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

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**」を選択することを推奨します。

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 Consoleで最近検出されたNetScalerインスタンスを、このウィンドウで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 Console 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 Console APIを使用することもできます。APIの使用方法の詳細については、「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。

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 Console GUIを使用して、ローカルシステムからSSLファイルとキーファイルを直接アップロードできます。NetScaler Consoleがすでに管理し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 Console APIを使用することもできます。

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

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、負荷分散方法のパラメータを選択し、仮想サーバーの証明書ファイルと証明書キーファイルをアップロードするか、NetScaler Consoleにすでに存在する証明書ファイルと証明書キーファイルを使用する必要があります。これらのパラメータは、以下の「parameters」セクションで指定されています。

```
parameters:

 -

  name: name

  type: string

  required: true

 -

  name: ip

  type: ipaddress

  required: true

 -

  name: lb-alg

  type: string

  allowed-values:

    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN
```

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

```
 -

  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

 -

  name: passphrase

  label: "SSL Certificate Key Passphrase"

  description: "The password used to protect the certificate's private key
file"

  type: password
```

StyleBookのコンポーネントセクションには、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 `ns::lbvserver` タイプで、次のとおりです。

- 「ns」は、`import-stylebooks` セクションで指定した組み込みの名前空間 netscaler.nitro.config およびバージョン 10.5 を参照するプレフィックスです。
- `lbvserver` はこの名前空間の組み込みStyleBookです。これは、同名のNetScaler NITRO `lbvserver` リソースに対応します。

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

2番目のコンポーネント `lbvserver-certificate-comp` は `stlb::vserver-certs-binds` タイプです。プレフィックス `stlb` は、StyleBookのimport-stylebooksセクションで指定されている名前空間「com.citrix.adc.stylebooks」およびバージョン1.0を参照します。
「com.citrix.adc.stylebooks」名前空間をフォルダと考えると、`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 Consoleの一部として出荷されます。

ユーザー定義のStyleBookで使用される `vserver-certs-binds` StyleBookを使用すると、証明書とキーファイルをターゲットのNetScalerインスタンスにアップロードし、証明書とキーファイルを適切な仮想サーバーにバインドするように構成することで、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指定する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
  description: Binds lbvserver with server certificate
  properties:
```

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

```
vserver-name: $components.my-lbvserver-comp.properties.name

certificates:

 -

  cert-name: $parameters.name + "-lb-cert"

  cert-file: $parameters.certificate

  ssl-inform: PEM

  key-name: $parameters.name + "-key"

  key-file: $parameters.key

  cert-password: $parameters.passphrase
```

このようなStyleBookから構成を作成するためにAPIを使用する場合、ファイル名のみを使用します（完全なファイルパスは使用しません）。これらのファイルは、NetScaler Consoleの証明書およびキーファイルフォルダにすでに存在している必要があります。アップロードされたSSL証明書ファイルはNetScaler Consoleの `/var/mps/tenants/.../ns_ssl_certs` ディレクトリに保存され、SSL証明書キーファイルはNetScaler Consoleの `/var/mps/tenants/.../ns_ssl_keys` ディレクトリに保存されます。

SSLファイルをアップロードするための構成の作成

以下の手順では、StyleBookの例からSSLプロトコルを使用して、選択したNetScalerインスタンス上に基本的な負荷分散仮想サーバー構成を作成します。この手順を使用して、NetScaler ConsoleにSSL証明書ファイルと証明書キーファイルをアップロードできます。

ファイルをアップロードするための構成を作成するには：

1. NetScaler Consoleで、**Applications** > **Configuration > StyleBooks** に移動します。**StyleBooks** ページには、NetScaler Consoleで利用可能なすべてのStyleBookが表示されます。
2. 下にスクロールして **Load Balancing Virtual Server (SSL)** を選択するか、検索フィールドに **Load Balancing Virtual Server (SSL)** と入力して **Enter** キーを押します。
3. StyleBookパネルで**構成の作成**をクリックします。

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

StyleBookのパラメータがユーザーインターフェイスページとして表示され、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。

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**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。NetScaler Consoleに存在するファイルを選択することもできます。
6. 構成を作成するターゲットのNetScalerインスタンスを選択し、**作成**をクリックします。

注:

更新アイコンをクリックして、NetScaler Consoleで最近検出されたNetScalerインスタンスを、このウィンドウで使用可能なインスタンスのリストに追加することもできます。

NetScaler Consoleでは、NetScaler Consoleの一部として提供される以下のデフォルトのStyleBookを使用すると、SSL証明書とキーをアップロードしてSSLサポートを作成できます。

- HTTP/SSLロードバランシングStyleBook (lb)
- HTTP/SSLロードバランシング (モニター付き) StyleBook (`lb-mon`)
- HTTP/SSLコンテンツスイッチングアプリケーション (モニター付き) (`cs-lb-mon`)
- CS、LB、およびSSL機能を使用するサンプルアプリケーションStyleBook (`sample-cs-app`)

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

namespace: com.example.ssl.stylebooks

version: "0.1"

description: "This stylebook defines a load balancing virtual server
configuration."

display-name: "Load Balancing Virtual Server (SSL)"

schema-version: "1.0"
```

© 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
  type: string
```

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

```
  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

 -

  name: key

  label: "SSL Certificate Key Passphrase"

  description: "The password used to protect the certificate's private key
file"

  type: password



components:
```

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

```
-
 name: my-lbvserver-comp
 type: ns::lbvserver
 properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
-
 name: lbvserver-certificate-comp
 type: stlb::vserver-certs-binds
 description: Binds lbvserver with server certificate
 properties:
  vserver-name: $ components.my-lbvserver-comp.properties.name
  certificates:
   -
    cert-name: $parameters.name + "-lb-cert"
    cert-file: $parameters.certificate
    ssl-inform: PEM
    key-name: $parameters.name + "-key"
    key-file: $parameters.key
```

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

```
    cert-password: $parameters.passphrase
```

NetScaler Console APIを使用して構成パックを作成する:

NetScaler Console APIを使用して、選択したNetScalerインスタンスにCertおよびKeyファイルをアップロードする設定パックを作成することもできます。APIの使用方法の詳細については、「APIを使用してCertおよびKeyファイルをアップロードする構成を作成する方法」(/ja-jp/netscaler-console-service/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/how-to-use-api-to-create-configurations-to-upload-cert-and-key-files.html)を参照してください。

NetScalerインスタンスで定義されているオブジェクトの表示

NetScaler ConsoleでStyleBook構成（設定パック）が作成された後、**「作成されたオブジェクトを表示」**をクリックして、ターゲットのNetScalerインスタンスで作成されたすべてのNetScalerオブジェクトを表示します。

StyleBook を使用して証明書ストアから SSL 証明書を管理する

NetScaler Console の証明書ストアは、SSL 証明書を一元的に保存および管理するのに役立ちます。そのため、SSL 証明書を NetScaler Console に保存し、NetScaler の構成中に再利用できます。

この記事では、NetScaler Console の証明書ストアから SSL 証明書をアップロードして再利用できる StyleBook 定義を作成する方法について説明します。

パラメータ

StyleBook 定義は、新しい組み込みパラメータタイプとして `certkey` をサポートしています。このパラメータタイプを使用して、NetScaler Console の証明書ストアから SSL 証明書を再利用します。

```
parameters:

-

    name: certificate

    label: Certificate

    description: "Certificate to be bound to this virtual load balanced
```

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

```
application"

    type: certkey

    required: true
```

この例では、証明書パラメータは NetScaler Console の証明書ストアからの SSL 証明書または証明書チェーンを指します。

StyleBook 定義では、`certkey` パラメータに対して次のプロパティを参照できます。

- `certkeyname` – インスタンスで構成する SSL 証明書キーの名前。
- `cert_filename` – SSL 証明書のファイル名。
- `password` – 必要に応じて、SSL 証明書にアクセスするために必要なパスワード。
- `key_filename` – SSL 証明書キーのファイル名。
- `keyfile_contents` – SSL 証明書のファイルコンテンツ。
- `subject` – SSL 証明書に記載されているサブジェクト。
- `issuer` – SSL 証明書を発行した機関を指します。
- `certchain_certkeyname` – サーバー証明書は、複数の階層型認証局 (CA) によって署名されることがあり、これは証明書がチェーンを形成することを意味します。

  証明書ストアに証明書チェーンがある場合、このプロパティを使用します。これにより、証明書を参照して結合できます。構成パックを作成する際、証明書チェーンはリストとして表示されます。

これらのプロパティは、**StyleBook** 定義で必要なコンポーネントを作成するのに役立ちます。

コンポーネント

StyleBook に `type: certkey` パラメーターがある場合、StyleBook ユーザーは NetScaler Console 証明書ストアからこのパラメーターの証明書を提供できます。このワークフローでは、NetScaler Console 証明書ストアから証明書を表示および選択するだけでなく、ユーザーは次のことも実行できます。

- 新しい証明書をアップロードします。
- 既存の証明書を更新します。例: 期限切れの証明書。
- 証明書を削除します。

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

注

- NetScaler Console SSL ダッシュボードを使用して、NetScaler Console 証明書ストア内の証明書を管理することもできます。
- NetScaler Console 証明書ストアで SSL 証明書が更新されると、その SSL 証明書に関連付けられている構成パックは自動的に更新されます。

StyleBook を構築する

以下は StyleBook 定義の例です。これは、NetScaler Console 証明書ストアの SSL 証明書を使用する完全な定義です。この StyleBook には、メインの証明書ファイルとキーファイルを NetScaler インスタンスにアップロードするコンポーネントが含まれています。これらのファイルがすでに NetScaler インスタンスに存在する場合、NetScaler Console はアップロード手順をスキップし、これらのコンポーネントは効果がありません。

```
name: lb-with-cert-from-certstore

namespace: com.example.stylebooks

version: "1.0"

display-name: Application using a CertStore certificate

description: This StyleBook defines a simple SSL Vserver.

schema-version: "1.0"



import-stylebooks:

 -

    namespace: netscaler.nitro.config

    version: "13.0"

    prefix: ns
```

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

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: certificate
  label: Application Certificate
  description: Certificate chain and key to be bound to this application
  type: certkey
  required: true



components:
```

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

```
 -

    name: pem-cert-files-comp

    type: ns::systemfile

    description: This component uploads the PEM certificate file onto the
NetScaler

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.cert_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.certfile_contents)

      fileencoding: BASE64

 -

    name: pem-KEY-files-comp

    type: ns::systemfile

    description: This component uploads the PEM key file onto the
NetScaler.

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.key_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.keyfile_contents)

      fileencoding: BASE64

 -
```

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

```
    name: cert-files-comp

    type: ns::sslcertkey

    description: This component creates the certkey on the NetScaler using
the uploaded files.

    condition: $parameters.certificate

    properties:

      certkey:  $parameters.certificate.certkeyname

      cert: $parameters.certificate.cert_filename

      key: $parameters.certificate.key_filename

 -

  name: lbvserver-comp

  type: ns::lbvserver

  description: This component creates the lbvserver of the application.

  properties:

   name: $parameters.name + "-lbvserver"

   servicetype: SSL

   ipv46: $parameters.ip

   port: 443

   lbmethod: ROUNDROBIN

  components:

      -

        name: sslvserver-comp
```

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

```
    type: ns::sslvserver
    description: This component configures SSL settings on the vserver
    properties:
      vservername: $parent.properties.name
      ssl3?: ENABLED
      tls1?: ENABLED
      tls11?: ENABLED
  -
   name: cert-bindings-adv-comp
   type: ns::sslvserver_sslcertkey_binding
   description: This component binds the certkey to the vserver
   condition: $parameters.certificate
   properties:
     vservername: $parent.properties.name
     certkeyname: $parameters.certificate.certkeyname
```

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

You can use the operations construct to configure NetScaler Console analytics to collect AppFlow records on all or some of the traffic transactions handled by any virtual server component that is part of a StyleBook. You can also use this construct to configure alarms to get insight into the traffic managed by the virtual server.

次の例は、StyleBookのoperationsセクションを示しています。

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

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
      target: $components.basic-lb-comp
      filter: HTTP.REQ.URL.CONTAINS("catalog")
  alarms:
   -
    name: lbvserver-alarm
    properties:
      target: $components.basic-lb-comp
      email-profile: $parameters.emailprofile
      sms-profile: "MyProdSMS"
      rules:
       -
         metric: "total_requests"
         operator: "greaterthan"
         value: 25
         period-unit: $parameters.period
       -
         metric: "total_bytes"
```

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

```
        operator: "lessthan"

        value: 60

        period-unit: "day"
```

The attributes in the analytics section are used to instruct NetScaler Console 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 Console policy expression to filter requests for which AppFlow records are collected on the virtual server.

このStyleBookから構成パックが作成されると、NetScaler Consoleのアナリティクス機能は、構成パックの作成プロセスで作成される際に指定された仮想サーバーでAppFlowレコードを収集するように構成されます。

alarmsセクションの属性は、targetプロパティによって識別される仮想サーバーでアラームを生成し、通知を送信するためのしきい値を設定するために使用されます。上記の例では、email-profileおよびSMS-profileプロパティは、通知の送信先を指定するために使用されます。rulesセクションはしきい値を定義します。たとえば、仮想サーバーによって処理される合計リクエストが25を超え、ユーザーによって定義された期間の場合、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。

- `>` の場合、`greaterthan`
- `<` の場合、`lessthan`
- `>=` の場合、`greaterthanequal`
- `<=` の場合、`lessthanequal`

StyleBookはメトリックにAPI名を使用し、NetScaler Consoleアナリティクスの 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 Consoleアナリティクスドキュメントを参照してください。

インスタンスの役割

StyleBookは、NetScalerインスタンスで以下の構成をサポートしています。

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

- 対称構成 - 複数のNetScalerインスタンスに構成パックが適用され、すべてのインスタンスに展開される構成が同じである場合。
- 非対称構成 - 複数のNetScalerインスタンスに構成パックが適用され、すべてのインスタンスに展開される構成が異なる場合。たとえば、デフォルトのMicrosoft Skype for Business StyleBookでは、各NetScalerインスタンスに異なる構成を展開する必要があります。

StyleBookの「インスタンスの役割」機能は、非対称構成を作成するのに役立ちます。ここでは、構成パック内の各NetScaler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。役割は、NetScalerインスタンスが受け取る構成パックの構成オブジェクトを決定します。

注意点:

- StyleBook内のインスタンスの役割のセットは、StyleBookの作成時に定義されます。
- 役割は、構成パックの作成時または更新時に特定のNetScalerインスタンスに割り当てられます。

ターゲットロールセクション

「target-roles」は通常、StyleBookの「import-StyleBooks」セクションの後、「parameters」セクションの前に配置されます。StyleBookでサポートされるすべての役割は、「target-roles」セクションで宣言されます。

次のStyleBookの例では、「target-roles」セクション内に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。

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

`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NetScalerインスタンスの最小必須数を指定します。`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NetScalerインスタンスの最大数を指定します。

これらのサブプロパティが指定されていない場合、その役割に構成できるNetScalerインスタンスの数に制限はありません。min-targets = 0 の場合、その役割に関連付けられた構成はオプションです。min-targets = 1 の場合、構成は必須であり、少なくとも1つのNetScalerインスタンスがその役割に構成されている必要があります。

役割「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ます。この暗黙的なロールはデフォルトロールと呼ばれ、StyleBook内の他のロールと同様に使用されます。構成パックを作成する際、NetScalerインスタンスに特定のロールが割り当てられていない場合、そのインスタンスは暗黙的に「default」ロールに割り当てられます。その後、そのインスタンスは「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NetScalerインスタンスにのみコンポーネントをデプロイしたい場合は、コンポーネントの一部としてroles属性を指定できます。コンポーネントの以下の例で示されています。

```
-

  name: C1

  type: ns::lbvserver

  roles:

    - A

  properties:

    name: lb1

    servicetype: HTTP

    ipv46: 1.1.1.1
```

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

```
    port: 80
```

この例では、コンポーネントは`lbvserver`を生成し、ロールAを果たすインスタンスにデプロイされます。コンポーネントのroles属性は`list`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ます。これらのロールは、StyleBookの`target-roles`セクションで宣言されているはずです。

注

StyleBook内のコンポーネントがロール属性を指定しない場合、そのコンポーネントによって生成される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。

2つのロールと4つのコンポーネントを持つStyleBookを考えてみましょう。

- コンポーネントC1はロールAとBを持ちます
- コンポーネントC2はロールBを持ちます
- 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は次のとおりです。

```
components:

  -

    name: C1

    type: ns::lbvserver

    roles:

      - A

      - B

    properties:
```

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

```
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
```

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

```
-

  name: C4

  type: ns::lbvserver

  roles:

    - default

  properties:

    name: lb4

    servicetype: HTTP

    ipv46: 14.14.14.14

    port: 80
```

コンポーネントC3にはロールが定義されていません。これは、その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すべて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NetScalerインスタンスにデプロイしたいとします。インスタンスへのロールの割り当ては、次の方法で行うことができます。

- ロールAはインスタンスT1、T2、T3、T4に割り当てられます
- ロールBはインスタンスT2、T3、T4に割り当てられています
- インスタンスT5にはどのロールも割り当てられていません

次の図は、ロールの割り当てを要約し、各NetScalerインスタンスが受け取る結果の構成を示しています。

コンポーネントC3は、このコンポーネントに`roles`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展開されます。

「ドライラン」機能を使用して、以下を表示および確認します。

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

- ロールの割り当て
- 各NetScalerインスタンスで作成された構成オブジェクト

StyleBookを構築する

StyleBook「demo-target-roles」の全内容は次のとおりです。

```
---

name: demo-target-roles

namespace: com.example.stylebooks

version: "1.2"

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

parameters:

  -

    name: appname

    type: string

    required: true

    key: true

target-roles:

  -
```

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

```
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
```

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

```
    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:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
```

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

```
      port: 80
```

次の図は、サンプル構成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、構成パックを作成または更新する際に、各NetScalerインスタンスのロールを次のように指定できます。「targets」ブロックで、個々のコンポーネントを展開したい特定のNetScalerインスタンスのUUIDを指定します。

```
"targets": [
            {
             "id": "<ADC-UUID>",
             "roles": ["A"]
            },
           ]
```

完全なサンプルREST APIが参考のために提供されています。

POST /`<IP`>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{
  "configpack": {
     "parameters": {
     "appname": "app1"
    },
     "targets": [
        {
```

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

```
        "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
      "roles": ["A"]
      },
      {
        "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
        "roles": ["A", "B"]
      },
      {
        "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
        "roles": ["A", "B"]
      },
      {
        "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
        "roles": ["A", "B"]
      },
      {
        "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
        "roles": ["default"]
      }
    ]
  }
```

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

```
}
```

非CRUD操作を実行するStyleBookを作成する

StyleBookは、NetScalerインスタンス上で必要な構成オブジェクトを計算することで、NetScaler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から追加、更新、または削除されます。その際に「望ましい状態」を指定します。

しかし、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。例えば、ロードバランサーオブジェクト (`lbvserver`) やNetScaler機能オブジェクト (`nsfeature`) は、「有効化」または「無効化」操作をサポートできます。同様に、NetScaler `certkeys` 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それらの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（例えば、`certkey` を `lbvserver` にバインドする）は非CRUD操作ではありません。NITROバインディングはそれ自体が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` と呼ばれるコンストラクトが追加されます。このコンストラクトでサポートされる属性は `action` と呼ばれます。この属性は、`enable`、`disable`、`link`、`unlink`、`import`、`export`、`create`、`archive`、および `apply` のような値を取ることができます。

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver
```

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

```
  meta-properties

   action: enable

  properties:

    name: $parameters.name

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg
```

この例では、`my-lbvserver-comp` コンポーネントは `ns::lbvserver` タイプです。「ns」は、import-stylebooksセクションで指定した名前空間 netscaler.nitro.config およびバージョン ** 10.5 を参照するプレフィックスです。`lbvserver` はこの名前空間のNITROリソースです。暗黙的なアクションとして、StyleBookは `lbvserver` を作成し、その上で「有効化」操作を完了します。

メタプロパティの `action` 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。

メタプロパティの式を指定できます。これらの式は、NetScalerオブジェクトに対して有効なメタプロパティアクションを動的に適用します。

例:

```
parameters:

-

    name: meta-action-lbvserver

    type: string

    default: disable

    allowed-values:
```

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

```
      - enable
      - disable


components:
  -
    name: c1
    type: ns::lbvserver
    meta-properties:
      action: $parameters.meta-action-lbvserver
    properties:
      name: $parameters.lbvserver
      ipv46: $parameters.ip
      port: 80
      servicetype: HTTP
```

この例では、StyleBookユーザーは構成パックの作成中に有効なメタプロパティアクションを指定できます。

DNSドメイン名を使用したGSLB構成の展開

NetScaler Consoleの新しいRBAC機能強化により、承認されたアプリケーション所有者のみがNetScaler Consoleで独自のDNSドメインを作成および管理できるようになります。特定のStyleBookを使用して、アプリケーション所有者が所有するDNSドメインからGSLB構成を作成することを承認できるようになりました。選択したDNSドメイン名がユーザーによって所有されている場合、NetScaler ConsoleアプリケーションダッシュボードでGSLB StyleBookを使用してGSLB構成を作成する際に使用できます。 NetScaler Consoleには、GSLB構成を構成するための2つのワークフローがあります。

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

1. **管理者向けのワークフロー**。NetScaler ConsoleでRBAC環境をセットアップします。つまり、GSLB StyleBookを作成およびインポートするには、ユーザーグループ、ポリシー、ロールを作成し、ユーザーをグループに割り当てる必要があります。管理者として、このワークフローを実行する必要があります。
2. **アプリケーション所有者向けのワークフロー**。アプリケーション所有者は、自身が所有するドメイン名を使用してGSLB構成を作成する必要があります。

次のフローチャートは、両方のワークフローを示しています。

GSLBワークフロー構成(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-workflow-1.png)

管理者向けのワークフロー

管理者として、NetScaler ConsoleでRBAC環境を作成するためのワークフローは、次の手順で構成されます。

まず、NetScalerインスタンスにGSLB構成を展開するためのStyleBookを作成します。このドキュメントでは、独自のStyleBookを作成するのに役立つYAMLコンテンツのサンプルを提供しています - StyleBookの構築。

カスタムStyleBookの作成方法の詳細については、「カスタムStyleBookの作成と使用」を参照してください。

注:

NetScaler Consoleは、StyleBookで「allowed-dynamic-values」という新しいコンストラクトをサポートしています。このコンストラクトを使用すると、ユーザーはNetScaler Consoleに存在するDNSドメイン値からリスト表示および選択でき、NetScaler Console GUIのStyleBookで「domain-name」パラメーターが自動的に入力されます。

参考として、「domain-name」パラメーターセクションの例を示します。

ここで使用されている「domain-name」パラメーターは単なる例です。このパラメーターは、カスタムStyleBookでは異なる場合があります。

```
-

  name: domain-name

   label: DNS Domain Name
```

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

```
description: GSLB DNS Domain Name

type: string

required: true

allowed-dynamic-values:

   source: local

   resource-type: dns_domain_entry
```

注:

現在、NetScaler Consoleでは、「allowed-dynamic-values」コンストラクトはどのデフォルトStyleBookでも使用されていません。デフォルトのGSLB StyleBookを使用して、新しいカスタムGSLB StyleBookを作成します。ドメイン名パラメータの部分を、上記で提供されているサンプルに置き換えます。任意のテキストエディタを使用して、新しいStyleBookを作成できます。

1. 管理者としてNetScaler Consoleにログオンします。
2. **Applications** > **Configurations** > **StyleBooks** の順に移動します。
3. **Import New StyleBook** をクリックし、新しいGSLB StyleBookをNetScaler Consoleにアップロードします。

   NetScaler ConsoleでStyleBookをインポートする方法の詳細については、カスタムStyleBookを使用する を参照してください。
4. **System** > **Users** > **Policies** の順に移動し、**Add** をクリックして、以下に示すようにアプリケーション所有者のアクセスポリシーを設定します。

   Citrixでは、アプリケーション所有者が設定したRBACルールを回避しないように、アクセスポリシーを作成することをお勧めします。
5. ポリシーの名前と簡単な説明を入力します。 セクションで、以下の表示/編集権限が必須でチェックされていることを確認します。

   a. Applications > ダッシュボード

   b. アプリケーション > 構成

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

c. Infrastructure > インスタンス

d. Infrastructure > ライセンス管理

e. Settings > ドメイン名

必要に応じて他の権限を付与し、**Create** をクリックします。

ダッシュボード、構成、インスタンス、ライセンス管理、およびDNSドメイン名のアクセスポリシーを作成します。(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-3.png)

6. **System** > **Users** > **Roles** に移動し、ロールを作成して、前の手順で作成したポリシーを割り当てます。
7. ロールの名前を入力し、簡単な説明を入力します。「Policies」セクションで、**AppOwnerExampleAccessPolicy** を選択します。

   アプリケーション所有者ロールを作成します。(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-4.png)
8. **System** > **Users** > **Groups** に移動し、グループを作成して、前の手順で作成したロールを関連付けます。
9. 名前と説明を入力し、「Roles」セクションで **AppOwnerExampleRole** を選択します。

   システムグループを作成します。(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-5.png)
10. **Next** をクリックします。
11. **Authorization Settings** タブで、アプリケーション所有者がアクセスできるNetScalerインスタンスと新しいGSLB StyleBookを選択します。

    認証設定(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-6.png)

    この手順を繰り返して、組織に必要な数のユーザーグループを作成します。**Create Group** をクリックします。
12. システムユーザーを作成し、そのユーザーをユーザーグループに割り当てます。このドキュメントは、ローカルで作成されたユーザーのみを指します。NetScaler Consoleが外部認証（LDAPなど）を使用するように設定されている場合、ユーザーグループにユーザーを作成する必要はありません。グループへのユーザーマッピングは、外部認証ディレクトリから取得されます。

    a. **System** > **Users** > **User** に移動します。

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

b. システムユーザーのユーザー名とパスワードを入力し、そのユーザーをグループに割り当てます。

ユーザーを作成します。(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-7.png)

注:

ステップ12はオプションであり、LDAPなどの外部認証が使用される場合は必須ではありません。

管理ワークフロー用のNetScaler Console REST API

NetScaler Consoleにログオンするための REST API

```
URL: http: //<MAS_IP>/nitro/v2/config/login

HTTPMETHOD: POST



Body Payload:

{

  "login": {

    "username": "<USER_NAME>",

    "password": "<PASSWORD>",

    "session_timeout": 1800

  }

}



The response results in a session cookie header, that can be sent with the rest of the API requests below.
```

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

```
Set-Cookie:
SESSID=##ED31F7C886E248CCDCA8F0E0AD2AA511ACCC5F46C48D6D2BCAA719A9DE62;path
=/;secure;HttpOnly
```

アクセス ポリシーを作成するためのREST API

```
URL: https://<MAS_IP>/nitro/v2/config/rba_policy

HTTP METHOD: POST



{

  "rba_policy": {

    "name": " AppOwnerAccessPolicy",

    "description": " ExampleCompany AppOwner Access Policy",

    "tenant_id": "7c12ec97-1472-4096-97e7-a5acb453cc5c",

    "statement": [

      {

        "access_type": true,

        "resource_type": "application",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,app_category"

      },

      {

        "access_type": true,
```

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

```
        "resource_type": "application",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,ns_vserver_license,app_category,app_summary,app_heal
th_dashboard_details,haproxy_frontend,haproxy_backend,haproxy_frontend_sta
ts"

      },

      {

        "access_type": true,

        "resource_type": "si_app_unit",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,app_summary,si_app_summary,si_device,security_app_da
shboard_details,si_geo_location,si_safety_app_firewall,si_safety_overview,
si_safety_security_check,si_safety_system_security,si_safety_signature"

      },

      {

        "access_type": true,

        "resource_type": "stylebooks",

        "operation_name": "get",

        "dependent_resources": "download,smtp_server,ns_vserver_license"

      },

      {

        "access_type": true,

        "resource_type": "stylebooks",
```


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

```
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "configpacks",
        "operation_name": "get",
        "dependent_resources":
"download,smtp_server,stylebooks,ns_vserver_license"
      },
      {
        "access_type": true,
        "resource_type": "configpacks",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "stylebooks_system_settings",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server"
      },
```


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

```
      {
        "access_type": true,
        "resource_type": "stylebooks_system_settings",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "ns_crvserver",
        "operation_name": "get",
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_cache_redirection_report,poll_ac
tivity_status,ns_emon_poll_policy,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "ns_crvserver",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"
      },
      {
        "access_type": true,
```


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

```
        "resource_type": "haproxy_frontend",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,haproxy_backend,haproxy_server"

      },

      {

        "access_type": true,

        "resource_type": "haproxy_frontend",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_server",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_server,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_server",

        "operation_name": "add",
```


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

```
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_lbvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_lb_vserver_report,ns_emon_poll_p
olicy,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_lbvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_service",

        "operation_name": "get",

        "dependent_resources":
```


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

```
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_visualizer_lb_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_service",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_visualizer_lb_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_servicegroup",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_servicegroupmember_binding,ns_visualizer_lb_bindings,lb_export_repo
rt"

      },

      {

        "access_type": true,

        "resource_type": "ns_servicegroup",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
```


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

```
,poll_activity_status,ns_servicegroupmember_binding,ns_visualizer_lb_bindi
ngs,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_authenticationvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_authentication_report,poll_activ
ity_status,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_authenticationvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "syslog_messages",

        "operation_name": "get",

        "dependent_resources": "download,smtp_server"

      },
```


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

```
      {
        "access_type": true,
        "resource_type": "ns_emon_poll_policy",
        "operation_name": "get",
        "dependent_resources": "download,poll_activity_status,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "ns_emon_poll_policy",
        "operation_name": "add",
        "dependent_resources":
"download,poll_activity_status,mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "ns_visualizer_gslb_bindings",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,ns_gslbvserver_domain,lb_export_report"
      },
      {
        "access_type": true,
```


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

```
        "resource_type": "ns_visualizer_gslb_bindings",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,poll_activity_status,ns_emon_poll_pol
icy,ns_gslbvserver_domain,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbservice",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbservice",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,poll_activity_status,ns_emon_poll_pol
icy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbvserver",
```


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

```
        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_global_server_load_balancing_rep
ort,poll_activity_status,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

     },

      {

        "access_type": true,

        "resource_type": "ns_vpnvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_vpnvserver",

        "operation_name": "get",
```


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

```
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_ssl_vpn_report,poll_activity_sta
tus,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_csvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_content_switching_report,ns_emon
_poll_policy,poll_activity_status,ns_visualizer_cs_bindings,lb_export_repo
rt"

      },

      {

        "access_type": true,

        "resource_type": "ns_csvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_visualizer_cs_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "dns_domain_entry",

        "operation_name": "get",
```


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

```
        "dependent_resources": ""

      },

      {

        "access_type": true,

        "resource_type": "dns_domain_entry",

        "operation_name": "add",

        "dependent_resources": ""

      },

      {

        "access_type": true,

        "resource_type": "devicewise_detail_summary",

        "operation_name": "get",

        "dependent_resources":
"download,mps_user_heatmap,ns_event,mps_agent,active_event,smtp_server,mps
_datacenter,event_severity_report,event_device_report,ns_conf,device_event
_summary"

      },

      {

        "access_type": true,

        "resource_type": "devicewise_detail_summary",

        "operation_name": "add",

        "dependent_resources": "mail_profile,slack_profile,smtp_server"

      },
```

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

```
      {

        "access_type": true,

        "resource_type": "cbwanopt",

        "operation_name": "get",

        "dependent_resources":
"download,device_backup,traceroute,inventory,inventory_status,ping,mps_dat
acenter,cbwanopt_device_profile,sdwanvw_device_profile,sdwanvw_snmp_config
,sdwanvw_appflowconfig,smtp_server,cbwanopt_snmp_config,cbwanopt_appflowco
nfig,sdwanvw,tag"

      },

      {

        "access_type": true,

        "resource_type": "cbwanopt",

        "operation_name": "add",

        "dependent_resources":
"inventory,managed_device,device_backup,upload,cbwanopt_device_profile,mps
_datacenter,mail_profile,slack_profile,smtp_server,sdwanvw_device_profile,
sdwanvw_snmp_config,sdwanvw_appflowconfig,cbwanopt_snmp_config,cbwanopt_ap
pflowconfig,sdwanvw,tag"

      },

      {

        "access_type": true,

        "resource_type": "device_login",

        "operation_name": "get",

        "dependent_resources": ""

      },
```


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

```
      {

        "access_type": true,

        "resource_type": "ns",

        "operation_name": "get",

        "dependent_resources":
"download,ns_config_replicate,ns_conf,ns_ns_runningconfig,ns_ns_savedconfi
g,active_event,device_backup,traceroute,inventory,inventory_status,ping,ns
_device_profile,nssdx_device_profile,sdx_snmp_config,sdx_syslog_config,smt
p_server,ns_cluster,ns_snmp_config,ns_syslog_config,ns_l7_latency_config,i
ca_l7_latency_update,af_vserver_policy,ns_vserver_appflow_config,mps_datac
enter,ns_appflow_param_config,ns_ns_license,ns_ns_mode,ns_network_interfac
e,advanced_analytics_config,tag"

      },

      {

        "access_type": true,

        "resource_type": "ns",

        "operation_name": "add",

        "dependent_resources":
"inventory,ns_l7_latency_config,ica_l7_latency_update,af_vserver_policy,ns
_config_replicate,managed_device,device_backup,upload,ns_device_profile,ns
sdx_device_profile,mps_datacenter,sdx_snmp_config,sdx_syslog_config,mail_p
rofile,slack_profile,smtp_server,ns_cluster,ns_snmp_config,ns_syslog_confi
g,ns_vserver_appflow_config,ns_appflow_param_config,advanced_analytics_con
fig,tag"

      },

      {

        "access_type": true,

        "resource_type": "haproxyhost",
```


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

```
        "operation_name": "get",

        "dependent_resources":
"download,traceroute,inventory,inventory_status,ping,mps_datacenter,smtp_s
erver,haproxy_device_profile,device_backup,tag"

      },

      {

        "access_type": true,

        "resource_type": "haproxyhost",

        "operation_name": "add",

        "dependent_resources":
"inventory,managed_device,mail_profile,slack_profile,smtp_server,mps_datac
enter,haproxy_device_profile,haproxy,device_backup,tag"

      },

      {

        "access_type": true,

        "resource_type": "docker_host",

        "operation_name": "add",

        "dependent_resources":
"inventory,ns_snmp_config,managed_device,ns,upload,mail_profile,slack_prof
ile,smtp_server,mps_datacenter,ns_device_profile,docker_nscpx_image"

      },

      {

        "access_type": true,

        "resource_type": "docker_host",

        "operation_name": "get",
```


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

```
        "dependent_resources":
"download,ns_snmp_config,ns_conf,ns_ns_runningconfig,ns_ns_savedconfig,smt
p_server,mps_datacenter,ns_device_profile,traceroute,inventory,inventory_s
tatus,ping,active_event,ns_ns_license,ns_ns_mode,ns_network_interface"

      },

      {

        "access_type": true,

        "resource_type": "perf_reports",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,perf_custom_dashboard"

      },

      {

        "access_type": true,

        "resource_type": "perf_reports",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,perf_report_counters,perf_res_util_report,perf_http_
req_tcp_conn_report,perf_lb_ssl_traffic_report,perf_ip_bytes_rxtx_report,p
erf_ip_pkt_rxtx_report,perf_icmp_pkt_rxtx_report,perf_icmp_bytes_rxtx_repo
rt,perf_icmpv6_pkt_rxtx_report,perf_icmpv6_bytes_rxtx_report,perf_ipv6_byt
es_rxtx_report,perf_ipv6_pkt_rxtx_report,perf_udp_bytes_rxtx_report,perf_u
dp_packets_rxtx_report,perf_cmp_bytes_rxtx_report,perf_cmp_tcp_bytes_rxtx_
report,perf_cmp_tcp_ratiosaving_report,perf_cmp_decmp_bytes_rxtx_report,pe
rf_cmp_decmp_ratiosaving_report,perf_tcp_server_conn_report,perf_tcp_surge
len_spareconn_report,perf_http_bytes_rx_report,perf_http_gets_posts_report
,perf_ssl_transactions_hits_report,perf_ssl_client_auth_report,perf_ssl_rs
a_dhkey_report,perf_ssl_frontend_ciphers_report,perf_ssl_backend_ciphers_r
eport,perf_wsdevice_cpu_utilization_report,perf_wsdevice_send_compression_
ratio_report,perf_wsdevice_connected_plugins_report,perf_wsdevice_data_red
uction_report,perf_wsdevice_link_utilization_report,perf_wsserviceclasssta
```


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

```
tstable_pass_through_connection_report,perf_wsserviceclassstatstable_servi
ce_class_report,perf_wsserviceclassstatstable_acceleration_report,perf_wsl
inkstatstable_throughput_report,perf_wslinkstatstable_packet_loss_report,p
erf_wsappstatstable_application_report,perf_wsqosstatstable_qos_report,per
f_ssl_cpu_keyexchange_report,perf_ssl_be_rsa_dhkey_report,perf_custom_dash
board,perf_ns_throughput_report,perf_network_interface_report"

      },

      {

        "access_type": true,

        "resource_type": "perf_threshold",

        "operation_name": "get",

        "dependent_resources":
"download,perf_reports,perf_report_counters,smtp_server,sms_server,sms_pro
file"

      },

      {

        "access_type": true,

        "resource_type": "perf_threshold",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,sms_server,sms_profile"

      },

      {

        "access_type": true,

        "resource_type": "perf_poll_config",

        "operation_name": "add",
```


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

```
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "perf_poll_config",
        "operation_name": "get",
        "dependent_resources": "smtp_server,download"
      },
      {
        "access_type": true,
        "resource_type": "license_server_info",
        "operation_name": "get",
        "dependent_resources":
"sms_server,license_proxy_server,jazz_license,download,sms_profile,smtp_se
rver,user_managed_tp_vserver,managed_vserver,user_managed_vserver,haproxy_
frontend,haproxy_backend,license_file,device_license_info,license_info,ns_
authenticationvserver,ns_gslbvserver,ns_vpnvserver,ns_csvserver,ns_crvserv
er,ns_lbvserver,autoselection_preference,license_threshold,license_expiry_
info"
      },
      {
        "access_type": true,
        "resource_type": "license_server_info",
        "operation_name": "add",
        "dependent_resources":
```


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

```
"sms_server,license_proxy_server,jazz_license,sms_profile,mail_profile,sla
ck_profile,smtp_server,user_managed_tp_vserver,managed_vserver,upload,lice
nse_file,license_info,license_threshold,mas_license,user_managed_vserver,a
utoselection_preference,license_expiry_info"

      }

    ],

    "ui": [

      {

        "access_type": true,

        "name": "ApplicationsDashboard",

        "display_name": "Dashboard"

      },

      {

        "access_type": true,

        "name": "SecurityDashboard",

        "display_name": "App Security Dashboard"

      },

      {

        "access_type": true,

        "name": "Stylebooks",

        "display_name": "StyleBooks"

      },

      {

        "access_type": true,
```


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

```
        "name": "Stylebooks",
        "display_name": "Configpacks"
      },
      {
        "access_type": true,
        "name": "StylebooksSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "CacheRedirection",
        "display_name": "Cache Redirection"
      },
      {
        "access_type": true,
        "name": "Servers",
        "display_name": "Servers"
      },
      {
        "access_type": true,
        "name": "VirtualServers",
        "display_name": "Virtual Servers"
```


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

```
    },
    {
      "access_type": true,
      "name": "Services",
      "display_name": "Services"
    },
    {
      "access_type": true,
      "name": "ServiceGroups",
      "display_name": "Service Groups"
    },
    {
      "access_type": true,
     "name": "Authentication",
      "display_name": "Authentication"
    },
    {
      "access_type": true,
      "name": "MonitoringAuditing",
      "display_name": "Auditing"
    },
    {
```

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

```
        "access_type": true,
        "name": "MonitoringSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "GSLBDomains",
        "display_name": "Domains"
      },
      {
        "access_type": true,
        "name": "GSLBServices",
        "display_name": "Services"
      },
      {
        "access_type": true,
        "name": "GSLBVirtualServer",
        "display_name": "Virtual Server"
      },
      {
        "access_type": true,
        "name": "NetScalerGateway",
```


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

```
        "display_name": "NetScaler Gateway"
      },
      {
        "access_type": true,
        "name": "ContentSwitching",
        "display_name": "Content Switching"
      },
      {
        "access_type": true,
        "name": "DNSDomainNames",
        "display_name": "DNS Domain Names"
      },
      {
        "access_type": true,
        "name": "NetworkDashboard",
        "display_name": "Instances Dashboard"
      },
      {
        "access_type": true,
        "name": "NetScalerSDWANWOInstances",
        "display_name": "NetScaler SD-WAN"
      },
```


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

```
    {
      "access_type": true,
      "name": "InstanceOperations",
      "display_name": "Instance Operations"
    },
    {
      "access_type": true,
      "name": "NetScalerInstances",
      "display_name": "NetScaler ADC"
    },
    {
      "access_type": true,
      "name": "NetScalerCPXDockerHost",
      "display_name": "Docker Hosts"
    },
    {
      "access_type": true,
      "name": "Reports",
      "display_name": "Reports"
    },
    {
      "access_type": true,
```


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

```
        "name": "Thresholds",
        "display_name": "Thresholds"
      },
      {
        "access_type": true,
        "name": "ReportingSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "Licenses",
        "display_name": "License Management"
      }
    ]
  }
}
```

アクセス ロールを作成するためのREST API

```
URL: https://<MAS_IP>/nitro/v2/config/rba_role

HTTPMETHOD: POST


Payload:
```

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

```
{

  "rba_role": {

    "name": "AppOwnerRole",

    "description": "ExampleCompany App Owner Role",

    "policies": [

      "AppOwnerAccessPolicy"

    ]

  }
```

新しいGSLB StyleBookをアップロードするためのREST API

```
URL: https://<MAS_IP>/stylebook/nitro/v2/config/stylebooks

HTTPMETHOD: POST



Payload:

{

    "stylebook": {

      "file_name": "my-own-gslb.yaml",

      "source": "bmFtZTogZ3NsYi1kbnMtZG9tYW...aXRvcm5hbWU=",

      "encoding": "base64"

    }

  }
```

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

注:

StyleBookの名前は、お使いのシステムで変更される可能性があります。

グループを作成し、選択したインスタンスとStyleBookを割り当てるためのREST API

```
URL: https://<MAS_IP>/nitro/v2/config/mpsgroup

HTTPMETHOD: POST



Payload:

{

  "mpsgroup": {

    "id": "",

    "name": "AppOwnerGroup1",

    "description": "ExampleCompany App Owner Group",

    "roles": [

      "AppOwnerRole"

    ],

    "enable_session_timeout": false,

    "assign_all_devices": false,

    "ass ign_all_apps": false,

    "application_names_with_regex": [



    ],

    "standalone_instances_id": [
```

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

```
      "72c178da-47df-4426-9acc-cd6316f92506",
      "c948061e-6240-4062-931c-f6988ef36e3b"
    ],
    "application_list": [


    ],
    "permission": "none",
    "application_names": [


    ],
    "authscope_props": [
      {
        "propname": "configuration_template_id",
        "propvalues": [
          "NONE"
        ]
      },
      {
        "propname": "dns_domain_entry_id",
        "propvalues": [
          "cf6631e5-2f56-4bb1-b0a5-90fabfc0e3e2",
          "b268905c-522d-47e3-a2ca-3f8d8a754373"
```

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

```
        ]
      },
      {
        "propname": "stylebook_id",
        "propvalues": [
          "gslbbb963abe85936913035e1d4dd14b56f7",
          "moni72fad4494466d102b19c18ac329fa9f3"
        ]
      }
    ],
    "tenant_id": "6d024111-6636-4571-a250-d47b31aba7a8"
  }
}
```

注:

上記のAPIペイロードで使用するDNSドメイン名およびGSLB StyleBookのIDを取得するには、エンティティ名に対応するIDを照会するために、通常のNetScaler Console APIを使用できます。たとえば、「app1.acme.com」というDNSドメインのIDを取得するには、次のNetScaler Console REST APIを使用できます。

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry?filter=name:
app1.acme.com

HTTPMETHOD: GET
```

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

```
The ID of this domain can be extracted from the following response.

{

  "errorcode": 0,

  "message": "Done",

  "operation": "get",

  "resourceType": "dns_domain_entry",

  "username": "nsroot",

  "tenant_name": "Owner",

  "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",

  "resourceName": "",

  "dns_domain_entry": [

    {

      "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",

      "name": "app1.acme.com",

      "id": "3e3d85ea-1c21-49b2-97f4-60fccdbae2e0",

      "description": "app1 domain name"

    }

  ]

}
```

同様に、名前空間がcom.citrix.adc.stylebook、バージョンが1.0、名前が`my-own-gslb`であるStyleBookのStyleBook IDを取得するには、次のAPIを使用できます。

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

```
URL: https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks?filter=name:my-own-gslb,namespace:com.citrix.adc.stylebooks,version:1.0

HTTPMETHOD: GET
```

応答には、StyleBookの詳細とそのID属性が含まれています。


```
{

  "stylebooks": [

    {

      "author": null,

      "builtin": "false",

      "builtins": "{"netscaler.nitro.config": "10.5"}",

      "deprecate": "false",

      "description": " This StyleBook is used to configure one or a number of NetScalers in different sites into a GSLB setup. It is assumed that the SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is already configured on the appliance.",

      "display_name": "HTTP/SSL LoadBalancing StyleBook",

      "filename": "my-own-gslb.yaml",

      "hide": null,

      "id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",

      "imported_by": "",

      "imported_datetime": "2018-05-25 17:20:32.848902",

      "name": "my-own-gslb",

      "namespace": "com.citrix.adc.stylebooks",
```


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

```
      "pkg_id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
      "primary_keys": "["name"]",
      "private": "false",
      "recompile": "false",
      "schema_version": "1.0",
      "source": "LS0tIApuYW1lOiBsYgpuYW1lc…",
      "system": null,
      "tags": "",
      "tenant_id": null,
      "user_sb": "false",
      "version": "1.0"
    },
    {
      …
    }
  ]
}
```


注:

上記のAPIは、フィルターに一致するStyleBookのリストを返します。IDを取得するには、応答から正しいStyleBook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.

システムユーザーを作成するためのREST API

注：

この手順はオプションです。

```
URL: https://<MAS_IP>/nitro/v2/config/mpsuser

HTTPMETHOD: POST



Payload:

{

  "mpsuser": {

    "name": "John",

    "password": "welcome",

    "external_authentication": false,

    "enable_session_timeout": false,

    "groups": [

      "AppOwnerGroup1"

    ]

  }

}
```

アプリケーション所有者向けのワークフロー

ユーザーは、資格情報を使用してアプリケーションユーザーとしてログオンする必要があります。ユーザーは、独自のDNSドメイン名を作成し、新しいGSLB StyleBookを使用するために、このタスクに従う必要があります。

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

1. NetScaler Consoleで、**設定 > ドメイン名**に移動します。
2. **追加**をクリックして新しいDNSドメインを作成します。NetScaler ConsoleでDNSドメインを作成します。

   DNSドメイン名を作成する(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-8.png)

   注：

   管理者として、これらのドメイン名を作成し、ユーザーグループに割り当てることもできます。

3. **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**をクリックします。
4. アプリケーションの名前を入力し、カテゴリを選択します。**StyleBookから新しいアプリケーションを作成**を選択し、**OK**をクリックします。選択したインスタンスに構成を展開するには、**自分のGSLB StyleBook**を選択します。

   アプリケーションを定義する(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-10.png)
5. StyleBook内のすべてのパラメーターに必要な値を入力します。

   a. リストからドメイン名を選択します。
   b. 必要に応じて、アプリケーションのGSLBサイトを追加します。
   c. すべてのGSLBサイトでターゲットのNetScalerインスタンスを選択します。
   d. GSLB構成を作成するには、**作成**をクリックします。

      GSLB構成を作成(/en-us/netscaler-console-service/media/rbac-on-gslb-domain-dns-names-11.png)

   注:

   StyleBookパラメーター「DNS Domain Name」には、NetScaler Consoleでユーザーに属するDNSドメインのリストのみが表示されます。

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

アプリケーション所有者ワークフロー用のNetScaler Console REST API

NetScaler Consoleにログオンするための REST API

```
URL: http: //<MAS_IP>/nitro/v2/config/login

HTTPMETHOD: POST



Payload:

{

  "login": {

    "username": "<USER_NAME>",

    "password": "<PASSWORD>",

    "session_timeout": 1800

  }

}
```

DNSドメイン名を作成するための REST API

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry

HTTP METHOD: POST

PAYLOAD: {"dns_domain_entry":{"name":"app1.acme.com","description":"app1
acme domain"

}

}
```

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

StyleBookを使用してアプリケーションを作成するためのREST API

```
URL: https://<MAS_IP>/nitro/v2/config/application

HTTPMETHOD: POST



Payload:

{

  "params": {

    "action": "app_discovery"

  },

  "application": {

    "id": "",

    "name": "app1",

    "app_c ategory": "ITOps",

    "stylebook_params": "{"name":"my-own-
gslb","namespace":"com.citrix.adc.stylebooks","version":"1.0","configpack_
payload":{"parameters":{"name":"app1","domain-
name":"app1.acme.com",]"ttl":"30","algorithm":"ROUNDROBIN","protocol":"HTT
P","sites":[{"name":"site1","ipaddress":"6.5.6.77","virtual-
ip":"88.6.5.44","virtual-port":"80"}]},"targets":
[ {"id":"72c178da-47df-4426-9acc-cd6316f92506"}, {"id":"0e4d0789-
bffe-4266-ba1c-09adfc61db4e"}, {"id":"b5af4455-3f06-4f56-
b0cb-3d9f868c1f94"}]}}"

  }

}
```

上記のペイロードでは:

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

- 「stylebook_params」には、使用するStyleBookの名前、名前空間、およびバージョンが含まれています。
- 「configpack_payload」には、上記の同等のGUIフォームに示されているStyleBookの入力済みパラメーターが含まれています。NetScaler Consoleは、ユーザーがアクセスできるDNSドメイン名のみがパラメーター「domain-name」の値として使用できることを保証します。
- 「targets」には、GSLB構成が展開されるNetScaler IDのリスト（GSLBサイト上のNetScalerインスタンス）が含まれています。

NetScalerの管理IPアドレスが与えられた場合にNetScaler IDを取得するには、以下のNetScaler Console APIを使用できます。

```
URL: https://<MAS_IP>/nitro/v2/config/ns?filter=ip_address:
192.168.153.162

HTTPMETHOD: GET
```

応答ペイロードには、このNetScaler®に関する情報（そのIDを含む）が含まれています。

```
{

  "errorcode": 0,

  "message": "Done",

  …..."tenant_id": "ec0eb868-0d6b-4729-bfbd-3005dd2694c1",

  "resourceName": "",

  "ns": [

    {

      "manufacturedate": "9/30/2009",

      "is_grace": "false",

      "hostname": "youcef-ns",

      "std_bw_config": "0",

      "gateway_deployment": "false",
```

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

```
      "gateway_ipv6": "",
      "ha_master_state": "Primary",
      "instance_available": "0",
      "device_finger_print": "",
      "instance_state": "Down",
      "reason": "Device not reachable",
      "name": "",
      "ent_bw_available": "0",
      "description": "",
      "id": "da9ffff2-c100-45f1-a913-c542718338b2",
      "mgmt_ip_address": "192.168.153.162",
      ….
    }
  ]
}
```

StyleBookを作成する

ファイル「my-own-gslb.yaml」のStyleBookの全内容は以下のとおりです。 このカスタムStyleBookはそのまま使用することも、必要に応じてカスタマイズして、必要なGSLB構成を生成することもできます。DNS名機能を利用するには、このStyleBookの重要なパラメータである「domain-name」がどのStyleBookにも存在している必要があります。

```
name: my-own-gslb
namespace: com.citrix.adc.stylebooks
version: "1.0"
```

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

```
display-name: My own GSLB StyleBook

description: This StyleBook is used to configure one or a number of
NetScalers in different sites into a GSLB setup. It is assumed that the
SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is
already configured on the appliance.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

  -

    namespace: com.citrix.adc.commontypes

    version: "1.0"

    prefix: cmtypes

parameters:

  -

    name: name

    label: Application Name

    type: string

    required: true

    key: true
```

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

```
-
  name: domain-name
  label: DNS Domain Name
  description: GSLB DNS Domain Name
  type: string
  required: true
  allowed-dynamic-values:
    source: local
    resource-type: dns_domain_entry


-
  name: ttl
  label: TTL for the Domain
  description: Time-To-Live value (number of seconds) for the Domain
  type: number
  default: 30


-
  name: algorithm
  label: LB Algorithm
  description: Global Load Balancing Algorithm
  type: string
```

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

```
    default: ROUNDROBIN
    allowed-values:
      - ROUNDROBIN
      - STATICPROXIMITY
      - SOURCEIPHASH


  -
    name: protocol
    label: Protocol
    description: The protocol of the GSLB VIP
    type: string
    default: HTTP
    allowed-values:
      - HTTP
      - FTP
      - TCP
      - UDP
      - SSL
      - SSL_BRIDGE
      - SSL_TCP
      - NNTP
      - ANY
```

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

```
      - SIP_UDP
      - SIP_TCP
      - SIP_SSL
      - RADIUS
      - RDP
      - RTSP
      - MYSQL
      - MSSQL
      - ORACLE


  -
    name: monitor
    label: LB Monitor
    description: Monitor to be bound to the GSLB service
    type: cmtypes::monitor


  -
    name: sites
    label: GSLB Sites
    description: Provide information about the GSLB Sites
    type: object[]
    required: true
```

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

```
    parameters:

      -

        name: name

        label: Site Name

        type: string

        required: true

      -

        name: ipaddress

        label: Site IP Address

        description: The IP Address of this Site. Use a SNIP IP address on
the site's appliance.

        type: ipaddress

        required: true

      -

        name: public-ipaddress

        label: Site Public IP Address

        description: The Public IP Address of this Site. It NATs to the
Site's IP address

        type: ipaddress

      -

        name: virtual-ip

        label: Site VIP IP

        description: The IP Address for the GSLB Service on this site (The
```

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

```
VIP on this Site)

        type: ipaddress

        required: true

      -

        name: virtual-port

        label: Site VIP Port

        description: The port number for the GSLB Service (VIP) on this
site

        type: tcp-port

        default: 80



components:

  -

    name: enable-gslb-comp

    type: ns::nsfeature

    description: Enables the GSLB feature

    meta-properties:

      action: enable

    properties:

      feature: ["GSLB", "LB"]

  -

    name: gslb-monitor-comp

    type: cmtypes::monitor
```

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

```
    condition: $parameters.monitor

    properties:

      monitorname: $parameters.name + "-" +
$parameters.monitor.monitorname + "-gslbmon"

      type: $parameters.monitor.type

      destip?: $parameters.monitor.destip

      destport?: $parameters.monitor.destport

      httprequest?: $parameters.monitor.httprequest

      send?: $parameters.monitor.send

      customheaders?: $parameters.monitor.customheaders

      respcodes?: $parameters.monitor.respcodes

      recv?: $parameters.monitor.recv

      lrtm?: $parameters.monitor.lrtm

      secure?: $parameters.monitor.secure

      interval?: $parameters.monitor.interval

      interval_units?: $parameters.monitor.interval_units

      resptimeout?: $parameters.monitor.resptimeout

      retries?: $parameters.monitor.retries

      downtime?: $parameters.monitor.downtime

  -

    name: gslb-vserver-comp

    type: ns::gslbvserver
```

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

```
    description: Creates a GSLB VServer config object
    properties:
      name: $parameters.name + "-gslbvserver"
      servicetype: $parameters.protocol
      lbmethod: $parameters.algorithm
    components:
      -
        name: gslb-domain-comp
        type: ns::gslbvserver_domain_binding
        properties:
          name: $parent.properties.name
          domainname: $parameters.domain-name
          ttl: $parameters.ttl
-
    name: gslb-site-comp
    type: ns::gslbsite
    description: Creates a GSLB Site config object
    repeat: $parameters.sites
    repeat-item: site
    properties:
      sitename: $parameters.name + "-" + $site.name + "-gslbsite"
      siteipaddress: $site.ipaddress
```

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

```
      publicip?: $site.public-ipaddress

    components:

      -

        name: gslb-service-comp

        type: ns::gslbservice

        description: Creates a GSLB Service

        properties:

          servicename: $parameters.name + "-" + $site.name + "-
gslbservice"

          ip: $site.virtual-ip

          servicetype: $parameters.protocol

          port: $site.virtual-port

          sitename: $parent.properties.sitename

        components:

          -

            name: gslb-vserver-service-binding-comp

            type: ns::gslbvserver_gslbservice_binding

            description: Creates a Binding between the GSLB vserver and
the GSLB Service

            properties:

              name: $components.gslb-vserver-comp.properties.name

              servicename: $parent.properties.servicename

          -
```

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

```
            name: gslb-service-monitor-binding-comp

            type: ns::gslbservice_lbmonitor_binding

            description: Creates a Binding between the GSLB service and
the GSLB monitor

            condition: $parameters.monitor

            properties:

              servicename: $parent.properties.servicename

              monitor_name: $components.gslb-monitor-
comp.properties.monitorname
```

StyleBookで特殊文字をリテラル形式で許可する

StyleBookの定義では、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ます。

StyleBookでは、逐語的な文字列を使用してNetScalerポリシー式をリテラル形式で含めることができます。ポリシー式には通常、特殊文字が含まれています。逐語的な文字列を使用しない場合、文字列を部分文字列に分割して特殊文字をエスケープする必要があります。

逐語的な文字列を作成するには、次のように特殊文字の間に文字列をカプセル化します。

`~{string}~`

StyleBook式で逐語的な文字列を使用できます。

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的な文字列の終わりを示すためです。

例：

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

```
---

name: test-deny-url

namespace: citrix.adc.stylebooks

version: "6.2"

display-name: StyleBook for creating an AppFw profile

description: This Stylebook configures an AppFw config.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "13.0"

parameters:

  -

    name: name

    type: string

    required: true

substitutions:

 default-deny-urls-regex:

     "Command_injection_attack": str("([ /=]|\\t|\\n)(ls|cat)([ ;'" + "\\
\"&].*)?$")

     "Command_injection_attack2": ~{([ /=]|\t|\n)(ls|rm|cat)([ ;'\"&].*)?
$}~
```

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

```
components:

  -

    name: appfw-profile-comp

    type: ns::appfwprofile

    properties:

      name: $parameters.name

      type: ["XML"]

    components:

          -

            name: appfw-profile-denyurl-default-binding-subcomp-all

            type: ns::appfwprofile_denyurl_binding

            properties:

                name: $parent.properties.name

                denyurl?: $substitutions.default-deny-urls-
regex["Command_injection_attack"]

                state?: "ENABLED"

          -

            name: appfw-profile-denyurl-default-binding-subcomp-all2

            type: ns::appfwprofile_denyurl_binding

            properties:

                name: $parent.properties.name

                denyurl?: $substitutions.default-deny-urls-
regex["Command_injection_attack2"]
```

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

```
                state?: "ENABLED"
```

この例では、`default-deny-urls-regex` の置換は逐語的な式を持っています。

- `"Command_injection_attack": str("([ /=]|\\t|\\n)(ls|cat)([ ;'" + "\\\"&].*)?$")`: StyleBookはこれを正規表現として処理します。
- `"Command_injection_attack2": ~{([ /=]|\t|\n)(ls|rm|cat)([ ;'\"&].*)?$}~`: StyleBookはこれを逐語的な式として処理します。この文字列内の特殊文字はリテラル形式になります。

複数の逐語的な文字列を連結する

逐語的な文字列を通常の文字列や補間を含む文字列と連結できます。その際、StyleBookは逐語的な文字列のみ解釈をスキップします。文字列間にプラス (+) 演算子を使用して連結します。

例：

```
value: "~{\"id\": \"}~ + %{$atom.key}% + ~{\", \"value\": \"}~ + %
{$atom.value}% + ~{\"}~"
```

この例では、`%{$atom.key}%` と `%{$atom.value}%` が解釈されます。そして、残りの解釈はスキップされます。

データソースの管理

NetScaler Consoleでデータソースを定義すると、StyleBook構成の作成または更新時に、外部ソースからのデータを入力として使用できます。そうしないと、StyleBookで必要とされる各入力を明示的に提供する必要があります。NetScaler Consoleでは、管理対象のNetScalerインスタンスをStyleBook構成への入力のデータソースとして使用できます。構成の作成または更新時に入力として機能するカスタムデータソースを定義することもできます。

コレクション: データベースが複数のテーブルを持つように、データソースは複数のコレクションを含むことができます。各コレクションには名前があり、類似したタプルのリストが含まれています。各タプルはキーと値のペアのセットです。たとえば、コレクションは、各タプルが(`<name>:<value>, <virtualip>:<value>`)を持つタプルで構成できます。

データソースタイプ: データソースタイプは、データが取得されるソースのタイプを区別します。NetScaler Consoleは2つのデータソースタイプをサポートしています。

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

- **managed-adc** - これは組み込みのデータソースです。NetScaler Consoleによって管理されている既存のNetScalerからデータを取得するために使用されます。詳細については、「NetScalerインスタンスをデータソースとして使用する」を参照してください。

  ターゲットのNetScalerインスタンスをデータソースとして使用することもできます。詳細については、「ターゲットNetScalerインスタンスをデータソースとして使用する」を参照してください。

- **カスタムデータソースタイプ** - NetScaler® Consoleにデータがローカルに投入されるカスタムデータソースタイプを定義できます。

  データソースタイプ `Environment` を検討します。このデータソースタイプには、2つのデータソース `Production` と `Staging` があります。StyleBook構成を作成する際、StyleBookユーザーはタイプ `Environment` の任意のデータソースを選択できます。選択に応じて、`Production` または `Staging` のいずれかのデータ値がStyleBookへの入力として使用されます。

  詳細については、「カスタムデータソースを使用する」を参照してください。

コレクションスキーマ: コレクションタプルに格納できるデータのタイプを記述します。コレクションスキーマは、タプル内の各キーの名前とその予期されるタイプを記述します。データベースの類推では、コレクションスキーマは、各列が明確に定義された名前とサポートするタイプを持つテーブルのデータベーススキーマに似ています。

次の図は、データソースのさまざまなコンポーネントとそれらの相互関係を一般的に表したものです。

データソースとしてNetScalerインスタンスを使用する

管理対象のNetScalerインスタンスをデータソースとして使用できます。`managed-adc` は、NetScaler Consoleでデータソースとしてすぐに使用できる組み込みのデータソースタイプです。NetScaler Console内の各管理対象NetScalerインスタンスは、デフォルトでデータソースです。設定パックの作成時にNetScaler Consoleによって管理されている既存のNetScalerからデータが必要な場合は、StyleBookでこれらのデータソースの使用を開始できます。

StyleBookの定義で、`datum` 組み込みタイプパラメータを指定します。StyleBookでデータソースタイプを使用できます。StyleBookユーザーは、そのソースからデータを取得するために使用できるデータソースを選択できます。

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

コレクションなしで組み込みデータソースを使用する

```
parameters:

  - name: selected-adc

    label: Select an existing NetScaler

    type: datum

    required: true

    data-source:

      type: managed-adc
```

この例では、`datum` パラメータを使用して、NetScaler Consoleによって管理されている任意のNetScalerインスタンスを選択します。`managed-adc` 組み込みデータソースを使用すると、NetScaler Consoleによって管理されている任意のNetScalerインスタンスからデータを取得できます。

StyleBookでは、選択したNetScalerインスタンスから任意の構成にアクセスできます。そして、その構成を、同じNetScalerまたは異なるNetScalerインスタンスで構成を作成または更新する際に使用できます。これは、選択したターゲットNetScalerインスタンスによって異なります。

データソースからコレクションにアクセスする:

選択したNetScalerインスタンスでコレクションにアクセスするには、次の式を使用します。

```
$parameters.selected-adc.collections.<collection-name>
```

例:

```
$parameters.selected-adc.collections.lbvserver
```

この式は、選択したNetScalerインスタンス上の `lbvserver` エンティティのリストを返します。たとえば、このリストを反復処理して、特定の条件を満たす特定の `lbvserver` を選択できます。

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

コレクションなしのStyleBookの例

```
name: add-vservers-from-managed-adc-instances

namespace: com.citrix.adc.stylebooks

version: "1.0"

schema-version: "1.0"



import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

    -

      name: selected-adc

      label: Select a NetScaler instance

      type: datum

      required: true

      data-source:

        type: "managed-adc"



components:
```

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

```
-

  name: sslvserver-comp

  type: ns::sslvserver

  repeat: $parameters.selected-adc.collections.lbvserver

  repeat-item: lbvs

  repeat-condition: $lbvs.attributes.servicetype == "SSL"

  properties:

    name: $lbvs.attributes.name

    ssl2: DISABLED

    ssl3: DISABLED

    tls1: DISABLED

    tls11: ENABLED

    tls12: ENABLED
```

設定パックGUIには、NetScaler Consoleによって管理されているNetScalerインスタンスが表示され、StyleBookユーザーは設定パックの作成または更新時に任意のNetScalerを選択できます。

このStyleBookは、選択したNetScalerを使用し、すべての `lbvserver` エンティティを反復処理します。SSL仮想サーバーを選択し、各仮想サーバーで許可されるSSLプロトコルバージョンを設定します。

次の式を使用すると、NetScalerインスタンス内の `lbvserver` エンティティのリストを反復処理できます。

```
repeat: $parameters.selected-adc.collections.lbvserver
```

- `collections`: NetScalerインスタンス上のすべてのエンティティタイプを指します。例えば、`csvserver`、`lbmonitor`、`servicegroup`などです。

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

- `lbvserver`: NetScalerインスタンス内のロードバランシング仮想サーバーエンティティのリストを指します。

コレクションで組み込みデータソースを使用する

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

この例では、`datum`パラメーターを使用して、ユーザーがNetScalerインスタンスと、`managed-adc`データソースタイプから特定の`lbvserver`の両方を選択できるようにします。

`parameters`セクションでコレクションタイプを定義すると、StyleBookユーザーはNetScalerインスタンスと、そのインスタンス上のコレクションから特定のエンティティを選択できます。

- [ ] **選択したアイテムの属性にアクセスする**:

StyleBookユーザーが仮想サーバーを選択すると、StyleBook内の次の式で、選択したアイテムの任意の属性にアクセスできます。

```
$parameters.selected-lbvserver.attributes.<attribute-name>
```

この例では、選択された`datum`は`lbvserver`です。したがって、NetScalerエンティティ`lbvserver`の任意の属性（例えば、`name`、`servicetype`、`ipv46`など）にアクセスできます。

例:

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

```
$parameters.selected-lbvserver.attributes.ipv46
```

この式は、選択されたロードバランシング仮想サーバーのIPを取得します。NetScalerエンティティ（コレクション）とその属性の詳細については、NetScaler NITRO APIリファレンスを参照してください。

コレクションから複数のアイテムを選択する:

以下のパラメーターセクションでは、StyleBookユーザーがコレクションの複数のアイテムを選択できます。

```
parameters:

  - name: selected-lbvservers

    label: Select existing lbvservers

    type: datum[]

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

この例では、datumパラメーターはデータソース配列を定義するために使用されます。ユーザーは、単一のNetScaler®インスタンスから、または複数のNetScalerインスタンスにわたって、1つ以上のlbvserverを選択できます。

以下のコードスニペットは、選択されたアイテムとその属性にアクセスする方法を示しています。

```
components:

  - name: sslvserver-comp

    type: ns::sslvserver

    repeat:
```

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

```
      repeat-list: $parameters.selected-lbvservers

      repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.name

      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

選択したアイテムの参照によるコレクションへのアクセス:

StyleBookユーザーが管理対象のNetScalerインスタンス上の特定のエンティティを選択できるようにするだけでなく、選択したNetScalerインスタンス上の同じまたは異なるコレクションから任意のエンティティにアクセスすることもできます。そのNetScalerインスタンス上の別のコレクションにアクセスするには、`components`セクションで次の式を使用します。

```
$parameters.selected-lbvserver.datasource.collections.<collection-name>
```

例:

```
$parameters.selected-lbvserver.datasource.collections.csvserver
```

この式は、選択したNetScalerインスタンスからコンテンツスイッチング仮想サーバーのリストを返します。

そして、次の式は、`lbvservers`と`servicegroups`間のすべてのバインディングのリストを返します。

```
$parameters.selected-
lbvserver.datasource.collections.lbvserver_servicegroup_binding
```

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

コレクションを含むStyleBookの例

以下は、管理対象のNetScalerインスタンスをデータソースとして使用する方法を示すStyleBookの例です。

```
name: bind-lb-to-servicegroup-using-ADC-as-datasource

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration where we allow the user to select an existing lbvserver on
the NetScaler using datum type parameter. Then a servicegroup for the
selected lb is created if it does not exist on the NetScaler. Finally, the
selected lbvserver is bound to the service "

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

  -

    name: selected-vserver

    label: "Select an Existing VServer"

    description: "Load Balancing Application Vservers to be bound to
service on the ADC"
```

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

```
    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver



components:

  -

    name: servicegroup-discovery-comp

    type: object

    repeat: $parameters.selected-
vserver.datasource.collections.servicegroup

    repeat-item: svcgrp

    repeat-condition: $svcgrp.attributes.servicegroupname ==
 $parameters.selected-vserver.attributes.name + "-svcgrp"

    properties:

      servicegroupname: $svcgrp.attributes.servicegroupname

  -

    name: servicegroup-creation-if-not-exists-comp

    type: ns::servicegroup

    condition: not exists($components.servicegroup-discovery-comp)

    properties:

      servicegroupname: $parameters.selected-vserver.attributes.name + "-
```

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

```
svcgrp"

      servicetype: $parameters.selected-vserver.attributes.servicetype

    components:

      -

        name: lbvserver-servicegroup-binding

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parameters.selected-vserver.attributes.name

          servicegroupname: $parent.properties.servicegroupname
```

このStyleBookでは、`components`セクションが、選択したロードバランシング仮想サーバー名と`svcgrp`を連結したものに一致するサービスグループ名を確認します。

選択したロードバランシング仮想サーバーの名前が`lbv1`の場合、このStyleBookは名前が`lbv1-svcgrp`のサービスグループを確認します。見つからない場合は、サービスグループ`lbv1-svcgrp`を作成し、`lbv1`仮想サーバーにバインドします。

次の式は、NetScalerインスタンス内のサービスグループのリストを取得します。

```
repeat: $parameters.selected-vserver.datasource.collections.servicegroup
```

この式では:

- `datasource`: NetScaler Consoleによって管理されている選択されたNetScalerインスタンスを指します。
- `collections`: NetScalerインスタンス内のすべてのエンティティを指します。
- `servicegroup`: NetScalerインスタンス内のサービスグループを指します。

コレクションデータのフィルタリング:

以下のパラメータセクションでは、StyleBook定義で組み込みデータソースコレクションにフィルタを指定する方法を説明します。これにより、StyleBookユーザーはフィルタリングされたコレクションから特定の項目を選択できます。

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

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver

      collection-filters:

        protocol: SSL
```

この例では、datumパラメータを使用して、ユーザーがNetScalerインスタンスと、managed-adcデータソースタイプからSSLプロトコルを持つ特定のlbvserverの両方を選択できるようにします。

StyleBookユーザーが仮想サーバーを選択した後、選択された項目の任意の属性は、前のセクションで説明したのと同じ方法でアクセスできます。

ターゲットのNetScalerインスタンスをデータソースとして使用する

設定のターゲットとなるNetScaler自体を、設定のデータソース入力として使用することもできます。このシナリオでは、ターゲットNetScaler上の既存の設定を参照して、そのNetScaler上に新しい設定を作成したい場合があります。

ターゲットインスタンスをデータソースとして使用する場合、StyleBookユーザーがNetScalerインスタンスを選択する必要がないため、`datum`組み込み型パラメータを使用する必要はありません。StyleBookの`components`セクションに、ターゲットNetScalerインスタンスからデータを取得する式を直接記述できます。

ターゲットNetScalerインスタンスから以下を取得するには、次の式を使用します。

- コレクション:

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

```
$current-target-as-datasource.collections.<collection-name>
```

例:

```
$current-target-as-datasource.collections.lbvserver
```

- 属性:

```
$current-target-as-datasource.collections.attributes.<attribute>
```

ターゲットNetScalerインスタンスをデータソースとして使用するStyleBookの例

ターゲットNetScalerインスタンスをデータソースとして使用する方法を示すStyleBookの例を次に示します。

```
---

name: lb-add-service-with-target-adc

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration."

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"
```

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

```
components:
  -
    name: servicegroup-comp
    type: ns::servicegroup
    properties:
      servicegroupname: "lb-demo-svcgrp"
      servicetype: "HTTP"


    components:
      -
        name: lbvserver-svg-binding
        type: ns::lbvserver_servicegroup_binding
        repeat: $current-target-as-datasource.collections.lbvserver
        repeat-item: lbvsrvr
        repeat-condition: $lbvsrvr.attributes.name == "lb-demo-lb"
        properties:
          name: $lbvsrvr.attributes.name
          servicegroupname: $parent.properties.servicegroupname
```

この例では、構成パックはターゲットNetScalerインスタンス内のロードバランシング仮想サーバーをチェックします。指定されたロードバランシング仮想サーバーのIPアドレスが一致した場合、名前とサービスグループ名を取得します。

ターゲットNetScalerインスタンスをデータソースとして(/en-us/netscaler-console-service/media/target-instance-as-datasource.png)

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

カスタムデータソースを使用する

(/ja-jp/netscaler-console-service/stylebooks/manage-data-sources/built-in-datasource.html)に加えて、入力データが複数の構成を作成するために繰り返し使用される場合、カスタムデータソースを定義して使用できます。入力データをNetScaler Consoleにデータソースとして保存できます。また、StyleBookユーザーが繰り返し入力を提供することなく、このデータを消費するようにStyleBookを変更できます。

StyleBook定義でカスタムデータソースを使用する前に、カスタムデータソースを定義するために以下を実行します。

1. データソースタイプを追加する(#add-a-data-source-type)。
2. データソースタイプの下にコレクションスキーマを追加する(#add-a-collection-schema-under-data-source-type)。
3. データソースを追加する(#add-a-data-source)。
4. コレクションデータを追加する(#add-a-collection-data)。

データソースを追加した後、StyleBook定義でこのデータソースを使用できます。詳細については、StyleBook定義でカスタムデータソースを使用するを参照してください。

データソースタイプを追加する

データを取得するソースを区別するために、データソースタイプを指定します。

1. **アプリケーション > 構成 > データソース**で。
2. **Data Source Type**を選択し、**Add**をクリックします。
3. データソースタイプの**Name**と**Description**を指定します。
4. **Proceed**をクリックして**Data Source Type**を保存します。**Close**をクリックして、変更を保存せずにワークフローを終了します。

この例では、データソースタイプは**Environment**に設定されています。このタイプは、アプリケーション環境をデータソースとして定義するために使用できます。

データソースタイプの下にコレクションスキーマを追加する

データソースタイプ を追加した後、""データソースタイプ** の **コレクションスキーマ** を追加する画面が表示されます。

1. **追加**をクリックします。
2. コレクションスキーマの**コレクション名**を指定します。

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

3. **説明**を入力します。
4. 必要に応じて、**属性の詳細**の下に属性（名前とそのタイプ）を追加します。
5. **作成**をクリックします。

コレクションタイプ(/en-us/netscaler-console-service/media/add-collection-type.png)

この例では、**App-virtual-servers**コレクションスキーマには4つの属性があります。したがって、保存したいコレクションには、設定されたデータ型のこれらの属性が必要です。

データソースを追加する

特定のデータソースタイプに対してデータソースを定義します。

1. **アプリケーション > 設定 > データソース**に移動します。
2. **データソース**タブを選択し、**追加**をクリックします。
3. **名前**を指定します。
4. **データソースタイプ**を選択し、**説明**を入力します。
5. **続行**をクリックして**データソース**を保存します。**閉じる**をクリックすると、変更を保存せずにワークフローを終了します。

この例では、**本番環境**がデータソースとして追加されています。

コレクションデータを追加する

データソースを追加すると、**データソース**のデータを入力する画面が表示されます。**コレクションスキーマ**のリストが表示されます。

1. コレクションデータを追加する**コレクションスキーマ**を選択します。
2. **コレクションデータの管理**をクリックします。
3. コレクションにデータを追加します。データを1つずつ追加するか、CSVファイルをアップロードできます。CSVファイルをアップロードする際は、列名がコレクションスキーマの属性名と一致していることを確認してください。
4. **OK**をクリックします。

コレクションなしでカスタムデータソースを使用する

次の`parameters`セクションでは、コレクションなしでStyleBook定義にカスタムデータソースを定義する方法について説明します。

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

```
parameters:

    - name: selected-environment

      label: Select a custom datasource environment

      type: datum

      required: true

      data-source:

        type: "Environment"
```

構成パックGUIには適用可能なデータソースが表示され、StyleBookユーザーはそれらのいずれかを選択して構成パックを作成できます。

この例では、`Production` データソースを使用してデータを取得します。

`Environment` データソースタイプで、`App-virtual-servers` コレクションタイプにアクセスするには、次の式を使用します。

```
$parameters.selected-environment.collections.App-virtual-servers
```

スニペットの例:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    repeat: $parameters.selected-environment.collections.App-virtual-
servers

    repeat-item: app

    properties:
```

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

```
    name: $app.attributes.Name + "-lb"
    ipv46: ip($app.attributes.IPv46 )
    port: $app.attributes.Port
    servicetype: $app.attributes.Protocol
  components:


    -
      name: servicegroup-comp
      type: ns::servicegroup
      properties:
        servicegroupname: $parent.properties.name + "-svcgrp"
        servicetype: $parent.properties.servicetype


      components:
        -
          name: lbvserver-svg-binding
          type: ns::lbvserver_servicegroup_binding
          properties:
            name: $parent.parent.properties.name
            servicegroupname: $parent.properties.servicegroupname
```

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

コレクションでカスタムデータソースを使用する

以下の `parameters` セクションでは、StyleBook 定義でカスタムデータソースを定義する方法について説明します。これにより、StyleBook ユーザーはコレクションの特定の項目を選択できます。

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

この例では、`datum` パラメータを使用してカスタムデータソースを定義します。`Production` データソースを使用して、`App-virtual-servers` コレクションスキーマからデータを取得します。

`Environment` データソースタイプで、`App-virtual-servers` コレクションからプロトコルにアクセスするには、次の式を使用します。

```
$parameters.selected-app-vserver.attributes.Protocol
```

スニペットの例:

```
components:

  - name: lbvserver-comp

    type: ns::lbvserver

    properties:
```

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

```
      name: $parameters.selected-app-vserver.attributes.Name

      ipv46: $parameters.selected-app-vserver.attributes.IPv46

      port: $parameters.selected-app-vserver.attributes.Port

      servicetype: $parameters.selected-app-vserver.attributes.Protocol
```

`parameters` セクションでコレクションタイプを定義すると、StyleBook ユーザーはデータソースとコレクションを選択できます。

コレクションから複数の項目を選択する:

以下のパラメータセクションでは、StyleBook ユーザーがコレクションの複数の項目を選択できます。

```
parameters:

  - name: selected-app-vservers

    label: Select app-vservers from the collection

    type: datum[]

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

この例では、datum パラメータを使用してカスタムデータソース配列を定義します。ユーザーは、単一のデータソースまたは複数のデータソースから「App-virtual-servers」コレクションの項目を1つ以上選択できます。

以下のコードスニペットは、選択した項目とその属性にアクセスする方法を示しています。

```
components:

  -
```

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

```
    name: lbvserver-comp

    type: ns::lbvserver

    repeat:

    repeat-list: $parameters.selected-app-vservers

    repeat-item: vserverObj

     properties:

       name: $vserverObj.attributes.Name

       ipv46: $vserverObj.attributes.IPv46

       port: $vserverObj.attributes.Port

       servicetype: $vserverObj.attributes.Protocol
```

コレクションデータのフィルタリング:

以下のパラメータセクションでは、StyleBook 定義でカスタムデータソースコレクションにフィルタを指定する方法について説明します。これにより、StyleBook ユーザーはフィルタリングされたコレクションから特定の項目を選択できます。

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

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

```
collection-filters:

  Protocol: SSL
```

この例では、datum パラメータを使用してカスタムデータソースを定義します。これは、Environment タイプのデータソースを使用して、App-virtual-servers コレクションスキーマからフィルタリングされたデータを取得します。

StyleBook ユーザーが仮想サーバーを選択した後、選択されたアイテムの任意の属性に、前のセクションで説明したのと同じ方法でアクセスできます。

APIを使用してStyleBookから構成を作成する

StyleBookを構築したら、NetScaler Console GUIを使用するか、NetScaler Console APIを使用してインポートする必要があります。インポート時にNetScaler ConsoleがStyleBookを検証します。検証が成功すると、StyleBookはNetScaler ConsoleのStyleBookカタログに表示され、構成の作成に使用できるようになります。

このStyleBookに基づいて構成を作成するために、StyleBook APIを使用できるようになりました。cURLコマンドラインツールやPostman Chromeブラウザ拡張機能など、任意のツールを使用してNetScaler ConsoleにHTTPリクエストを送信できます。

注：

StyleBook APIは、開発者ポータルでOpenAPI仕様を使用して完全に文書化されています。

例1

ロードバランシング仮想サーバーを作成するためのStyleBookで作成された`lb-vserver` StyleBookを検討してください。このStyleBookから構成パックを作成するには、次のREST APIを使用します。

HTTPメソッド: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

リクエストヘッダー:

コンテンツタイプ: application/json

アクセプト: application/json

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

リクエストボディペイロード:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

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

このHTTPリクエストでは、ID 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 Consoleから取得されます。

NetScaler Consoleによって管理されているインスタンスのIDを取得するには、NetScaler Console APIを使用できます。たとえば、IPアドレスが192.168.153.160であるNetScalerインスタンスのインスタンスIDを取得するには、次のAPIを使用できます。

HTTPメソッド: GET

URL: `https://<IP>/nitro/v2/config/ns?filter=ip_address:192.168.153.160`

リクエストヘッダー:

受け入れ: application/json

応答にはJSONペイロードにIDが含まれています:

予期される応答ヘッダー (成功時):

200 OK

コンテンツタイプ: application/json

予期される応答本文 (成功時):

```
{

  "errorcode": 0,

  "message": "Done",

  "operation": "get",

  "resourceType": "ns",

  "username": "nsroot",

  "tenant_name": "Owner",

  "resourceName": "",

  "ns":
```

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

```
  [
    {
    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
   }
 ]
}
```

構成（構成パック）が正常に作成されると、次のHTTP応答が返されます:

予期される応答ヘッダー (成功時):

202 OK

コンテンツタイプ: application/json

予期される応答本文 (成功時):

```
{
  "job":
  {
    "job_id": "1460806080"
  }
}
```

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

ID 1460806080 を使用して一意に識別される最初のジョブが作成されました。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。

ジョブステータスを照会するには、次のURLを使用できます。

`https://<IP>/stylebook/nitro/v2/config/jobs/<jobid>`

例2

同じStyleBookを使用して、別の構成または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アドレスを指定します。負荷分散方法として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。

HTTPメソッド: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

リクエストヘッダー:

コンテンツタイプ: application/json

アクセプト: application/json

リクエストボディペイロード:

```
{

  "configpack":

  {

    "parameters": {

      "name": "lb1",

      "vip-ipaddress": "10.102.117.31",

      "lb-alg": "LEASTCONNECTION"

    },
```

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

```
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "instance_id": "abcdee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

このHTTPリクエストでは、IPアドレス10.102.117.31を持つ負荷分散仮想サーバーlb1が、ID「deecee30-f478-4446-9741-a85041903410」と「abcdee30-f478-4446-9741-a85041903410」を持つ2つのNetScalerインスタンス上に作成されます。

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。

予期される応答ヘッダー (成功時):

202 OK

コンテンツタイプ: application/json

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

予期される応答ボディ（成功時）：

```
{

    "job": {

        "job_id": "165769629"

    }

}
```

この新しい構成パックには、165769629という異なるID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。REST APIを使用して、このStyleBookから次のように構成パックを作成します。

HTTPメソッド： POST

URL： `https://<IP>/stylebook/nitro/v2/config/configpacks`

リクエストヘッダー：

コンテンツタイプ: application/json

アクセプト: application/json

リクエストボディペイロード：

```
{

  "configpack":

  {

    "parameters":

    {
```

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

```
      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers": ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
    },
    "targets":
    [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abcdefgi-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "basic-lb-config",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
}
```

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

予期される応答ヘッダー（成功時）：

202 OK

コンテンツタイプ: application/json

予期される応答ボディ（成功時）：

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

このHTTPリクエストでは、負荷分散構成が2つのNetScalerインスタンスで実行されます。これらのNetScalerインスタンスにログオンして、仮想サーバーと2つのサービスがバインドされたサービスグループが作成されているかどうかを確認できます。

例 4

複合StyleBookの作成で作成した複合StyleBook **composite-example** を検討してください。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。

HTTPメソッド: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

リクエストヘッダー:

コンテンツタイプ: application/json

受諾: application/json

リクエストボディペイロード:

```
{

  "configpack":

  {
```

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

```
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
    },
    "targets":
    [
     {
      "id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "id": "abcdefgg-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "composite-example",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
```

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

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。

予期される応答ヘッダー (成功時):

202 OK

コンテンツタイプ: application/json

予期される応答ボディ (成功時):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

構成の更新

構成を更新するには、次のAPIを使用できます。ここでは、IPアドレス10.102.29.54を持つバックエンドサーバーが、ロードバランシング仮想サーバー`myapp:に追加されます。

HTTPメソッド: PUT

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks/<configpackid>`

リクエストヘッダー:

コンテンツタイプ: application/json

受け入れ: application/json

リクエストボディペイロード:

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

```
{
  "configpack": {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
  },
  "targets":
   [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abdcedff-d589-4557-8632-a74032802412"
     }
   ]
  }
}
```

構成パックの更新が成功すると、次のHTTP応答が受信されます。

予期される応答ヘッダー (成功時):

202 OK

コンテンツタイプ: application/json

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

予期される応答ボディ (成功時):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

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、次のように構成パックを削除するためのAPIを使用できます。

設定パックの削除が成功すると、次のHTTP応答が受信されます。

HTTPメソッド: DELETE

URL: `https://<DNS-or-IP>//stylebook/nitro/v2/config/configpacks/<configpackid>`

リクエストヘッダー:

受諾: application/json

予期される応答ヘッダー (成功時):

202 OK

コンテンツタイプ: application/json

予期される応答ペイロード (成功時):

```
{

    "job": {

        "job_id": "3628681382"

    }
```

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

```
}
```

NetScalerインスタンスにログオンし、この設定パックの一部であるすべての構成オブジェクトが削除されていることを確認します。

すべてのインスタンスからではなく、特定のNetScalerインスタンスから構成を削除するには、構成の更新で構成パックの更新操作を使用します。JSONペイロードの`targets`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 を使用して構成を作成する

このStyleBookに基づいて構成を作成するには、StyleBook APIを使用します。cURLコマンドラインツールやPostman Chromeブラウザ拡張機能など、任意のツールを使用してNetScaler ConsoleにHTTPリクエストを送信できます。

証明書とキーファイルをアップロードするために、NetScaler ConsoleにSSL証明書と証明書キーファイルをアップロードするためのStyleBookを作成する方法で作成したStyleBookの例を検討してください。StyleBookから構成パックを作成するには、次のようにREST APIを使用します。

POST

`https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks?mode=async`

```
{

    "configpack": {

        "stylebook": {

            "name": "lb",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "1.1"

        },

        "parameters": {

            "lb-appname": "lbapp1",

            "lb-virtual-ip": "192.168.1.1",
```

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

```
            "lb-virtual-port": "443",
            "lb-service-type": "SSL",
            "svc-service-type": "HTTP",
            "svc-servers": [
                {
                    "ip": "193.1.1.1",
                    "port": "80"
                }
            ],
            "certificates": [
                {
                    "cert-name": "cert1",
                    "cert-file": {
                        "name": "c3.pem",
                        "contents": "<base64 encoded content>",
                        "encoding_type": "base64"
                    },
                    "ssl-inform": "PEM",
                    "key-file": {
                        "name": "c3.key",
                        "contents": "<base64 encoded content>",
                        "encoding_type": "base64"
```

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

```
                    }
                }
            ]
        },
        "targets": [
            {
                "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
            }
        ]
        }
    }
}
```

これにより、構成ジョブの完了を追跡するために使用できるジョブIDが返されます。

```
{
    "job": {
        "job_id": "388922985"
    }
}
```

ジョブのステータスと構成ジョブが完了した時期を確認するには、ジョブポーリングAPIを使用します。

GET

`https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/388922985`

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

```
200 OK

{

    "job": {

        "job_id": "388922985",

        "status": "completed",

        "progress_info": [...],

        "result": {

            "config_key": "388922985",

            "created_by": "nsroot",

            "created_datetime": "2023-01-14 01:46:05.410998",

            "created_datetimestamp": "2023-01-14 01:46:05",

            "id": "388922985",

            "incarnation_number": "0",

            "last_modified_by": "nsroot",

            "last_modified_datetime": "2023-01-14 01:46:05",

            "lock": "Y",

            "name": "sample-dns-stylebook",

            "namespace": "com.citrix.adc.tests",

            "primary_keys": "{}",

            "sb_id": "samp4ed0c4c90aefaadaff6422b0c395f67f",

            "status": "completed",

            "target_devices_json": "[{\"instance_id\": \"49a45044-
```


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

```
ceb3-4e9d-8a5d-e3fe225d90ed\", \"id\": \"1833061454\", \"group_id\": \"\",
\"instance_ip\": \"192.168.153.165\", \"hostname\": \"ctx-adc-dc01-v-
prod-54\", \"instance_role\": \"[\\\"default\\\"]\",
\"incarnation_number\": \"0\"}]",

            "tenant_id": "1a45fd70-7ce3-4bff-8642-1bd7f7e97673",

            "version": "1.0"

        }

    }

}
```

ジョブID (388922985) は構成パックを識別します。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。

APIを使用して、あらゆるファイルタイプをアップロードする構成を作成する

NetScaler Console APIを使用して、選択したNetScalerインスタンスにファイルをアップロードする構成パックを作成することもできます。

あらゆる種類のファイルをアップロードするために、NetScaler Consoleにファイルをアップロードする StyleBookを作成する方法で作成したStyleBookの例を検討してください。

このStyleBookから構成パックを作成するには、以下のREST APIを使用します。

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks?mode=async`

```
{

    "configpack": {

        "stylebook": {

        "name": "filetest",

        "namespace": "test.adc.stylebook",

        "version": "1.0"
```

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

```
        },
        "parameters": {
            "nameoffile": "file1",
            "fileupload": {
                "name": "relate.txt",
                "contents": "base64 encoded content",
                "encoding_type": "base64"
            }
        },
        "targets": [
            {
                "instance_id": "9419667d-27b7-495a-b87a-d3b5ee747dd3"
            }
        ],
    }
}
```

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 Consoleにインポートします。REST APIを使用して、cURLコマンドラインツールやPostman Chromeブラウザ拡張機能などの任意のツールで、このStyleBookから構成パックを作成します。たとえば、NetScalerインスタンス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メソッド: POST

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

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/actions/import?mode=async`

```
{

    "import": {

        "file_name": "add_dnssoarec.yaml",

        "source": "<base 64 encoded content of the sb definition>",

        "encoding": "base64"

    }

}
```

ここで、`source`属性の値は、StyleBookファイルの内容をbase64エンコードしたものです。StyleBookファイルのYAMLコンテンツをオンラインツールに貼り付けることができます。たとえば、`<https://www.browserling.com/tools/file-to-base64>`を使用して、`source`属性の値として使用できるbase64文字列を取得します。

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回のAPI操作でアップロードすることもできます。次の手順を実行します。

- `file_name`属性を.tgzファイルに変更します
- `source`属性を.tgzファイルの内容のbase64エンコードに変更します

ツールでAPIが正常に実行されると、ジョブIDを含む応答が返されます。このジョブIDを使用して、操作の完了まで追跡します。

```
200 ACCEPTED
```

応答本文:

```
{

    "job": {

        "job_id": "12345678"
```

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

```
    }
}
```

ジョブIDを使用して、操作のステータスを追跡します。

HTTPメソッド: GET

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/<job-id>`

ジョブのステータスが返されます。

```
200 OK
```

応答本文:

```
{
    "job": {
        "job_id": "<job-id>",
        "progress_info": [
            {
                "is_last": "true",
                "message": "No job found",
                "status": "failed"
            }
        ],
        "status": "completed"
    }
```

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

```
}
```

「completed」のステータス値は、StyleBookが正常にインポートされたことを示します。
StyleBookに関する情報を取得して、操作のステータスを確認します。

HTTPメソッド: GET

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/samples/1.0/demo-helper-object`

インポートされたStyleBookの詳細が表示されます。

```
200 OK
```

応答本文:


```
{

    "stylebook": {

        "builtin_namespaces": {},

        "created_datetime": "2023-01-14 00:13:59",

        "custom": true,

        "dependencies": [],

        "deprecate": "false",

        "description": "This Stylebook is a test",

        "display_name": "Test StyleBooks",

        "encoding": "BASE64",

        "header": "Test StyleBooks",

        "icon": "''",

        "id": "demo575731aacbfc20b4ff00b3b60ea59855",
```


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

```
        "is_updatable": true,
        "name": "demo-helper-object",
        "namespace": "samples",
        "primary_keys": {},
        "private": false,
        "repository_name": "",
        "reverse_dependencies": [],
        "schema_version": "1.0",
        "source": "<base 64 encoded content of the stylebook definition>",
        "tenant_id": "1a45fd70-7ce3-4bff-8642-1bd7f7e97673",
        "username": "abc",
        "version": "1.0"
    }
}
```

APIを使用してカスタムStyleBookを更新する

APIを使用してカスタムStyleBookを更新できます。StyleBookを更新する際、バージョンを変更せずにStyleBookに変更を加えることができます。また、StyleBookバンドルからインポートされた定義を更新することもできます。

POST： `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<Namespace>/<version>/<Name>/actions/update?mode=async`

ペイロード：

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

```
{

    "update": {

        "encoding": "base64",

        "source": "<base 64 encoded content of the stylebook definition>"

}

}

    }

}
```

注

このAPIは非同期であり、ジョブIDを返します。このジョブIDは、StyleBookをインポートするためのAPIと同様に、更新ジョブの完了を追跡するために使用できます。

カスタムStyleBookをダウンロードするためのAPIの使用

カスタムStyleBookをダウンロードするには、以下のStyleBook REST APIを使用します。

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download`

cURLコマンドラインツールなどの任意のツールでAPIを実行できます。IPアドレス、名前、バージョン、および名前空間フィールドを変更した後、Postman Chromeブラウザ拡張機能を使用することもできます。

このAPIを実行すると、カスタムStyleBookはzipファイルとしてローカルコンピューターにダウンロードされます。

依存StyleBookをダウンロードし、圧縮タイプを指定するためのAPIの使用

依存StyleBookの完全なツリーをダウンロードし、圧縮形式（ここでは.tgz）を指定するには、以下のAPIを使用します。

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

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download?dependencies=true&compress_type=tgz`

応答には、StyleBookとその依存関係（存在する場合）がtarballで表示されます。

```
200 OK

Content-disposition: attachment; filename=samples_1.0_demo-helper-object.tgz

Content-Type: application/x-zip

....zipped content...
```

APIを使用してカスタムStyleBookを削除する

カスタムStyleBookを削除するには、以下のStyleBook REST APIを使用します。

DELETE: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>?dependencies=true`

URL内の依存関係クエリパラメータが指定されていないか、その値がfalseに設定されている場合、StyleBookのみが削除されます。StyleBookの依存関係は削除されません。

カスタムStyleBookとその依存関係がNetScaler Consoleから正常に削除されると、HTTP応答ステータスコード200が返されます。

注

依存するStyleBookを持つカスタムStyleBookは削除できません。

たとえば、NetScaler Consoleで`lb-virtual-ssl-extended`という名前のStyleBookを作成したとします。後でそのStyleBookを削除することにしました。

cURLコマンドラインツールなどの任意のツールでAPIを実行できます。IPアドレス、名前、バージョン、および名前空間のフィールドを変更した後、Postman Chromeブラウザ拡張機能を使用することもできます。

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

APIを使用して既存の構成パックを更新する

StyleBook API を使用して、NetScaler Console の既存の構成パックを更新できます。

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

ペイロード:

```
{

    "configpack": {

        "stylebook": {

            "name": "waf-adv",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "1.3"

        },

        "parameters": {

            "name": "TestApp1",

            "lbname": "my-lbv",

            "waf-settings": {

                "rule": "true",

                "type": [

                    "HTML"

                ],

                "profile-settings": {

                    "logeverypolicyhit": false,

                    "enablesignatures": {
```

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

```
                    "signaturename": "waf-sign1"
                },
                "sqlinjection-settings": {
                    "sqlinjectionaction": [
                        "log",
                        "stats"
                    ],
                    "sqlinjection-default-settings": {
                        "sqlinjectiontransformspecialchars": true,
                        "sqlinjectionchecksqlwildchars": true,
                        "sqlinjectiontype": "SQLSplCharANDKeyword",
                        "sqlinjectionparsecomments": "checkall",
                        "sqlinjectiongrammar": "OFF"
                    }
                },
                "bufferoverflow-settings": {
                    "bufferoverflowaction": [
                        "log"
                    ],
                    "bufferoverflowmaxurllength": "2048",
                    "bufferoverflowmaxheaderlength": "4096",
                    "bufferoverflowmaxcookielength": "4096",
```


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

```
                        "bufferoverflowmaxquerylength": "65535",
                        "bufferoverflowmaxtotalheaderlength": "65535"
                    }
                }
            }
        },
            "targets": [
            {
                "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
            }
            ]
    }
}
```

HTTPステータス202とジョブIDを含む応答本文が返されます。ジョブIDを使用して、更新操作のステータスを追跡できます。

```
{
    "job": {
        "job_id": "1092579455"
    }
}
```

このジョブID（この例では1092579455）は、ジョブポーリングAPIを使用して追跡できます。

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

GET: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/1092579455`

応答にステータスが「completed」と設定されている場合、更新操作は正常に完了しています。このフィールドの他の値は、更新ジョブの失敗を示します。失敗の原因は、**progress_info** オブジェクトで確認できます。


```
{

    "job": {

        "job_id": "4268148987",

        "status": "completed",

        "progress_info": [

            {

                "is_last": "false",

                "message": "Validated the parameters",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Configuration audit completed",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Computed configuration objects",

                "status": "success"
```


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

```
            },
            {
                "is_last": "false",
                "message": "Prepared objects for applying configuration on
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved existing data for updatable objects
on instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Applied configuration on instance
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved data for configuration audit on
instance 192.168.153.165",
                "status": "success"
```


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

```
            },
            {
                "is_last": "false",
                "message": "Logged out from instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "true",
                "message": "Saved configpack.",
                "status": "completed"
            }
        ],
        "result": {
            "status": "completed",
            "id": "4268148987",
            "config_key": "4268148987",
            "created_by": "nsroot",
            "created_datetime": "2023-01-20 18:57:58.985435",
            "created_datetimestamp": "2023-01-20 18:57:58",
            "last_modified_by": "nsroot",
            "last_modified_datetime": "2023-01-20 19:00:32",
            "name": "sample-dns-stylebook",
```


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

```
            "namespace": "com.citrix.adc.tests",

            "version": "1.0"

        }

    }

}
```

APIを使用してターゲットインスタンスを更新する

構成パックの更新ペイロードで、NetScalerインスタンスを追加、削除、または置換するために`targets`セクションを変更します。

例:

次の例では、ペイロード内の`targets`オブジェクトが変更され、新しいターゲットNetScalerが構成に追加されています。

```
{

    "targets": [

        {

            "instance_id": "<Existing-ADC-instance-ID>"

        },

        {

            "instance_id": "<New-ADC-instance-ID>"

        }

    ],

}
```

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

更新が成功すると、構成は新しいNetScalerインスタンスに展開されます。構成のターゲットを変更することは、NetScaler間でアプリケーション構成を移動したい場合に役立ちます。たとえば、メンテナンスのためにNetScalerを構成から削除する必要がある場合は、`targets`オブジェクトを変更します。

注

構成を現在のすべてのターゲットインスタンスから削除するには、空の`targets`オブジェクトを使用します。NetScaler Consoleの構成は保持されますが、以前に展開されていたすべてのNetScalerから削除されます。必要に応じて、構成を再度更新して、1つまたは複数のターゲットを指定できます。

以下のAPI例は、既存のすべてのターゲットから構成を削除します。

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

ペイロード:

```
{

    "configpack": {

        "stylebook": {

            "name": "waf-adv",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "1.3"

        },

        "parameters": {

            "name": "TestApp1",

            "lbname": "my-lbv",

            "waf-settings": {
```

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

```
            "rule": "true",
            "type": [
                "HTML"
            ],
            "profile-settings": {
                "logeverypolicyhit": false,
                "enablesignatures": {
                    "signaturename": "waf-sign1"
                },
                "sqlinjection-settings": {
                    "sqlinjectionaction": [
                        "log",
                        "stats"
                    ],
                    "sqlinjection-default-settings": {
                        "sqlinjectiontransformspecialchars": true,
                        "sqlinjectionchecksqlwildchars": true,
                        "sqlinjectiontype": "SQLSplCharANDKeyword",
                        "sqlinjectionparsecomments": "checkall",
                        "sqlinjectiongrammar": "OFF"
                    }
                },
```

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

```
                    "bufferoverflow-settings": {
                        "bufferoverflowaction": [
                            "log"
                        ],
                        "bufferoverflowmaxurllength": "2048",
                        "bufferoverflowmaxheaderlength": "4096",
                        "bufferoverflowmaxcookielength": "4096",
                        "bufferoverflowmaxquerylength": "65535",
                        "bufferoverflowmaxtotalheaderlength": "65535"
                    }
                }
            }
        },
        "targets": []
    }
}
```

API を使用して構成を監査する

API を使用して、StyleBook 構成パックによって行われた変更を現在の NetScaler 構成と比較できます。この比較により、次のことができます。

- StyleBook 構成パックと NetScaler 構成間の構成ドリフトを検出します。
- 構成パックによって行われた変更を反映していない、NetScaler 上で変更または削除されたオブジェクトを特定します。

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

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/audit?mode=async`

APIを使用して設定パックをエクスポートする

NetScaler ConsoleからStyleBook APIを使用して設定パックをエクスポートできます。エクスポートバンドルはローカルコンピューターに保存されます。これには、設定パックで定義されたすべてのパラメーターを含むJSONファイルと、関連するシステムファイルが含まれます。

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/export`

ペイロード:

```
{
    "export": {
        "options": {
            "include_stylebook": true,
            "include_targets": false,
            "compress_type": "zip",
            "password_protect": false
        },
        "passphrase": ""
    }
}
```

関連するStyleBookおよびターゲットインスタンスとともに設定パックをエクスポートすることを選択できます。

設定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。バンドルの種類は、指定された`compress_type`によって異なります。

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

APIを使用して構成パックを新しいStyleBookにアップグレードする

StyleBook APIを使用して、既存のStyleBookから新しいStyleBookに構成パックをアップグレードできます。

POST `http://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/actions/upgrade?mode=async`

ペイロード:

```
{

    "upgrade": {

            "stylebook": {

            "name": "customer-template",

            "namespace": "neustar.citrix.adc.stylebooks",

            "version": "6.2"

        },

        "configpack_ids": [

            "1644278065",

            "2750234437"

        ]

    }

}
```

このペイロードの例では、リストされている構成パックは1644278065と2750234437です。これらの構成パックは、名前`customer-template`、バージョン6.2の新しいStyleBookに更新されます。

構成パックのアップグレードジョブのステータスを取得するには、ジョブポーリングAPIを使用します。

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

GET: `https://<ADM-IP-address>/stylebook/nitro/v1/config/jobs/<job-ID>`

注

応答本文のステータスフィールドが**completed** (成功を示す) または**failed**に設定されるまで、**GET**メソッドを繰り返します。

APIを使用して、コンフィグパックからターゲットインスタンスをデタッチする

コンフィグパックからターゲットインスタンスをデタッチすると、そのコンフィグパックに加えられた変更は、そのインスタンスに展開されません。APIを使用してターゲットインスタンスをデタッチできます。

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/detach_targets`

ペイロード:

```
{
    "detach_targets": [
        {
            "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c",
            "id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
        }
    ]
}
```

APIを使用して、config packからNetScalerインスタンスを強制的に削除する

NetScalerインスタンスがconfigpackを削除せずにNetScaler Consoleから削除された場合、エラーが発生する可能性があります。そのため、config packからそのインスタンスを強制的に削除する必要があります。

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

StyleBook APIを使用して、config packからNetScalerインスタンスを強制的に削除できます。

PUT： `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async&force_targets_delete=true`

```
{
    "configpack": {
        "stylebook": {
            "name": "test-policy-patset",
            "namespace": "com.citrix.adc.stylebooks",
            "version": "1.1"
        },
        "parameters": {
            "lbname": "test11"
        },
        "targets": [
            {
                "instance_id": "f9bdf101-61ec-46a7-bf09-e9ce097b7cfd",
                "instance_ip": "10.106.100.116",
                "roles": [
                    "default"
                ]
            }
        ]
```

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

```
    }

}
```

API を使用して設定パックを削除する

以下の StyleBook API を使用して設定パックを削除できます。

DELETE `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

HTTP ステータス 202 と応答ペイロードが表示されます。応答ペイロードにはジョブ ID が含まれており、これを使用して削除操作のステータスを追跡できます。

応答ペイロードは次のとおりです。

```
{

    "job": {

        "job_id": "1841028854"

    }

}
```

削除ジョブ操作を追跡するには、ジョブ ID (この例ではジョブ ID は 1841028854) を使用してジョブポーリング API を使用します。

GET `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/1841028854`

応答のステータスフィールドが「completed」に設定されている場合、次の例に示すように、削除ジョブ操作は成功しています。

```
{

    "job": {

        "job_id": "3920886024",

        "status": "completed",
```

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

```
        "progress_info": [
            {
                "is_last": "false",
                "message": "Validated the parameters",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Configuration audit completed",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Computed configuration objects",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Prepared objects for applying configuration on
192.168.153.165",
                "status": "success"
            },
```


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

```
            {

                "is_last": "false",

                "message": "Retrieved existing data for updatable objects
on instance 192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Applied configuration on instance
192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Retrieved data for configuration audit on
instance 192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Logged out from instance 192.168.153.165",

                "status": "success"

            },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            {
                "is_last": "true",
                "message": "Removed configpack.",
                "status": "completed"
            }
        ]
    }
}
```

削除操作は、次のシナリオで失敗する可能性があります。

- 設定が存在する NetScaler インスタンスがダウンしている
- NetScaler インスタンスが NetScaler Console から到達できない
- 設定が NetScaler 上で利用できなくなった

NetScaler から削除できない場合でも、NetScaler Console から設定の削除を強制できます。このような場合、NetScaler の設定は手動で復元する必要があります。

NetScaler Console から設定の削除を強制するには、API にクエリ文字列「force=true」を追加します。

DELETE `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async&force=true` 。

StyleBookの文法

独自のStyleBookを設計し、NetScaler Consoleにインポートして、NetScaler Console GUIまたはAPIを使用して構成を作成できます。独自のStyleBook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、StyleBook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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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	StyleBookのインポート
パラメーター	パラメータ-デフォルトソース構文
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
Condition構成要素	「繰り返しコンストラクト」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/repeat-construct.html)
「繰り返し条件コンストラクト」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	「出力」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/outputs.html)
「ネストされた繰り返し」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/nested-repeats.html)	「親参照」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/parent-reference.html)
「パラメータ参照」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/parameter-reference.html)	「置換参照」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/substitutions-reference.html)
「コンポーネント参照」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/components-reference.html)	「操作」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/operations.html)
「変数参照」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/variable-reference.html)	「アラーム」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/alarms.html)
「分析」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/analytics.html)	「組み込み関数」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/built-in-functions.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「式」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/expressions.html)	「依存関係の検出」(/ja-jp/netscaler-console-service/stylebooks/stylebooks-grammar/dependency-detection.html)
「インプレース補間」(/ja-jp/netscaler-console-service/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、ユーザー定義変数に名前を付けるために、以下の予約語を使用しないでください。`$<var-name>`

- StyleBook, パラメータ, 置換, コンポーネント, プロパティ, 出力, 親, 自身, 操作, 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, parent-context, parent_context

独自のStyleBookを設計する方法に関する情報と例については、「」(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks.html)を参照してください。

ヘッダー

StyleBookの最初の6行はヘッダーセクションで構成されます。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します。これは必須のセクションです。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	説明
説明	StyleBookの機能について定義する説明。この説明はNetScaler Console GUIに表示されます。これはオプションの属性です。
表示名	StyleBookの表示名。この名前はNetScaler Console GUIに表示されます。これはオプションの属性です。
作成者	StyleBookを作成する作成者または組織。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付け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`。これは必須の属性です。
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	StyleBooksスキーマのバージョンです。NetScaler Consoleの現在のリリースでは、「1.0」という値を取ります。これは必須属性です。
プライベート	この属性がtrueに設定されている場合、StyleBookはNetScaler Console GUIに表示されません。これは、他のStyleBookの構成要素であり、ユーザーが直接使用することを意図していないStyleBookにとって便利な設定です。これはオプション属性です。デフォルト値はfalseです。

例:

© 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"
```

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StyleBookが一意に識別されます。NetScaler Consoleでは、名前、名前空間、およびバージョンの組み合わせが同じ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2つの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、自分の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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

現在のStyleBookで参照したいStyleBookの**名前空間**と**バージョン**番号を宣言する必要があります。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、StyleBookを使用して構成を作成および実行できることを意味します。

import-stylebooksセクションで使用される**プレフィックス**属性は、名前空間とバージョンの組み合わせを参照するための短縮形です。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
```

この例では、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、**\<namespace-shorthand\>::\<type-name\>**という表記を使用できます。たと

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、**stlb::\<stylebook-name\>**という表記を使用できます。

注

慣例により、「ns」プレフィックスはNetScalerのNITRO名前空間を参照するために使用されます。

パラメータ

このセクションでは、設定を作成するためにStyleBookで必要となるすべてのパラメータを定義できます。StyleBookが受け取る入力を記述します。このセクションはオプションですが、ほとんどのStyleBookで必要となる場合があります。パラメータセクションは、NetScalerインスタンスで設定を作成するために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 Consoleにインポートして設定を作成する際、GUIはStyleBookのこのセクションを使用してフォームを表示します。このフォームは、定義されたパラメータ値の入力を受け取ります。

以下のセクションでは、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、$parameters.\<name>という表記で他のセクションのパラメータを参照できます。

必須ですか？はい

'ラベル'

NetScaler Console GUIでこのパラメータの名前として表示される文字列。

必須ですか？いいえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'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、NetScaler Console GUIにこのテキストが表示されます。

必須ですか？いいえ

タイプ

これらのパラメーターが取りうる値のタイプ。 パラメーターは、以下の組み込みタイプのいずれかになります。

- `string`: 文字の配列。長さが指定されていない場合、文字列値は任意の数の文字を取ることができます。ただし、min-length および max-length 属性を使用することで、文字列タイプの長さを制限できます。
- `number`: 整数。min-value および max-value 属性を使用することで、このタイプが取りうる最小値と最大値を指定できます。
- `boolean`: true または false のいずれか。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、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 Console GUIから構成パックを作成または更新する際、以下のいずれかのアクションを実行できます。

  - ネットマスク長を有効にし、IPアドレスとネットマスク長を入力する
  - 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アドレスを入力する
- `tcp-port`: TCPまたはUDPポートを表す0から65535までの数値。
- `password`: 不透明な/秘密の文字列値を表します。NetScaler Console GUIがこのパラメーターの値を表示する場合、アスタリスク (*****) で表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `certfile`: 証明書ファイルを表します。この値を使用すると、NetScaler Console GUIを使用してStyleBook構成を作成する際に、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、NetScaler Consoleの`/var/mps/tenants/\<tenant_path>/ns_ssl_certs`ディレクトリに保存されます。

  証明書ファイルは、NetScaler Consoleによって管理される証明書のリストに追加されます。

- `keyfile`: 証明書キーファイルを表します。この値を使用すると、NetScaler Console GUIを使用してStyleBook構成を作成する際に、ローカルシステムからファイルを直接アップロードできます。アップロードされた証明書ファイルは、NetScaler Consoleのディレクトリ`/var/mps/tenants/\<tenant_path>/ns_ssl_keys`に保存されます。

  証明書キーファイルは、NetScaler Consoleによって管理される証明書キーのリストに追加されます。

- `certkey`: このタイプは、NetScaler Console証明書ストアからSSL証明書を選択するために使用されます。このストアには、NetScaler Consoleサーバーにアップロードされた既存のSSL証明書が一覧表示されます。そのため、SSL証明書をNetScaler Console証明書ストアという1か所に保存し、必要に応じて再利用できます。

  構成パックを作成する際、ユーザーは証明書ストアからSSL証明書を追加または選択できます。また、ユーザーは複数の構成パックに対して同じ証明書を選択できます。

- `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ために使用されます。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」セクションを持つことができます。
- `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際に、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'ネットワーク'

`type: ipaddress`の場合、`network`属性を指定して、NetScaler Console IPAMネットワークからIPアドレスを自動割り当てできます。

NetScaler Consoleは、StyleBook構成を作成する際に、`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`フィールドが`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。

「ダイナミックアロケーション」

`dynamic-allocation`属性は、`type:ipaddress`のパラメータ定義に追加されます。この属性を使用して、NetScaler Console IPAMネットワークを動的にリスト表示します。この属性は、入力として`true`または`false`のいずれかを受け入れることができます。`type: ipaddress`の場合、NetScaler ConsoleにあるNetScaler Console IPAMネットワークを動的にリスト表示するには、`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たいIPアドレスを指定します。

   IPアドレスが指定されていない場合、NetScaler Consoleは選択したIPAMネットワークからIPアドレスを自動的に割り当てます。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"

  type: ipaddress

  dynamic-allocation: true

  required: true
```

この例では、`virtual-ip`フィールドにはNetScaler ConsoleにあるNetScaler Console IPAMネットワークがリスト表示されます。リストからネットワークを選択し、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には、「キー」パラメータとして定義された1つ以上のパラメータを設定できます。**Configuration > Config Packs**ページには、パラメータの値が**表示キー**として表示されます。

同じStyleBookから異なる構成パックを作成する場合、各構成は、このパラメータに対して異なる値を持つことができます。この値はGUIに表示キーとして表示されます。このキーを使用して、構成パックをソートまたはフィルタリングできます。

例:

```
parameters:

  - name: example-appname

    type: string

    label: Application Name

    required: true

    key: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBookユーザーが構成パックを作成すると、パラメータ`example-appname`の値が表示キーとして表示されます。StyleBookユーザーはこのキーを使用して、この構成パックを識別できます。

注

構成パックの**Config Key**は、そのパラメータのいずれかに設定されたキー属性を上書きします。したがって、ユーザーがConfig Keyに値を入力すると、この値が**表示キー**列に表示されます。

デフォルト値はfalseです。

必須? いいえ

'必須'

パラメーター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、そのパラメーターは必須であり、ユーザーは構成を作成する際にこの パラメーターの値を指定する必要があります。

NetScaler Console GUIは、ユーザーにこのパラメーターの有効な値を強制的に提供させます。

デフォルト値はfalseです。

必須? いいえ

'許可される値'

この属性を使用して、タイプが「string」に設定されている場合に、パラメーターの有効な値のリストを定義します。

NetScaler Console GUIから構成を作成する際、ユーザーはこのリストからパラメーター値を選択するよう求められます。このリストは静的であり、ユーザーはリストから値を選択することしかできません。ユーザーがリストに値を追加できるようにしたい場合は、`allow-new-values` 属性を使用します。

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: ipaddress

      type: string

      allowed-values:

            -  SOURCEIP

            -  DEST IP

            -  NONE
```

例 2:

```
-

      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[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      allowed-values:

            -  80

            -  81

            -  8080

            -  8081
```

必須ですか？いいえ

'新しい値の許可'

この属性を使用して、パラメータの動的リストを追加します。NetScaler Console GUIから構成を作成または更新する際に、ユーザーはリストに値を追加できます。

ユーザーがパラメータリストに値を追加できるようにする場合は、trueを指定します。`allow-new-values`と`allowed-values`属性を組み合わせて使用できます。この組み合わせにより、パラメータの推奨値のリストを定義し、新しい値も受け入れることができます。

```
-

      name: port

      type: tcp-port

      allowed-values:

            -  80

            -  81

            -  8080

      allow-new-values: true
```

この例では、ユーザーは構成パックの作成または更新中に、80、81、8080から選択するか、パラメータ`port`に新しい値を入力することができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'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した場合、デフォルト値が使用されます。

以下の条件が満たされている場合、パラメータは値を持ちません。

- パラメータにデフォルト値がありません。
- ユーザーがパラメータに値を指定しません。

例 1：

```
-

      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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: timeout

      type: number

      default: 20
```

例 4:

```
-

      name: tcpport

      type: tcp-port

      default: 20
```

必須? いいえ

パターン

この属性を使用して、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。 パラメータのタイプが「string」の場合に。

例:

```
-

      name: appname

      type: string

      pattern: "[a-z]+"
```

必須? いいえ

最小値

この属性を使用して、`number` または `tcp-port` タイプのパラメータの最小値を定義します。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

数値の `min-value` は負の値になることがあります。ただし、`tcp-port` の `min-value` は正の値でなければなりません。

必須? いいえ

最大値

この属性を使用して、`number` または `tcp-port` タイプ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。

値として定義された文字の最小長がゼロ以上であることを確認してください。

例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: appname

      type: string

      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`で定義された文字の長さ以上であることを確認してください。

例：

```
-

      name: appname

      type: string

      max-length: 64
```

必須ですか？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てください。

例：

```
-

      name: server-ips

      type: ipaddress[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      min-items: 2
```

必須ですか？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項目の最大数を定義します。 リスト。

定義されている場合、項目の最大数が項目の最小数よりも大きいことを確認してください。

例:

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2

      max-items: 250
```

必須ですか？いいえ

「GUI」

この属性を使用して、NetScaler Console GUIでのパラメータのレイアウトをカスタマイズします。

必須ですか？いいえ

「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、NetScaler Console GUIで`type: object[]` パラメータを表示する列数を定義します。

必須ですか？いいえ

「更新可能」

この属性は、`gui` 属性のサブ属性です。この属性を使用して、設定作成後にパラメータを更新できるかどうかを指定します。この属性は、文字列、ブール値、数値などの単純なパラメータ型にのみ設定してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

値が`false`に設定されている場合、設定を更新するときにパラメータフィールドはグレー表示されます。

必須ですか？ いいえ

「collapse_pane」

この属性は、`gui`属性のサブ属性です。この属性を使用して、このオブジェクトパラメータのレイアウトを定義するペインを折りたたみ可能にするかどうかを指定します。

値が true に設定されている場合、ユーザーはこの親パラメータの下にある子パラメータを展開または折りたたむことができます。

例:

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    description: Name of the application

    type: string

    required: true

-

    name: ip

    label: IP Address

    description: The virtual IP address used for this application

    type: ipaddress

    required: true

-

    name: svc-servers
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
label: Servers

type: object\[\]

required: true

parameters:

  -

        name: svc-ip

        label: Server IP

        description: The IP address of the server

        type: ipaddress

        required: true

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            name: svc-port

            label: Server Port

            description: The TCP port of the server

            type: tcp-port

            default: 80

        -

            name: lb-alg

            label: LoadBalancing Algorithm

            type: string

            allowed-values:

               - ROUNDROBIN
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            - LEASTCONNECTION

        default: ROUNDROBIN

    -

        name: enable-healthcheck

        label: Enable HealthCheck?

        type: boolean

        default: true
```

以下は、リストのすべての属性と、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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        max-length: 3

        min-items: 1

        max-items: 3

        pattern: "\[A-Z\]+"

        allowed-values:

          - SP

          - LB

          - CS

        default:

          - LB
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「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。構成パックを作成すると、NetScaler Console GUI は `allowed-values` リストの値をラジオボタンとして表示します。

例:

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two

        - Three
```

「One」、「Two」、「Three」の値は、NetScaler Console GUI で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、StyleBook 構成フォームにおけるパラメータの表示または初期値を、別のパラメータで指定された値に基づいて動的に制御します。

この属性は、フォーム上のパラメータの動作を制御するソースパラメータに指定します。他のパラメータを制御する複数の条件を含めることができます。たとえば、ソースパラメータ `protocol` には、`protocol` パラメータの値が `SSL` の場合にのみ表示される依存パラメータ `certificate` を持たせることができます。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `read-only`：パラメータは読み取り専用になります。
- `show`：パラメータが非表示の場合、フォームに表示されます。
- `hide`：パラメータはフォームから削除されます。
- `set-value`：パラメータ値は、value属性で指定された値に設定されます。

- **value**：アクションが`set-value`の場合のターゲットパラメータの値。

ユーザー入力がソースパラメータで指定された値と一致すると、ターゲットパラメータの表示または値が指定されたアクションに従って変更されます。

例：

```
-

   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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            - 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。

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

`is_policy_expression`

この属性は、`gui`属性のサブ属性です。この属性を使用して、ポリシー式エディターでポリシー式を作成できるようにします。 パラメーター定義で`is_policy_expression`を`true`に設定します。この属性は、「string」型のパラメーターでのみ使用できます。

例:

```
parameters:

  -



    name: expression

    type: string

    label: Expression

    required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    gui:

      is_policy_expression: true
```

Parameters-default-sources コンストラクト

このコンストラクトを使用して、他のStyleBookからパラメータ定義を再利用できます。

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に、一度定義し、**parameters-default-sources** コンストラクトを使用して、これらのパラメータを必要とするStyleBookにその定義をインポートできます。

たとえば、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ことがあります。代わりに、たとえば `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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"

parameters:

  -

      name: lb-appname

      label: Load Balanced Application Name

     description: Name of the Load Balanced application

      type: string

      required: true

  -

      name: lb-virtual-ip

      label: Load Balanced App Virtual IP address
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        label: Load Balanced App Protocol

        description: Protocol used for the Load Balanced application.

        type: string

        default: HTTP

        required: true

        allowed-values:

             - HTTP

             - SSL

             - TCP
```

その後、これらのパラメータを使用する他のStyleBookを作成できます。

```
    -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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:**
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
**            - cmtypes::vip-params**


     parameters:


         -


           name: monitorname


           label: Monitor Name


           description: Name of the monitor


           type: string


           required: true


         -


           name: type


           label: Monitor Type
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        description: Type of the monitor

        type: string

        required: true

        allowed-values:

          - PING

          - TCP

          - HTTP

          - HTTP-ECV

          - TCP-ECV

          - HTTP-INLINE
```

StyleBook `acme-biz-app` では、まず「import-stylebooks」セクションを使用して `vip-params` StyleBookの名前空間とバージョンがインポートされます。次に、**parameters-default-sources** コンストラクトが追加され、StyleBook名、つまり `vip-params` が指定されます。この

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータは、`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します。このアプローチを使用すると、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つつ、残りのインポートされたパラメータをそのまま使用することで、効果的に活用できます。

parameters-default-sources コンストラクトは、次の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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      required: true


      parameters-default-sources:


              - cmtypes::vip-params
```

このアプローチは、StyleBook `vip-params` のパラメータを、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するのと似ています。

Parameters-source コンストラクト

`parameters-source`コンストラクトを使用すると、コンフィギュレーションパックの作成中に、インポートされたパラメータがGUIにどのように表示されるかを制御できます。このコンストラクトを説明するStyleBookの例を以下に示します。

```
parameters:

  -

    name: appname

    label: "LBVserver Name"

    description: "Name of the Load Balancer"

    type: string

    required: true

  -

   parameters-source: stlb::lb

  -

    name: vip-ipaddress

    label: "Load Balancer IP Address"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    description: "IP Address of the Load Balancer VIP"

    type: ipaddress

    required: true
```

この例では、`parameters-source`コンストラクトが`parameters`セクションに追加されています。`parameters-source`には、`parameters-default-sources`セクションのリスト項目に相当する値が含まれています。`parameters-source`を使用すると、異なるStyleBookからパラメータを目的の位置にインポートし、GUIにレンダリングできます。一方、`parameters-default-sources`セクションは属性をインポートし、GUIの冒頭にのみレンダリングします。

パラメータ条件

StyleBookの定義では、パラメータはStyleBookユーザーが構成パックを作成するために提供する入力を定義します。場合によっては、次のようにパラメータの動作を変更したい場合があります。

- ある条件が満たされた場合にのみ、一部のパラメータをユーザーに表示する。
- あるパラメータの許容値が別のパラメータに依存するようにする。
- 特定の条件でのみパラメータを必須として設定する。

これらの場合、パラメータ条件を定義するには`parameters-conditions`セクションを使用します。パラメータ条件には、次の属性があります。

- `target`: 条件を適用するパラメータを指定します。
- `action`: ターゲットパラメータが条件に一致した場合に実行するアクションを指定します。この機能は、次のアクションをサポートしています。
    - パラメータの表示または非表示
    - デフォルト値の設定
    - 必須フィールドとして設定
    - 許容値の設定
    - パラメータのラベルを設定
    - パラメータの説明を設定
    - パラメータペインの折りたたみまたは展開
    - パラメータのパターンを設定する(#set-pattern)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `condition`: 満たすべき条件を指定します。
- `value`: アクションに応じて、ターゲットパラメータの属性値を設定します。

注

現在、リストオブジェクト内のパラメータにはパラメータ条件を適用できません。

「show」または「hide」

アクションが`show`で、指定された条件が`True`を返すと、ターゲットパラメータがGUIに表示されます。

アクションが`hide`で、指定された条件が`True`を返すと、ターゲットパラメータがGUIから非表示になります。

例:

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: show

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初は、`security-settings`パラメータの証明書詳細は非表示になっています。ユーザーがSSLまたはSSL-Bridgeプロトコルを選択すると、証明書詳細が表示されます。

「デフォルト設定」

アクションが`set-default`で、指定された条件が`True`を返すと、ターゲットパラメータの値はデフォルト値に設定されます。

例1:

```
parameters-conditions:

  -

   target: $parameters.port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    action: set-default

    condition: $parameters.protocol == "SSL"

    value: 443

   -

    target: $parameters.port

    action: set-default

    condition: $parameters.protocol != "SSL"

    value: 80
```

例2:

```
parameters-conditions:

  -

    target: $parameters.port

    action: set-default

    value: if-then-else($parameters.protocol == "SSL", 443, 80)
```

ユーザーが**SSL**プロトコルを選択すると、デフォルトのポート値は`443`に設定されます。その他のプロトコルの場合、デフォルトのポート値は`80`に設定されます。例1と例2は同じ結果になります。

'必須設定'

アクションが`set-required`で、指定された条件が`True`を返す場合、ターゲットパラメータは構成パックを作成するための必須フィールドになります。

```
parameters-conditions:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    target: $parameters.security-settings.cert-details

    action: set-required

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初は、`security-settings`パラメータに証明書の詳細が必要ない場合があります。ユーザーが**SSL**または**SSL-Bridge**プロトコルを選択すると、証明書の詳細は構成パックを作成するための必須フィールドになります。

'許可値の設定'

アクションが`set-allowed-values`で、指定された条件が`True`を返す場合、ターゲットパラメータでは指定された値のみを選択できます。

例-1:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-allowed-values

    value:

     - "SSL"

    condition: $parameters.lb-virtual-port ==  443
```

ユーザーがロードバランサーの仮想ポートとして`443`を指定すると、アプリケーション名では**SSL**オプションのみが許可されます。

例-2;

```
parameters:

    -

      name: root-certificates
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: "Root Certificates"
    type: object[]
    parameters:
      -
        name: certkey-name
        label: "SSL Root CertKey Name"
        type: string
        required: true
  -
    name: im-certificates
    label: "Intermediate Certificates"
    type: object[]
    parameters:
      -
        name: certkey-name
        label: "Name of Intermediate CertKey"
        type: string
        required: true
      -
        name: link-options
        label: "Link to Root or Intermediate CertKey?"
        type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          allowed-values:
            - Root
            - Intermediate
          default: Root
          required: true
        -
          name: link-certkey
          label: "Linked to Root/Intermediate CertKey Name"
          type: string
          required: true
parameters-conditions:
  -
    repeat: $parameters.im-certificates
    repeat-item: imcert
    parameters-conditions:
    -
      target: $imcert.link-certkey
      action: set-allowed-values
      condition: $imcert.link-options == "Root"
      value: $parameters.root-certificates[*].certkey-name
    -
      target: $imcert.link-certkey
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    action: set-allowed-values

    condition: $imcert.link-options == "Intermediate"

    value: $parameters.im-certificates[*].certkey-name
```

この例は、SSL証明書の値の設定に関するものです。パラメータ条件の繰り返しコンストラクトは、すべての中間証明書（`im-certificates`）を反復処理し、各証明書の`link-options`パラメータをチェックします。

`link-options`パラメータが特定の値と一致する場合、`link-certkey`パラメータで許可されている値が、それぞれの証明書リストに追加されます。

たとえば、`link-options`パラメータが`Root`の場合、`link-certkey`パラメータで許可されている値が`root-certificate`リストに追加されます。

証明書をリストに追加するには、次の表記が使用されます。

- ルート証明書の場合：

  ```
  $parameters.root-certificates[*].certkey-name
  ```

- 中間証明書の場合：

  ```
  $parameters.im-certificates[*].certkey-name
  ```

'ラベルの設定'

アクションが`set-label`で、指定された条件が`True`を返すと、ターゲットパラメーターのラベルが指定されたテキストに変更されます。

例:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-label
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   value: if-then-else($parameters.lb-service-type == "TCP",
"TCPApp","UDPApp")
```

ユーザーがロードバランサープロトコルとして**TCP**を選択すると、アプリケーションのラベルは**TCPApp**に変更されます。ユーザーが別のオプションを選択すると、アプリケーションのラベルは**UDPApp**に変更されます。

'set-description' の設定

アクションが`set-description`で、指定された条件が`True`を返すと、ターゲットパラメーターの説明が指定されたテキストに変更されます。この説明は、ターゲットパラメーターのツールチップに表示されます。

例:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-description

   value: if-then-else($parameters.lb-service-type == "TCP", "Select a TCP
application name","Select a UDP application name")
```

ユーザーがロードバランサープロトコルとして**TCP**を選択すると、アプリケーションのツールチップに「`Select a TCP application name`」というテキストが表示されます。ユーザーが別のオプションを選択すると、アプリケーションの説明に「`Select a UDP application name`」が表示されます。

'collapse-pane' または 'expand-pane' のオプション

アクションが`collapse-pane`で、指定された条件が`True`を返すと、ターゲットパラメーターのペインがGUIで折りたたまれます。

アクションが`expand-pane`で、指定された条件が`True`を返すと、ターゲットパラメーターのペインがGUIで展開されます。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details

    action: expand-pane

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初は、`security-settings`パラメーターの証明書詳細ペインは展開されていない場合があります。ユーザーが**SSL**または**SSL-Bridge**プロトコルを選択すると、GUIで証明書詳細ペインが展開されます。

「セットパターン」

アクションが`set-pattern`で、指定された条件が`True`を返すと、ターゲットパラメーターフィールドが指定されたパターンに設定されます。

例:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-pattern

    value: "[a-z]+"
```

この例では、アプリケーション名には小文字のアルファベットのみが許可されます。

ネストされたパラメーター条件

StyleBookの定義では、パラメーター条件内に別のパラメーター条件を指定できます。これらの条件はネストされたパラメーター条件と呼ばれ、これらの条件を定義するために繰り返し構造を使用します。ネストされたパラメーター条件は、あるパラメーターから別のパラメーターに対してアクションを適用したい場合に役立ちます。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

    repeat: $parameters.lbvservers

    repeat-item: lbvserver

    parameters-conditions:

      -

        target: $lbvserver.port

        action: set-allowed-values

        condition: $lbvserver.protocol == "HTTPS"

        value: $parameters.ssl-ports
```

この例では、ユーザーがロードバランシング仮想サーバーにHTTPSプロトコルを選択すると、ポート値が動的に入力されます。そして、これはリスト内の各ロードバランシング仮想サーバーに適用されます。

置換

置換は、StyleBook内の複雑な式を置き換えることができる短縮名を定義するために使用され、StyleBookをより読みやすくします。

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ます。これはエラーの原因となる可能性があります。

置換は、このドキュメントの後の例で説明されているように、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。最初のものは、8181の短縮形として使用できる `http-port` です。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

置換:

`http-port: 8181`

これにより、ポート番号に覚えやすい名前を指定し、使用回数に関係なくStyleBookの1箇所でこのポート番号を定義できます。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、覚えやすい名前 `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

          port: $substitutions.http-port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          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。次はマップ置換の例です。

```
substitutions:


    secure-port:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        true: int("443")


        false: int("80")


    secure-protocol:


        true: SSL


        false: HTTP
```

次の例は、マップ secure-port と secure-protocol を使用する方法を示しています。

```
components:


 -


    name: my-lbvserver-comp


    type: ns::lbvserver


    properties:


         name: $parameters.name + "-lb"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          servicetype: $substitutions.secure-protocol[$parameters.is-
secure]


          ipv46: $parameters.ip


          port: $substitutions.secure-port[$parameters.is-secure]


          lbmethod: $parameters.lb-alg
```

ここで、StyleBookのユーザーがパラメータ `is-secure` にブール値「true」を指定した場合、またはNetScaler Console 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** の値が割り当てられ、ポートプロパティには **443** の値が割り当てられます。しかし、ユーザーがこのパラメータに「false」を指定した場合、またはNetScaler Console GUIで対応するチェックボックスをクリアした場合、`servicetype` プロパティには **HTTP** の値が割り当てられ、ポートには **80** の値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つ以上の引数を受け取ることができます。引数は、例えば文字列、数値、`ipaddress`、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(name): $name の値に文字列 "-lb" を連結したもの

この例では、「name」という文字列引数を受け取り、その引数の文字列に「-lb」を接尾辞として追加する文字列を作成する置換関数「form-lb-name」を定義しています。この置換関数を使用する式は次のように記述できます。

`$substitutions.form-lb-name("my")`

`my-lb` を返します。

別の例を考えてみましょう。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

置換:

`cspol-priority(priority): 10100 - 100 * $priority`

置換 `cspol-priority` は、priority という引数を受け取り、それを使用して値を計算する関数です。StyleBook の残りの部分では、この置換は次の例に示すように使用できます。

```
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)
```

次に示すのは、値がリストである `slist` という置換の例です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
substitutions:


  slist:


    - a


    - b


    - c
```

置換の値は、以下の `sdict` という置換の例に見られるように、キーと値のペアの辞書にすることもできます。

```
substitutions:


  sdict:


    a: 1


    b: 2


    c: 3
```

リストと辞書を組み合わせることで、より複雑な属性を作成できます。たとえば、`slistofdict` という置換は、キーと値のペアのリストを返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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、その値自体が別のリストです。

```
sdictoflist:


  a:


    - 1


    - 2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
b:

  - 3

  - 4
```

コンポーネントでは、これらの置換は condition、properties、repeat、repeat-condition の各構成で使用できます。

コンポーネントの次の例は、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
```

リストまたは辞書を値とす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CS仮想サーバーに紐付けられたすべてのLB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この構成を構築し、各LB仮想サーバーでその構成を繰り返すことを避けることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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における置換とコンポーネントを示しています。`cs-lb-mon` StyleBooksのプロパティを構築する際、複雑な置換「lb-properties」は、CS仮想サーバーに関連付けられたLB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、サーバーをパラメータとして受け取り、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のlb-poolパラメータに割り当てます。

```
substitutions:


  cs-port[]:


    true: int("80")


    false: int("443")


  lb-properties(name, servicetype, vip, port, servers):


    lb-appname: $name


    lb-service-type: $servicetype


    lb-virtual-ip: $vip


    lb-virtual-port: $port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    svc-servers: $servers


    svc-service-type: $servicetype


    monitors:


      -


        monitorname: $name


        type: PING


        interval: $parameters.monitor-interval


        interval_units: SEC


        retries: 3


components:


  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: cs-pools


    type: stlb::cs-lb-mon


    description: | Updates the cs-lb-mon configuration with the different
pools provided. Each pool with rule result in a dummy LB vserver, cs
action, cs policy, and csvserver_cspolicy_binding configuration.


    condition: $parameters.server-pools


    repeat: $parameters.server-pools


    repeat-item: pool


    repeat-condition: $pool.rule


    repeat-index: ndx


    properties:


      appname: $parameters.appname + "-cs"


      cs-virtual-ip: $parameters.vip
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      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。

```
substitutions:


     port:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        HTTP: 80


        DNS: 53


        SSL: 443
```

この例では、HTTPは80に、DNSは53に、SSLは443にマッピングされています。パラメータとして与えられた特定のプロトコルのポートを取得するには、次の式を使用します。

$substitutions.port

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、一連のlbvserverコンポーネントと、それに対応するサービスグループおよびバインドされたサーバーを作成します。

```
substitutions:

  apps:

    -

      name: lb1

      vip: 1.2.3.4

      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Componentsコンストラクトは、StyleBook内で最も重要なセクションと見なされます。このセクションでは、作成する必要がある構成オブジェクトを定義します。このコンストラクトを使用すると、同じタイプの構成オブジェクトを1つまたは複数構築できます。

componentsコンストラクトは、parametersセクションで提供される入力を使用して、StyleBookによって生成される構成を適応させることができます。ほとんどのStyleBookにはcomponentsセクションがありますが、これはオプションのセクションです。

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
`name`	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
`description`	StyleBookにおけるこのコンポーネントの役割の説明。
`type`	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` または `servicegroup` などです。コンポーネントに組み込みタイプ属性がある場合、NetScaler上にそのタイプの構成オブジェクトを作成します。たとえば、コンポーネントが組み込みタイプ `lbvserver` を参照する場合、このコンポーネントは、構成のターゲットであるNetScalerインスタンス上にロードバランシング仮想サーバーを作成します。**複合タイプ**: このタイプは、NetScaler Consoleに作成してインポートした既存のStyleBookを参照します。コンポーネントに複合タイプ属性がある場合、参照されるStyleBookで指定されたすべての構成オブジェクトを、構成のターゲットであるNetScalerインスタンス上に作成します。これにより、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。
`meta-properties`	メタプロパティは、NetScalerオブジェクトに対して実行されるアクションを定義します。有効なメタプロパティアクションとして、静的または動的な値を取ることができます。メタプロパティの式を指定すると、NetScalerオブジェクトに対して有効なメタプロパティアクションが動的に適用されます。この属性は、NetScalerオブジェクトに対して非CRUD操作を実行したい場合にStyleBookで使用できます。詳細については、「非CRUD操作を実行するStyleBookの作成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	説明
`properties`	コンポーネントタイプ属性に使用できるサブ属性。コンポーネントに有効なプロパティは、そのタイプによって決定されます。組み込みタイプの場合、これらは対応するNITROオブジェクトのプロパティまたは属性です。タイプが別のStyleBookであるコンポーネント、つまり複合タイプの場合、プロパティはそのStyleBookで定義されたパラメーターに対応します。

例:

```
components:

   -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name

        servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        ipv46: $parameters.ip


        port: 80


        lbmethod: $parameters.lb-alg
```

この例では、`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) 型で、"ns" は import-stylebooks セクションで指定した名前空間 `netscaler.nitro.config` およびバージョン 10.5 を参照するプレフィックスであり、`lbvserver` はこの名前空間内の 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4つとオプション属性1つ (`lbmethod`) 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` とポートに静的な値を指定していますが、name、ipv46、および `lbmethod` プロパティは入力パラメータ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名は、`$parameters.\<name>` 表記を使用して参照します (例: $parameters.ip)。

利用可能なすべてのNetScaler NITROリソースとその属性/プロパティの詳細については、NetScaler NITRO REST API ドキュメントを参照してください。

注

NITROリソースタイプ (そのコンポーネントプロパティ) の属性名には小文字を使用する必要があります。そうしないと、StyleBookのインポートは失敗します。

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組み込み型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、パラメーターオブジェクト、他のコンポーネントのプロパティ、または他のコンポーネントの出力などの他のセクションから入力を受け取り、それらを他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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポーネントには、オブジェクトタイプ、またはコンポーネントセクションを含まない別のStyleBookの2つのタイプがあります。

次の例は、NetScalerインスタンス上でモニター (`lb-mon-comp`) を使用してロードバランシングサーバーを作成するために使用されるStyleBookのスニペットを示しています。

```
parameters:

  -

    name: appname

    type: string

  -

    name: ips

    type: ipaddress[]

  -

    name: vip

    type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: help-comp

    type: cmtypes::server-ip-port-params

    repeat:

      repeat-list: $parameters.ips

      repeat-item: server-ip

    properties:

      ip: $server-ip

      port: 80

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: lb-mon-comp

type: stlb::lb-mon

properties:

  lb-appname: $parameters.appname

  lb-virtual-ip: $parameters.vip

  lb-virtual-port: 80

  lb-service-type: HTTP

  svc-service-type: HTTP

  svc-servers: $components.help-comp.properties
```

パラメーターセクションでは、アプリケーション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` パラメーターは、各項目に2つのサブパラメーター`ip` とポート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、このStyleBookのパラメーターセクションは、$parameters.ipsを介してのみサーバーIPを受け入れます。StyleBookは、すべてのサーバーがポート80で実行されていると仮定します。`lb-mon` StyleBookを使用してロードバランシング構成を作成するには、$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に設定されています）で構成されるオブジェクトを構築します。したがって、help-compはIPアドレスのリストを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。

オプションプロパティ

コンポーネントのプロパティが、パラメータ参照のような単純な式、またはより複雑な式から値を取得することがあります。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。

例えば、設定したいプロパティの1つが、タイプがns::lbvserverであるコンポーネントの`lbmethod` (ロードバランシングアルゴリズム) であるとします。プロパティ`lbmethod`の値は、以下に示すように、ユーザーが提供するパラメータ値から取得されます。

```
components


  -


      name: lbvserver_comp


      type: ns::lbvserver


      properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        name: $parameters.lb-appname + "-lb"

        servicetype: $parameters.lb-service-type

        ipv46: $parameters.lb-virtual-ip

        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
```

ここで、パラメータ**lb-advanced.algorithm**がオプションパラメータであるとします。ユーザーがオプションであるためこのパラメータに値を提供しない場合、式**$parameters.lb-advanced.algorithm**は空白値に評価されます。そのため、`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、プロパティをオプションとして注釈付けできます。以下に例を示します。

```
components


   -


     name: lbvserver_comp

     type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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し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


  -


    name: lbvserver_comp


    type: ns::lbvserver


    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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。タイプ「ns::lbvserver」でデフォルト値が定義されている場合、`lbmethod`はそのデフォルト値を取る可能性があることに注意してください。

プロパティ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のさまざまなセクションに分散している場合があります。たとえば、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取得されることがあります。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識別するリストです。

たとえば、`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します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb.name

      ipv46: $parameters.lb.ipv46
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      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$parameters.lbオブジェクトから取得されていることに注目してください。これらは単一のソースから取得されていますが、プロパティはStyleBookで再度定義されています。さらに、`lbvserver`の構成に関連する$parameters.lbオブジェクトへの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


    type: ns::lbvserver


components:


```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-


  name: lb-comp


  type: ns::lbvserver


  properties-default-sources:


    - $parameters.lb
```

上記の例では、properties-default-sources構成要素を使用することで、コンポーネント定義のサイズが削減され、コンポーネントを簡潔に定義できるようになります。さらに、コンポーネントのプロパティのソースが変更されるたびに、その変更が自動的に反映されます。たとえば、$parameters.lbオブジェクトに`persistencetype`という新しいプロパティが追加された場合、`persistencetype`が`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に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算出

このセクションでは、properties-default-sources構成要素がコンポーネントで使用された場合に、プロパティがどのように取得されるかについて説明します。まず、StyleBooksコンパイラは、そのタイプ（上記の例では`lbvserver`）に基づいて、コンポーネントのプロパティのリストを識別します。次に、コンパイラは、定義されている順序（コンポーネントのproperties-default-sourcesセクション内）で複数のソースからこれらのプロパティを取得します。プロパティが複数のソースに存在する場合、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、構成オブジェクトまたは親コンポーネントによって作成されたコンテキストを参照して、独自の構成オブジェクトを作成できます。ネストされたコンポーネントは、親コンポーネントで作成された各オブジェクトに対して1つ以上のオブジェクトを作成できます。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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    port: 80


    lbmethod: $parameters.lb-alg


    components:


      -


       name: my-svcg-comp


       type: ns::servicegroup


       properties:


          name: $parameters.name + "-svcgrp"


          servicetype: HTTP


       components:


          -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                properties:


                  ip: $srv


                  port: str($parameters.svc-port)


                  servicegroupname: $parent.properties.name
```

この例では、多層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。また、`my-svcg-comp` コンポーネントには2つの子コンポーネントが含まれています。`my-svcg-comp` コンポーネントは、組み込みのNITROリソースタイプ「`servicegroup`」の属性に値を提供することで、NetScalerインスタンス上にサービ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。2番目の子コンポーネントである `members-svcg-comp` は、サービスのリストを親コンポーネントによって作成されたサービスグループにバインドするために使用されます。このバインディングは、StyleBookの繰り返しコンストラクトを使用して、パラメータ `svc-servers` に指定されたサービスのリストを反復処理することで実現されます。繰り返しコンストラクトの詳細については、「繰り返しコンストラクト」を参照してください。

コンポーネントのネストを使用せずに、同じ構成オブジェクトを作成することもできます。詳細と例については、「基本的な負荷分散構成を作成するためのStyleBook」を参照してください。

条件コンストラクト

条件コンストラクトを使用すると、コンポーネントを条件付きにすることができます。条件コンストラクトの値は、trueまたはfalseに評価されるブール式です。条件がtrueの場合、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例:

```
components:

      -

        name: servicegroup-comp

        type: ns::servicegroup

        condition: $parameters.svc-server-ips

        properties:

              name: $parameters.name + "-svcgrp"

              servicetype: HTTP
```

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 `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、null値がこのパラメータに割り当てられ、falseと評価されると、StyleBookエンジンはこのコンポーネントの存在を無視し、`servicegroup` 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                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（スキップされず）、コンポーネント間に依存関係が作成された場合にのみ、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。

繰り返しコンストラクト

コンポーネントの **repeat** コンストラクトを使用して、同じタイプの複数の構成オブジェクトを構築できます。

以下の例では、**members-svcg-comp** コンポーネントは、サービスのリストを親コンポーネントによって作成されたサービスグループにバインドするために使用されます。各サーバーをサービスグループにバインドする構成オブジェクトを作成するには、**repeat** 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のリストを反復処理します。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** コンストラクトでは **srv** と呼ばれます）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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        components:
             -
                name: my-svcg-comp
                type: ns::servicegroup
                properties:
                     name: $parameters.name + "-svcgrp"
                     servicetype: HTTP
                components:
                      -
                      name: lbvserver-svg-binding-comp
                      type: ns::lbvserver\servicegroup\binding
                      properties:
                            name: $parent.parent.properties.name
                            servicegroupname: $parent.properties.name
                      -
                      name: members-svcg-comp
                      type: ns::servicegroup\servicegroupmember\binding
                      repeat:
                        repeat-list: $parameters.svc-servers
                        repeat-item: srv
                      properties:
                             ip: $srv
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                              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。
- 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            port: $parameters.svc-port


            servicegroupname: $parent.properties.name
```

リストを反復処理する際に現在の項目を参照できるだけでなく、**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。以下の例では、**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


            port: $parameters.base-port + repeat-index
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                servicegroupname: $parent.properties.name
```

repeat-item コンストラクトと同様に、反復処理の現在のインデックスを参照するために、異なる変数名を割り当てることができます。前の例は、以下の例と同等です。

```
    -

            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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                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」構成要素の使用方法を示しています。

例:

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        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構造を使用すると、コンポーネントの定義に応じて、各コンポーネントに複数の繰り返し構造を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:

```
parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

      name: vips

      type: ipaddress[]

  -

      name: vip-ports

      type: tcp-port[]

components:

  -

      name: lbvservers-comp

      type: ns::lbvserver

      repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        repeat-list: $parameters.vips


        repeat-item: ip


        repeat:


             repeat-list: $parameters.vip-ports


             repeat-item: port


    properties:


        name: str("lb-") + str($ip) + '-' + str($port)


        servicetype: HTTP


        ipv46: $ip


        port: $port
```

この例では、`$parameters.vips`内の各項目に対して、`$parameters.vip-ports`のすべての項目を反復処理します。したがって、`$parameters.vips`で指定された各`ipaddress`に対して、$parameters.vip-portsで指定されたすべてのポートに対して`lbvserver`構成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のプレフィックスとして

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「lb」を持つオブジェクトの名前を定義します。したがって、各反復処理で、`$ip + $port`はIPアドレスとポート番号の一意の組み合わせを定義します。

`repeat-item`属性が指定されていない場合、コンパイラはそれに対してデフォルト値を生成します。repeat-itemのデフォルト値は、各繰り返しレベルに対してそれぞれ`$repeat-item`、`$repeat-item-1`、`$repeat-item-2`です。同様に、`repeat-index`属性が指定されていない場合、コンパイラはそれに対してデフォルト値を生成します。repeat-indexのデフォルト値は、各繰り返しレベルに対してそれぞれ$repeat-index、$repeat-index-1、および$repeat-index-2です。

次の例では、ネストされた繰り返しオブジェクトにrepeat-item属性とrepeat-index属性がない場合の命名規則について説明します。

例:

```
components:


-


     name: lbvservers-comp


     type: ns::lbvserver


     repeat:


         repeat-list: $parameters.vips


         repeat:


            repeat-list: $parameters.vip-ports
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
properties:

   name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)

   servicetype: HTTP

   ipv46: $repeat-item

   port: $repeat-item-1
```

出力

出力セクションでは、StyleBookがすべての構成オブジェクトの作成を正常に完了した後に、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に柔軟性をもたらします。

次の表は、出力セクションで使用される属性について説明しています。

属性	説明	必須
名前	公開したい構成オブジェクトに対応する出力の名前。	はい
説明	出力を説明するテキスト文字列。	いいえ
値	この属性は、StyleBookによって返される値を抽出する方法を指定します。	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例：

```
outputs:


 -


   name: lbvserver


   description: LBVServer component


   value: $components.my-lbvserver-comp


 -


   name: svc-grp


     description: ServiceGroup name


     value: $components.my-svcg.properties.name
```

この例では、**lbvserver** コンポーネントと、StyleBook によって作成される `servicegroup` の**名前**を公開します。**lbvserver** と呼ばれる出力の値は、コンポーネント **my-lbvserver-comp** です。同様に、**svc-grp** と呼ばれる出力の値は、コンポーネント **my-svcg** によって作成される `servicegroup` の名前です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ参照

コンポーネント構成では、パラメータセクションで定義されたパラメータを `$parameters.<parametername>` 表記を使用して参照します。`<parametername>` 自体がパラメータを含む場合（タイプがオブジェクトの場合）、`$parameters.<parametername>.<sub-parametername>` の表記を使用する必要があります。

例:

```
parameters:


  -


    name: name


    label: Name


    type: string


    required: true


     -


      name: vip


      label: Virtual IP and Port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: object

    required: true

    parameters:

      -

        name: ip

        label: Virtual IP

        description: The Virtual IP Address

        type: ipaddress

        required: true

          -

            name: port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      ipv46: $parameters.vip.ip


      port: $parameters.vip.port
```

親参照

ネストされたコンポーネントを使用している場合、$parent 表記を使用して親コンポーネントを参照できます。親コンポーネントが repeat コンストラクトを使用して複数の構成オブジェクトを構築し、各イテレーション内で子コンポーネントが他の構成オブジェクトを構築する場合、$parent 表記は常に親コンポーネントの現在のイテレーションを参照します。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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    servicetype: HTTP


    ipv46: $parameters.ip


    port: 80


    lbmethod: $parameters.lb-alg


    components:


      -


        name: my-svcg-comp


        type: ns::servicegroup


        properties:


          name: $parameters.name + "-svcgrp"


          servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        components:

         -

           name: lbvserver-svg-binding-comp

           type: ns::lbvserver_servicegroup_binding

           properties:

              name: $parent.parent.properties.name

              servicegroupname: $parent.properties.name

                -

                  name: members-svcg-comp

                  type: ns::servicegroup_servicegroupmember_binding

                  repeat: $parameters.svc-servers
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    repeat-item: srv


                    properties:


                      ip: $srv


                      port: str($parameters.svc-port)


                      servicegroupname: $parent.properties.name
```

最上位コンポーネントに至るまで、親の親のプロパティにアクセスすることで、コンポーネントの階層を上位に移動することもできます。例えば、**lbvserver-svg-binding-comp** コンポーネントのプロパティ名が、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するのは、**$parent.parent** 表記を使用することによってです。

コンポーネントリファレンス

コンポーネント構成では、`$components.<componentname>`表記を使用してStyleBookのトップレベルコンポーネントを参照します。トップレベルコンポーネント内にネストされたコンポーネントがある場合、それらを参照するために`$components.<componentname>.components.<component-name>`表記が使用され、以下同様です。

例:

```
components:


 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: my-lbvserver-comp

    type: ns::lbvserver

    properties:

       name: $parameters.name + "-lb"

       servicetype: HTTP

       ipv46: $parameters.ip

       port: 80

       lbmethod: $parameters.lb-alg

-

    name: my-svcg-comp

    type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

       name: $parameters.name + "-svcgrp"

       servicetype: HTTP

-

    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv

    properties:

       ip: $srv

       port: str($parameters.svc-port)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        servicegroupname: $components.my-svcg-comp.properties.name


-


    name: lbvserver-svg-binding-comp


    type: ns::lbvserver_servicegroup_binding


    properties:


        name: $components.my-lbvserver-comp.properties.name


        servicegroupname: $components.my-svcg-comp.properties.name
```

この例では、最後のコンポーネント**lbvserver-svg-binding-comp**を構築する前に、コンポーネント**my-svcg-comp**と**my-lbvserver-comp**を構築する必要があります。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、**`$substitutions.<substitution-name>`** 表記を使用して、置換セクションで定義された置換を参照します。例: **$substitutions.http-port**。

置換がマップである場合、マップ内の要素を**`$substitutions.<substitutions-name>[<map-key>]`**として参照できます。例: **`$substitutions.protocol-map[$parameters.port]`**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

変数参照

コンポーネントでrepeatおよびrepeat-item構成要素を使用して複数の構成オブジェクトを構築する場合、repeat-item構成要素に変数名を割り当てることができます。この変数は、`$<varname>` という表記を使用して、そのコンポーネントのプロパティまたは子コンポーネントで参照できます。コンポーネントでrepeat構成要素がrepeat-item構成要素なしで使用される場合、$repeat-itemというデフォルト変数を使用してイテレーション項目にアクセス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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    domain: $server-name

  components:

    -

      name: service-members-comp

      type: ns::service

      properties:

        name: $server-name + "-service"

        servername: $parent.properties.name

        servicetype: $parameters.svc-service-type

        port: $parameters.svc-server-port
```

上記の例では、変数名「server-name」がrepeat-item構成要素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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

操作

`Operations`は、StyleBookのオプションセクションです。このセクションでは、NetScaler Console Analyticsを設定して、すべてのトラフィックトランザクションまたは一部のトラフィックトランザクションでAppFlowレコードを収集できます。StyleBookを使用してNetScalerインスタンス上に作成された仮想サーバーが、トラフィックトランザクションを処理します。また、仮想サーバーで特定のトラフィック条件が満たされたときにアラームをトリガーするようにNetScaler Consoleを設定することもできます。

StyleBookを介してNetScaler Consoleを設定し、以下にリストされているさまざまなNetScaler Consoleインサイトからトラフィック統計を収集できます。

- Bot インサイト
- Web インサイト
- Security インサイト
- 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分析のために、Web インサイトと Security インサイトの両方、またはそのいずれかを有効にします。ただし、VPN仮想サーバーの場合は、HDX インサイトとNetScaler Gateway インサイトの両方、またはそのいずれかを有効にする必要があります。

StyleBookを介してNetScalerインスタンスで有効になっているNetScaler Consoleインサイトは、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 インサイトを有効にすると、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「クライアント側測定」が有効になります。この機能が有効になっていると、NetScaler ConsoleはHTMLインジェクションを介して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と、管理者はL7遅延の問題を特定できます。

特定のNetScaler Consoleインサイトを有効にした後、**アプリケーション概要**ページを表示して、そのインサイトに関連する脅威の詳細を確認します。

例 1:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の例は、StyleBookで操作セクションを記述して、VPN仮想サーバーでHDX インサイトと NetScaler Gateway インサイトの両方を有効にする方法を示しています。

```
name: simple-vpn-ops


namespace: com.example.stylebooks


schema-version: "1.0"


version: "0.1"


description: Test StyleBook to enable hdxinsight and gatewayinsight on a
VPN vserver


import-stylebooks:


  -


    namespace: netscaler.nitro.config


    version: "10.5"


    prefix: ns
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: vpnvserver-comp

    type: ns::vpnvserver

    properties:

      name: str("vpn-") + str($current-target.ip)

      servicetype: SSL

      ipv46: 1.1.21.37

      port: 443

operations:

    analytics:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      -


        name: comp-ops


        properties:


          target: $components.vpnvserver-comp


          filter: "true"


          insights:


            -


              type: hdxinsight
            -
              type: gatewayinsight


outputs:


  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: myvpns



    value: $components.vpnvserver-comp
```

例2：

以下の例は、StyleBookでoperationsセクションを記述して、ロードバランシング仮想サーバー上でWeb Insight、Security Insight、およびBot Insightを有効にする方法を示しています。

```
---

name: enable-insights

namespace: com.acme.stylebooks

description: "This StyleBook enables Web,Security & Bot Insight on Load
Balancing Vserver"

display-name: "SB Operations"

schema-version: "1.0"

version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -
    name: lbname
    type: string
    required: true
   -
    name: vip
    type: ipaddress
    required: true
   -
    name: appflowfilter
    type: string
    required: true


components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lbname
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: HTTP
      ipv46: $parameters.vip
      port: 80


outputs:
  -
    name: mylb
    value: $components.my-lbvserver-comp


operations:
  analytics:
    -
      name: lbvserver-op
      properties:
        target: $outputs.mylb
        filter: $parameters.appflowfilter
        insights:
          -
            type: webinsight
          -
            type: securityinsight
          -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        type: botinsight
```

分析

分析セクションの各要素は、StyleBookで作成された1つ以上の仮想サーバーに対して、NetScaler Consoleの分析機能を構成するために使用されます。

分析セクションの要素には、次の属性があります。

属性	説明	必須
名前	分析要素の名前。	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と評価されると、分析要素全体がスキップされます。	いいえ
繰り返し	リストを反復処理します。	いいえ
繰り返し条件	ブール式。式がfalseと評価された場合、現在の反復はスキップされます。	いいえ
繰り返し項目	現在の反復における項目の名前。	いいえ
繰り返しインデックス	現在の反復におけるインデックス値の名前。	いいえ
プロパティ	分析操作プロパティのリスト。	はい
ターゲット	リスト内のプロパティの1つです。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、その仮想サーバーの分析情報が収集されます。	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	説明	必須
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、分析情報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、仮想サーバーを通過するすべてのトラフィックで分析データが収集されます。	いいえ
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種類です。デフォルトでは、(#target-virtual-servers-and-insight-types)で指定されている仮想サーバーの種類に基づいて、許可されているすべてのインサイトがターゲット仮想サーバーに構成されます。	いいえ
トランスポートモード	リスト内のプロパティの1つです。この属性の値は、`logstream`または`ipfix`のいずれかです。`logstream`がデフォルト値です。	いいえ
クライアント側測定	リスト内のプロパティの1つです。この属性の値は、ENABLEDまたはDISABLEDのいずれかです。DISABLEDがデフォルト値です。	いいえ
HTTP-X-フォワーデッド-フォー	リスト内のプロパティの1つ。この属性の値は、ENABLEDまたはDISABLEDのいずれかです。この属性は、クライアントIP情報をバックエンドサーバーに渡す	いいえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	説明	必須
	ためのX-Forwarded-Forヘッダーの挿入を有効または無効にします。DISABLEDがデフォルト値です。	
HDXInsight の有効化	リスト内のプロパティの1つ。この属性の値は、ICAまたはTCPのいずれかです。この属性は、特定のトラフィックデータに対して `hdxinsight` を有効にします。ICAがデフォルト値です。	いいえ

例 1: 単一の仮想サーバーの分析を構成する

```
operations:



  analytics:

    -

    name: lbvserver-ops-comp

    properties:

        target: $components-basic-lb-comp.outputs.lbvserver-name

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        transport-mode: logstream

        client-side-measurements: ENABLED

        insights:

          -

            type: webinsight
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          -

            type: securityinsight
```

例 2: VPN仮想サーバーのリストの分析を構成する

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        http-x-forwarded-for: ENABLED

        insights:

          -

            type: hdxinsight

            enable-hdxinsight-for: TCP
```

分析セクションの各属性は、ターゲットプロパティによって識別される仮想サーバーでAppFlowレコードを収集するようにNetScalerインスタンスを構成します。

ターゲット仮想サーバーとインサイトタイプ

ターゲット仮想サーバーと対応する許可されるインサイトタイプは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ターゲット仮想サーバー	インサイトタイプ
LBVサーバー	ウェブインサイト、セキュリティインサイト、ボットインサイト
CSVサーバー	Web インサイト、Security インサイト、Bot インサイト
VPNサーバー	HDXインサイト、ゲートウェイインサイト

注

IPFIXは、StyleBooksで仮想サーバーの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

オペレーションセクションのアラームサブセクションは、アナリティクスサブセクションと同様の構造と属性を持っています。唯一の違いは、プロパティ属性にあります。（プロパティ属性以外の）すべての属性のリストについては、アナリティクスを参照してください。

以下に示すプロパティは、アラームサブセクションで利用できます。

属性	説明	必須
`target`	NetScalerで構成され、アラームが構成されている仮想サーバーの名前を評価する式。	はい
`email-profile`	NetScaler Console Analytics機能で定義され、アラームがトリガーされたときに通知したいメールアドレスのリストが含まれている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-profile`	NetScaler Console Analytics機能で定義され、アラームがトリガーされたときに通知したい電話番号のリストが含ま	いいえ (`email-profile` または `sms-profile` のいずれかを定義する必要があります)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	説明	必須
	れているSMSプロファイルの名前。	
`rules`	ターゲットプロパティで定義された仮想サーバーのアラームをトリガーする条件を定義するルールの一覧。	はい
`metric`	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
`operator`	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
`value`	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
`period-unit`	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。この属性には、day、hour、または weekly の値を指定できます。これは、ルールが満たされた場合、アラームが期間単位で1回送信されることを意味します（例：1日1回）。	はい

以下の表は、NetScaler仮想サーバーに関連して追跡されるメトリックのリストを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カウンター	説明	詳細な説明	NETSCALER CONSOLEの計算
VPN仮想サーバーの場合：			
total_requests	VPNセッション起動総数	ユーザーが指定した時間間隔中にこのVPN仮想サーバーで開始されたアクティブセッションの総数。	単調増加カウンター。新しいセッションが起動されるたびに増加します。
app_count	VPNアプリ起動数	ユーザーが指定した時間間隔中にこのVPN仮想サーバーで起動された一意のVPNアプリケーションの総数。	新しいアプリケーションが起動されるたびに単調増加するカウンター
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 Console	この仮想サーバーによって処理された合計バイト数をカウン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カウンター	説明	詳細な説明	NETSCALER CONSOLEの計算
		に転送された合計バイト数。	トするための単調増加カウンター。
application_response_time	応答時間	仮想サーバーの平均応答時間。	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から、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:

```
operations:

alarms:

 -

  name:lbvserver_alarm

  properties:

      target: $outputs.lbvserver

      email-profile: $parameters.emailprofile

      sms-profile: "NetScalerSMS"

      rules:

      -

        metric: "total_requests"

        operator: "greaterthan"

        value: 25
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        period-unit: weekly

        -

          metric: "total_bytes"

          operator: "lessthan"

          value: 1024

          period-unit: day
```

式

StyleBookの最も強力な機能の1つは、式を使用することです。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、パラメータ値とリテラル文字列を連結する式です。

例:

```
$parameters.appname + "-mon"
```

この式は、`appname`という名前のパラメータを取得し、`-mon`という文字列と連結します。

注

StyleBook定義でパラメータと式を定義する際に、予約済みキーワードの使用をサポートしています。予約済みキーワードは、`and`、`false`、`in`、`not`、`true`、および`or`です。

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 (/)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- モジュロ (%)

例:

- 2つの数値を加算する: $parameters.a + $parameters.b
- 2つの数値を乗算する: $parameters.a * 10
- ある数値を別の数値で除算した後の剰余を求める:

`15%10` の結果は `5` になります

文字列式

- 2つの文字列を連結する (+)

例:

2つの文字列を連結する: str("app-") + $parameters.appname

リスト式

2つのリストをマージする (+)

例:

- 2つのリストを連結する: $parameters.external-servers + $parameters.internal-servers
- もし `$parameters.ports-1` が で、 `$parameters.port-2` が の場合、 `$parameters.ports-1 + $parameters.ports-2` はリスト として表示されます。

関係式

- **==** : 2つのオペランドが等しいかどうかをテストし、等しい場合はtrueを返し、そうでない場合はfalseを返します。
- **!=** : 2つのオペランドが異なるかどうかをテストし、異なる場合はtrueを返し、そうでない場合はfalseを返します。
- **\>** : 最初のオペランドが2番目のオペランドより大きい場合、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の場合、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、それ以外の場合はfalseを返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **\<=** : 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、それ以外の場合はfalseを返します。

例:

- 等価演算子の使用: `$parameters.name = = "abcd"`
- 不等価演算子の使用: `$parameters.name != "default"`
- その他の関係演算子の例
  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`
  - `10 <= 9`
  - `10 == 10`
  - `10 != 1`

論理式 - ブール

- **and**: 論理「and」演算子。両方のオペランドが真の場合、結果は真になり、それ以外の場合は偽になります。
- **or**: 論理「or」演算子。いずれかのオペランドが真の場合、結果は真になり、それ以外の場合は偽になります。
- **not**: 単項演算子。オペランドが真の場合、結果は偽になり、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（int()組み込み関数を使用）、数値が文字列に変換される（str()組み込み関数を使用）式を型キャストできます。同様に、`tcp-port`を数値にキャストでき（`int()`組み込み関数を使用）、IPアドレスを文字列にキャストできます（str()組み込み関数を使用）。

任意の演算子の前後に区切り文字を使用します。以下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`、`(`、`[`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例:

- `abc + def`
- `100 % 10`
- `10 > 9`
- `$item in $parameters.some-list`

スプラット式

スプラット式 `[*]` は、複雑なリストから特定の属性をすべての反復処理で取得するためのより簡単な方法を提供します。StyleBook 定義にスプラット式を含めることができるようになりました。

構文:

```
list[*].attribute
```

この式は、左側に指定されたリストのすべての項目を反復処理し、右側に指定された属性値を返します。

リストから各仮想サーバーのIPアドレスまたはホスト名を取得したい場合は、次のスプラット式を使用できます。

例 1:

```
$parameters.server-members[*].hostname
```

この式は、すべてのサーバーメンバーからホスト名のリストを返します。

例 2:

```
$parameters.server-members[*].sub-domains[*].name
```

この式は、各サーバーメンバーのサブドメイン下のすべての名前のリストを返します。

これらの式は常に、最も右側の要素タイプのリストを返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

逐語的文字列式

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、逐語的文字列を使用できます。これらの文字列には、エスケープ文字、バックスラッシュ、引用符、括弧、空白、角括弧などが含まれます。逐語的文字列では、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。逐語的文字列を使用しない場合、文字列を部分文字列に分割して特殊文字をエスケープする必要があります。

逐語的文字列を作成するには、次のように特殊文字の間に文字列をカプセル化します。

```
~{string}~
```

StyleBook 式で逐語的文字列を使用できます。

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的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=")}~
```

詳細については、StyleBook で特殊文字をリテラル形式で許可する を参照してください。

ターゲット式

StyleBook の定義では、`$current-target` 式を使用して現在のターゲット NetScaler インスタンスを参照できます。ターゲット NetScaler インスタンスの IP アドレスを具体的に参照するには、この式を次のように使用します。

```
$current-target.ip
```

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

 -

  name: lb-comp

  type: ns::lbvserver

  properties:

    name: $current-target.ip + "-lbvserver"
```

この例では、`lbvserver` の名前はターゲット NetScaler インスタンスの IP アドレスを使用しています。

式の型検証

StyleBook エンジンは、コンパイル時に強力な型チェックを可能にするようになりました。つまり、StyleBook の作成中に使用される式は、構成パックの作成時ではなく、StyleBook 自体のインポート時に検証されます。

パラメーター、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（繰り返し項目、繰り返しインデックス、置換関数の引数）などへのすべての参照は、その存在と型についてすべて検証されます。

型チェックの例:

次の例では、`lbvserver` StyleBook のポートプロパティの予期される型は `tcp-port` です。NetScaler Console では、型検証はコンパイル時（インポート時）に行われます。コンパイラは、文字列と `tcp-port` が互換性のない型であると判断し、そのため、StyleBook コンパイラはエラーを表示し、StyleBook のインポートまたは移行に失敗します。

```


components:

  -

    name: lbvserver-comp

    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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:

StyleBookをNetScaler Consoleにインポートすると、コンパイラは無効な式を識別してフラグを付けます。その結果、StyleBookはNetScaler Consoleにインポートされません。

次の例では、`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。ただし、`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。

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
```

データ型の暗黙的な型変換

異なるデータ型にStyleBook式を使用すると、StyleBookエンジンは出力を適切なデータ型に暗黙的に型変換するようになりました。データ型の暗黙的な型変換は、二項演算と値の割り当てをサポートします。

二項演算の例:

- `string`型と`number`型の2つの変数を加算(+)すると、出力データ型は`string`に設定されます。

`$parameters.appname + '_' + $parameters.app_instance_num`

- `string`型と`ipaddress`型の2つの変数を加算(+)すると、出力データ型は`string`に設定されます。

`$parameters.appname + '_' + $parameters.instance_ip`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ipaddress`型と`number`型の2つの変数を加算(+)すると、出力データ型は`ipaddress`に設定されます。

```
$parameters.instance_ip + $parameters.number
```

- `ipaddress`型と`number`型の2つの変数を減算(-)すると、出力データ型は`ipaddress`に設定されます。

```
$parameters.instance_ip - $parameters.number
```

- `string`型と`number`型の2つの変数を乗算(*)すると、出力データ型は`string`に設定されます。

```
$parameters.dummy_str * $parameters.count
```

値の割り当ての例:

- 変数が`string`データ型として定義されている場合、割り当てられた値は定義されたデータ型に変換されます。

```
name: $parameters.port * 3
```

- 変数が`portnumber`データ型として定義されている場合、割り当てられた値は例外を除いて`portnumber`データ型に変換されます。

```
port: $index + $parameters.lower_limit
```

リストのインデックス付け

リストの項目には、直接インデックスを付けることでアクセスできるようになりました。

式	説明
`$components.test-lbs[0]`	`thetest-lbs`コンポーネント内の最初の項目を参照します
`$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`コンポーネントの2番目のアイテムのプロパティ`servicegroupname`を参照します。これは、`lbcomps`コンポーネントの最初のアイテムからの出力です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBookのポリシー式

StyleBook GUIを使用すると、リストから項目を選択してNetScaler®ポリシー式を構築でき、より迅速かつ正確に式を作成できます。

StyleBookのポリシー式を使用すると、柔軟でカスタマイズ可能な構成を作成できます。さまざまなパラメーター、属性、または変数に基づいて条件を指定できます。ポリシー式は、NetScalerポリシー構成を実装するためによく使用されます。

STYLEBOOK GUIでポリシー式エディターを有効にする

パラメーターでEPAまたは式エディターを使用できるようにするには、パラメーター定義で `is_policy_expression` GUI属性を指定します。この設定を有効にすると（trueに設定）、このパラメーターの値を入力するときに**式エディター**を呼び出すことができます。

```
parameters:

  -

    name: expression

    type: string

    label: Expression

    required: true

    gui:

      is_policy_expression: true
```

ポリシー式の作成と構築

1. **アプリケーション > 構成 > StyleBook**に移動します。**StyleBook**ページには、NetScaler Consoleで利用可能なすべてのStyleBookが表示されます。
2. パラメーターにポリシー式を含むStyleBookを選択します。
3. **構成の作成**をクリックします。**構成の作成**ページで、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します。
4. **式**フィールドの横にあるアイコンをクリックします。**式の作成**ページが表示されます。

   式を使用した構成の作成(/en-us/netscaler-console-service/media/stylebooks-expression-create.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. **式の作成**で、直感的なドロップダウンを使用してポリシー式を構築します。**送信**をクリックします。

   式エディター(/en-us/netscaler-console-service/media/stylebooks-expression-editor.png)

   カスタムポリシー式を作成する場合は、**EPAエディター**または**式エディター**をクリックして式を構築します。**式のプレビュー**で式を確認し、**送信**をクリックします。
6. 構成を展開するターゲットのNetScalerインスタンスを選択し、「**Submit**」をクリックします。

インプレース補間

StyleBook式を使用して文字列の一部を置換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式を使用している文字列の部分は、その式の値に置換されます。文字列にStyleBook式を含めるには、次の表記法を使用します。

```
"...%{...}%..."
```

「%{」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。

例えば、文字列 `lb-%{$parameters.appname}%-svc` は、StyleBook式のインプレース補間を含む文字列式です。文字列式の値は、補間式の値に依存します。**$parameters.appname** に「app1」が割り当てられているとします。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、例えば「jpeg」が含まれているかどうかをチェックするポリシー式を作成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、StyleBookに文字列パラメータ、例えば `$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されます。そのためには、文字列連結を使用して結果を実現します。式は次のようになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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

補間内では、boolean、number、`tcp-port`、`ipaddress`、string のいずれかの型の値を生成する式を使用できます。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式で置換できます。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。

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。

$parameters.port が 80 の場合、内部文字列「**%{$parameters.port + 1}%**」は「lb-81」を返します。ここでは、この式は別の補間式の中にネストされています。

以下の表は、補間のさまざまなタイプを例と対応する結果とともに説明しています。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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-%{トゥルー}%	lb-トゥルー

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

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
`str("%{quotewrap(abcd)}%")`	`\"abcd`
`str("%{quotewrap(https://)}%+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	`<https://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

補間におけるエスケープ文字

文字列の一部として「% {」または「}%」の文字がある場合、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) + \}\%}%") returns "%{1.1.1.1}%" if $parameters.vip is 1.1.1.1
```

次の表に、いくつかの式とその結果を示します。

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。

たとえば、組み込み関数 `str()` を使用して、数値を文字列に変換できます。

```
str($parameters.order)
```

または、組み込み関数 `int()` を使用して、文字列を整数に変換できます。

```
int($parameters.priority)
```

以下は、StyleBook の式でサポートされている組み込み関数と、その使用方法の例のリストです。

文字列()

`str()` 関数は、入力引数を文字列値に変換します。

許可される引数の型:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `string`
- `number`
- `tcp-port`
- `boolean`
- `ipaddress`

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(True)` 関数は `"True"` を返します。
- `str(NetScaler Console)` 関数は `"NetScaler Console"` 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。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

長さ()

`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 Console")` 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。

最小値()

`min()` 関数は、引数としてリストまたは一連の数値またはTCPポートを受け取り、最小の項目を返します。

数値/TCPポートの系列の例:

- `min(80, 100, 1000)` 関数は `80` を返します。
- `min(-20, 100, 400)` 関数は `-20` を返します。
- `min(-80, -20, -10)` 関数は `-80` を返します。
- `min(0, 100, -400)` 関数は `-400` を返します。

数値/TCPポートのリストの例:

- サポート `$parameters.ports` はTCPポートのリストであり、値は `[80, 81, 8080]` です。

  `min($parameters.ports)` 関数は `80` を返します。

マックス()

`max()` 関数は、引数としてリストまたは一連の数値またはTCPポートを受け取り、最大の項目を返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数値/TCPポートの系列の例:

- `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ポートのリストであり、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。

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：

「`hex(100)`」関数は「`0x64`」を返します。

lower() 関数

「`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:

「`lower("NetScaler Console")`」関数は「`NetScaler Console`」を返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

upper() 関数

「`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:

「`upper("NetScaler Console")`」関数は「`NetScaler Console`」を返します。

sum() 関数

「`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]
```

「`sum($substitutions.list-of-numbers)`」関数は「`88`」を返します。

例2:

`$parameters.ports`が`[80, 81, 82]`の場合、`sum($parameters.ports)`関数は`243`を返します。

pow() 関数

`pow()`関数は2つの数値を引数として受け取り、最初の引数を2番目の引数の累乗で表す数値を返します。

例:

`pow(3,2)`関数は`9`を返します。

ip()

`ip()`関数は、整数、文字列、またはIPアドレスを引数として受け取り、入力値に基づいてIPアドレスを返します。

例:

- `ip`関数でIPアドレスを指定します。

  `ip(3.1.1.1)`関数は`3.1.1.1`を返します。
- `ip`関数で文字列を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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、入力の同等の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。

ip_network()

`ip_network` 関数は、IPアドレスとネットマスク長を引数として受け取り、IPネットワーク表記を返します。

例-1:

`ip_network(1.1.1.1, 28)` 関数は `1.1.1.1/28` を返します。

例-2:

`$parameters.ipaddr` の値として `1.1.1.1` を考慮します。
`ip_network($parameters.ipaddr, 30)` 関数は `1.1.1.1/30` を返します。

例-3:

`$parameters.netmask-len` の値として `24` を考慮します。`ip_network(23.1.12.76, $parameters.netmask-len)` 関数は `23.1.12.76/24` を返します。

network_ip()

The `network_ip()` 関数は、指定されたIPネットワークの最初のIPアドレスを返します。

例：

The `network_ip(1.1.1.1/28)` 関数は `1.1.1.0` を返します。この例では、`1.1.1.0` が指定されたネットワークの最初のIPアドレスです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

subnets() 関数

The `subnets()` 関数は、指定されたIPネットワークとネットマスク長からサブネットのリストを返します。

例：

The `subnets(1.1.1.1/28, 30)` 関数は、指定されたIPネットワークとネットマスク長からサブネットリストを返します。出力は次のようになります。

```
[1.1.1.0/30', '1.1.1.4/30', '1.1.1.8/30', '1.1.1.12/30']
```

netmask_ip()

The `netmask_ip()` 関数は、指定されたIPネットワークのネットマスクIPアドレスを返します。

例：

The `netmask_ip(1.1.1.1/28)` 関数は `255.255.255.240` を返します。指定されたIPネットワークの場合、`255.255.255.240` がネットマスクIPアドレスです。

is_netmask_ip()

The `is_netmask_ip()` 関数は入力として `ipaddress` を受け入れます。そして、指定された値が有効なネットマスクIPアドレスである場合、`True` を返します。

例 1：

「`is_netmask_ip(255.255.255.240)` 関数は、指定された値が有効なネットマスクIPアドレスであるため、`True` を返します。」.

例 2:

「`is_netmask_ip(255.255.255.232)` 関数は、指定された値が有効なネットマスクIPアドレスではないため、`False` を返します。」.

broadcast_ip()

「`broadcast_ip()` 関数は、指定されたIPネットワークのブロードキャストIPアドレスを返します。」.

例:

「`broadcast_ip(1.1.1.1/28)` 関数は `1.1.1.15` を返します。指定されたIPネットワークの場合、`1.1.1.15` がブロードキャストIPアドレスです。」.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シーアイディーアール()

「`cidr()` 関数は、指定されたIPネットワークのCIDR表記を返します。」.

例:

「`cidr(1.1.1.1/28)` 関数は `1.1.1.0/28` を返します。指定されたIPネットワークの場合、`1.1.1.0/28` がCIDR表記です。」.

is_cidr()

「`is_cidr()` 関数は入力として `ipnetwork` を受け入れます。そして、指定された値がIPネットワークのCIDR表記と一致する場合、`True` を返します。」.

例-1:

「`is_cidr(1.1.1.0/24)` 関数は、指定された値が与えられたネットワークのCIDR表記であるため、`True` を返します。」.

例-2:

`is_cidr(1.1.1.1/28)`関数は、指定されたネットワークのCIDR表記が指定された値と異なるため、`False`を返します。

is_in_network()

`is_in_network()`関数は`ipnetwork`と`ipaddress`の値を受け入れます。そして、指定されたIPアドレスが指定されたIPネットワーク内に存在する場合、`True`を返します。

例-1:

`is_in_network(1.1.1.1/24, 1.1.1.121)`関数は、`1.1.1.121`アドレスが`1.1.1.1/24`ネットワークの一部であるため、`True`を返します。

例-2:

`is_in_network(1.1.1.1/28, 2.1.1.1)`関数は、`2.1.1.1`アドレスが`1.1.1.1/28`ネットワークの一部ではないため、`Fasle`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:

The `base64.decode("YWJjZA==")` 関数は `abcd` を返します。

イグジスツ()

The `exists()` 関数は任意の型の引数を取り、ブール値を返します。入力に何らかの値がある場合、戻り値は `True` です。入力引数に値がない場合（つまり、値がない場合）、戻り値は `False` です。

The `$parameters.monitor` はオプションのパラメーターであるとします。設定パックを作成する際にこのパラメーターに値を指定すると、`($parameters.monitor)` 関数は `True` を返します。

そうでない場合、`False` を返します。

フィルター()

The `filter()` 関数は2つの引数を取ります。

引数1：1つの引数を取り、ブール値を返す置換関数。

引数2：リスト。

この関数は、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。最初の 引数にある置換関数に渡されたときに。

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、True を返します。そうでない場合、`False` を返します。

仮に、`$parameters.ports` が `[81, 80, 81, 89]` であるとします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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。

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：

`$parameters.servicetype`の値が`HTTP`の場合、`if-then-else($parameters.servicetype == HTTP, 80, 443)`関数は`80`を返します。それ以外の場合、関数は`443`を返します。

例2：

`$parameters.servicetype`の値が`HTTP`の場合、`if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)`関数は`$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:

`$parameters.servicetype`が`HTTP`の値を持つ場合、`if-then-else($parameters.servicetype == HTTP, 80)`は`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：`number`、`tcp-port`、`string`、`ipaddress`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で区切られます。引数2が指定されていない場合、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した場合：

    `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つのスペースと見なします。

map() 関数

`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 を使用したマップ

  `map(str, $parameters.nums)` 関数は `["81", "82", "83"]` を返します。

  マップ関数の結果は文字列のリストであり、各要素は入力リスト ($parameters.nums) の対応する要素に str 関数を適用することによって計算されます。

- 置換関数を使用したマップ
  - 置換:

    `add-10(port): $port + 10`

  - 式:

    `map($substitutions.add-10, $parameters.nums)` 関数は数値のリスト `[ 91, 92, 93 ]` を返します。

このマップ関数の結果は数値のリストです。各要素は、入力リスト `($parameters.nums)` の対応する要素に置換関数 `$substitutions.add-10` を適用することによって計算されます。

quotewrap() 関数

`quotewrap()` 関数は文字列を引数として受け取り、入力値の前後に二重引用符文字を追加した文字列を返します。

例:

「`quotewrap("NetScaler Console")` 関数は `"NetScaler Console"` を返します。」

リプレース()

「`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: 次の組み込み型の `string` またはリスト」:

- `string`
- `number`
- `ipaddress`
- `tcp-port`
- `boolean`

「引数2: 引数1で指定された型と一致する型の単一の値または値のリスト」

「引数3: 引数1で指定された型と同じ型の単一の値 (オプション)」

「`replace()` 関数は、引数1内の引数2のすべての出現箇所を引数3に置き換えます。」.

「引数3が指定されていない場合、引数1から引数2のすべての出現箇所が削除されます。」.

例:

- 「`replace('abcdef', 'def', 'xyz')` 関数は `abcxyz` を返します。」.

  `def` のすべての出現箇所は `xyz` に置き換えられます。
- `replace('abcdefabc', 'def')` は `abcabc` を返します。

  引数3がないため、`def` は結果の文字列から削除されます。
- `replace('An#example@to%replace!characters', ['@', '#', '!', '%'], '_')` 関数は `An_example_to_replace_characters` を返します。

  出力文字列には、`['@', '#', '!', '%']` で指定された文字の代わりにアンダースコア (_) が含まれます。
- `replace([10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4], [10.10.10.2, 10.10.10.4])` 関数は `[10.10.10.1, 10.10.10.3]` を返します。

  引数3がないため、`10.10.10.2` と `10.10.10.4` は結果のIPアドレスリストから削除されます。
- `replace([8080, 8081, 8082, 8083, 8084], 8083, 80)` 関数は `[8080, 8081, 8082, 80, 8084]` を返します。

  `8083` のすべての出現箇所は `80` に置き換えられます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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('Stylebooks', 6)` は `Styleb` 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: `$parameters.input_list` が `['ADC', 'VPX', 'ADC', 'CPX']` の場合、`distinct($parameters.input_list)` 関数は `['ADC', 'VPX', 'CPX']` を返します。

url.encode()

`url.encode()` 関数は、RFC 3986 に従って ASCII 文字セットを使用して文字が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:

The `url.decode("a%2Fb%2Fc")` 関数は `a/b/c` を返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イズ・アイピーブイフォー()

The `is-ipv4()` 関数はIPアドレスを引数として受け取り、そのIPアドレスがIPv4形式である場合にブール値 `True` を返します。

The `is-ipv4(10.10.10.10)` 関数は `True` を返します。

イズ・アイピーブイシックス()

The `is-ipv6()` 関数はIPアドレスを引数として受け取り、そのIPアドレスがIPv6形式である場合にブール値 `True` を返します。

The `is-ipv6(2001:DB8::)` 関数は `True` を返します。

startswith() 関数

The `startswith()` 関数は、文字列が指定されたプレフィックスで始まるかどうかを判断します。この関数には、2つの必須文字列引数が必要です。

```
startswith(str, sub_str)
```

この関数は、文字列 (`str`) が部分文字列 (`sub_str`) で始まる場合に `True` を返します。

例:

- The `startswith('Citrix', 'Ci')` 関数は `True` を返します。
- The `startswith('Citrix', 'iC')` 関数は `False` を返します。
- The `startswith('Citrix', 'Ab')` 関数は `False` を返します。

endswith() 関数

`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)
```

文字列 (`str`) が部分文字列 (`sub_str`) で終わる場合、この関数は `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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンテインズ()

`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。この関数は、2つの必須文字列引数を必要とします。

許可される引数タイプ:

- `string`
- `number`
- `tcp-port`
- `boolean`
- `ipaddress`

`contains(str, sub_str)`

この関数は、文字列 (`str`) 内にサブストリング (`sub_str`) が含まれている場合に `True` を返します。

例:

- `contains('Citrix', 'tri')` 関数は `True` を返します。
- `contains('Citrix', 'Ci')` 関数は `True` を返します。
- `contains('Citrix', 'ti')` 関数は `False` を返します。

この関数を使用して、特定の項目がリストに属しているかどうかを確認することもできます。

例:

```
list_of_strings = [“Citrix”, “Core”, ”Values”, ”Integrity”]



contains($parameters.list_of_strings, “Values”)
```

この例では、リストに `Values` 項目が含まれているため、`contains()` 関数は `True` を返します。

substring() 関数

文字列からサブストリングを抽出するには、`substring()` 関数を使用します。

`substring(str, start_index, end_index)`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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` (任意)

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。

マッチ()

`match()` 関数は、入力文字列が定義された正規表現パターンと一致するかどうかをチェックします。この関数は、正規表現パターンと検索文字列を引数として受け入れます。オプションで、大文字と小文字を区別するパターンを無視するためにブール型を指定することもできます。

例：

- `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "A2_B2")` は `True` を返します。
- `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "a2_b2")` は `False` を返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "a2_B2", $parameters.ignore_case)` は `True` を返します。

sha256()

この関数を使用して、任意の文字列のSHA-256ハッシュを計算します。この関数は、任意の長さの文字列入力を受け入れ、固定長（64文字）のハッシュ文字列を返します。

例：

```
components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:

            name: sha256(lbserver-name)

            servicetype: SSL

            ipv46: 10.10.10.10
```

この例では、`lbserver-name` はNetScalerオブジェクト上でハッシュ文字列として表示されます。

この関数は、式を入力として受け入れることもできます。

例：

```
components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            name: sha256($parameters.lb-appname)

            servicetype: SSL

            ipv46: 10.10.10.10
```

リレート()

`relate()` 関数は、一連のリストから辞書オブジェクトのリストを形成します。

2つの引数を取ります。

引数1：キー名を表す文字列のリスト。

引数2：リストのリスト。各リストには、引数1の対応するキー名の値が含まれます。引数2の各リストは同じ長さである必要があります。引数2のリストの数は、引数1の文字列の数と等しくなければなりません。

例:

```
name: test_relate_3

description: "Hello World StyleBook."

namespace: com.citrix.adc.stylebooks

schema-version: "1.0"

version: "1.1"



import-stylebooks:

    -

        namespace: netscaler.nitro.config

        prefix: ns

        version: "10.5"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
    parameters:
-
    name: namesofservers
    description: "Provide the names of LB VServers"
    type: string[]
-
    name: listofips
    description: "Provide the list of IP Addresses"
    type: string[]
-
    name: list_of_keys
    type: string[]
    default:
    - "name"
    - "ip"


substitutions:
    list_of_values: [$parameters.namesofservers,$parameters.listofips]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    components:

    -

        name: svc-comp

        type: object

        properties:

        svcdetails: relate($parameters.list_of_keys,
$substitutions.list_of_values)



    -

        name: lb-comp

        type: ns::lbvserver

        repeat: $components.svc-comp.properties.svcdetails

        repeat-item: svcd

        properties:

            name: $svcd['name']

            servicetype: HTTP

            ipv46: $svcd['ip']

            port: 80
```

この例では：

- `parameters`セクションには、`name`と`ip`を持つ`list_of_keys`というリストがあります。
- `substitutions`セクションには、以下の2つのリストを持つ`list_of_values`というリストがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 仮想サーバー名のリスト (`string`)
- IPアドレスのリスト (`string`)。

`relate()` 組み込み関数は、 `list_of_keys` と `list_of_values` を引数として受け入れます。この関数は、各オブジェクトが最初のリストからの名前と2番目のリストからのIPアドレスを持つ辞書オブジェクトのリストを作成します。

以下の仮想サーバーのリストを提供する場合：

```
["lb1","lb2"]
```

および仮想サーバーIPアドレスのリストを次のように：

```
["1.1.1.1","2.2.3.3"]
```

`relate()` 関数は、以下のリストを返します。

```
[\{"name": "lb1", "ip": "1.1.1.1"},\{"name": "lb2", "ip": "2.2.3.3"}]
```

StyleBookは、 `components` セクションで、この辞書オブジェクトのリストを反復処理して、対応する仮想サーバーを作成します。

マルチプル()

`multiple()` 関数は2つの引数を取ります。

引数1： `number` 、 `string` 、 `boolean` 、 `ipaddress` 、 `tcp-port` 、または `password`

引数 2: `number`

`multiple(argument1, argument2)` 関数は、引数1の多くのコピーを含むリストを返します。コピーの数は、引数2に渡された数と同じです。

例:

- `multiple(10.10.10.10, 3)` 関数は `[10.10.10.10, 10.10.10.10, 10.10.10.10]` を返します。
- `multiple(8080, 4)` 関数は `[8080, 8080, 8080, 8080]` を返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リバース()

reverse()関数は、項目のリストを引数として受け取り、同じ項目を逆順に並べたリストを返します。

引数には、次の組み込み型のリストを指定できます。

- 文字列
- 数値
- IPアドレス
- IPネットワーク
- TCPポート
- ブール値
- パスワード
- オブジェクト
- ファイル
- 証明書ファイル
- キーファイル
- 証明書キー

例:

- reverse() は を返します。
- reverse() は を返します。
- reverse() は を返します。

依存関係の検出

StyleBook内のコンポーネントは、同じStyleBook内の他のコンポーネントのプロパティまたはセクションを参照できます。コンポーネントはそれ自体で完結したブロックであり、実行される順序と同じ順序で記述されているとは限りません。StyleBookコンパイラは、コンポーネントが記述されている順序をチェックし、論理的な順序で実行します。

例:

```
components:

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

      name: $components.lbvserver-comp.properties.name

      servicegroupname: $components.sg-comp.properties.servicegroupname

-
    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: HTTP
```

上記の例では、**lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp** の3つのコンポーネントが定義されています。このStyleBookを実行すると、`lbvserver-comp` が最初に作成されます。`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` もまだ作成されていない `sg-comp` に依存しているためです。その結果、コンパイラはコンポーネントが作成されるまでにその依存関係が解決されるようにコン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポーネントを並べ替え、この並べ替えられたコンポーネントのリストを実行します。上記のStyleBookの実行順序は、`lbvserver-comp`、`sg-comp`、および`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。これは、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、そ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します。コンパイラは、循環依存関係が存在する場合、それを特定して報告できます。

次の例は、コンポーネントの循環依存関係を示しています。

```
components:


  -


    name: lbvserver-comp


    type: ns::lbvserver


    properties:


      name: $components.lb-sg-binding-comp.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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

-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: sg-comp


    type: ns::servicegroup


    properties:


      servicegroupname: mysg


      servicetype: $components.lbvserver-comp.properties.servicetype
```

上記の例では、**lbvserver-comp**、**lb-sg-binding-comp**、および **sg-comp** の3つのコンポーネントがあります。`lbvserver-comp` コンポーネントは、`lb-sg-binding-comp`、`lb-sg-binding` コンポーネントに依存しています。そして、これらのコンポーネントは `sg-comp` に依存しています。`sg-comp` コンポーネントは `lbvserver-comp` に依存しています。ここでは、これらのコンポーネント間に依存関係の循環が形成されており、これは自動的に解決できません。その結果、このStyleBookは実行できません。StyleBookコンパイラはこれを検出し、StyleBookがNetScaler Consoleにインポートされるのを防ぎます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セキュリティ

NetScaler Consoleのセキュリティ機能は、アプリケーションのセキュリティ体制を可視化します。セキュリティメトリクスを監視し、セキュリティ違反を調査し、APIを保護し、Webアプリケーションファイアウォール（WAF）の学習と推奨事項を使用してセキュリティ構成を強化できます。

以下のトピックは、アプリケーションセキュリティの監視と管理に役立ちます。

- アプリケーションセキュリティダッシュボード
  - 統合セキュリティダッシュボード
- セキュリティ違反
  - アプリケーション概要
  - すべての違反
- APIセキュリティ
- WAF学習
- WAF推奨事項

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、検出されたアプリケーションのセキュリティメトリックの概要を提供します。このダッシュボードには、同期攻撃、スモールウィンドウ攻撃、DNSフラッド攻撃など、検出されたアプリケーションのセキュリティ攻撃情報が表示されます。

アプリケーションセキュリティダッシュボードでセキュリティメトリックを表示するには：

1. **Security > Security Dashboard**に移動します。
2. インスタンスリストからインスタンスの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次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。値は1から7の範囲です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

脅威インデックスは攻撃情報に基づいています。違反タイプ、攻撃カテゴリ、場所、クライアントの詳細などの攻撃関連情報は、アプリケーションに対する攻撃に関する洞察を提供します。違反情報は、違反または攻撃が発生した場合にのみNetScaler Consoleに送信されます。多くの侵害や脆弱性が高い脅威インデックス値につながります。

- **安全インデックス**。NetScalerインスタンスが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、どれだけ安全に構成されているかを示す1桁の評価システムです。アプリケーションのセキュリティリスクが低いほど、安全インデックスは高くなります。値は1から7の範囲です。

  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導入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アドレスを表示します。

2 - 脅威インデックススコア、発生した違反の合計、ブロックされた違反の合計などの詳細を表示します。

3 - 選択したインスタンスの仮想サーバーを表示します。

4 - クライアントに基づいたセキュリティ違反を表示します。各クライアントに対してApp Security Investigatorグラフが表示されます。各クライアントIPをクリックして結果を表示できます。

5 - マップビューと表形式ビューで違反を表示します。

6 - 違反の詳細を表示します。グラフにマウスポインターを合わせると、違反の種類、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ト違反の詳細をさらに表示したい場合は、**App Security Investigator**の**XSS**用に表示されているグラフをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

安全性インデックスの詳細

アプリケーションの脅威エクスポージャーを確認した後、そのアプリケーションにどのようなアプリケーションセキュリティ構成が設定されており、どのような構成が不足しているかを判断したいと考えるでしょう。この情報は、アプリケーションの安全性インデックスの概要をドリルダウンすることで取得できます。

安全性インデックスの概要では、以下のセキュリティ構成の有効性に関する情報が提供されます。

- **Application Firewall Configuration**。設定されていないシグネチャとセキュリティエンティティの数を示します。
- **NetScaler Console System Security**。設定されていないシステムセキュリティ設定の数を示します。

Safety Indexの詳細を表示するには、仮想サーバー/アプリケーションを選択し、**Safety Index**タブをクリックします。

詳細が表示されます。

1 - Application Firewall構成の詳細情報を表示します。

2 - システムセキュリティの詳細情報を表示します。各セキュリティグループをクリックすると、ステータスとCitrixの推奨事項に関する詳細が表示されます。

3 - セキュリティチェックとシグネチャ違反の概要を表示します。

仮想サーバーのsecurity insightを有効にし、**Security > Security violations**に移動することで、脅威環境の概要も表示できます。安全指数ユースケースの詳細については、security insightを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

統合セキュリティダッシュボード

統合セキュリティダッシュボードは、保護を設定し、分析を有効にし、アプリケーションに保護を展開できる単一ペインのダッシュボードです。このダッシュボードでは、さまざまなテンプレートオプションから選択し、単一のワークフローで構成プロセス全体を完了できます。開始するには、**セキュリティ > セキュリティダッシュボード**に移動し、**アプリケーションの管理**をクリックします。**アプリケーションの管理**ページでは、保護されたアプリケーションと保護されていないアプリケーションの詳細を表示できます。

注:

- 新規ユーザーの場合、またはStyleBooksを介して、あるいはNetScaler®インスタンスで直接保護を設定していない場合、**セキュリティ > セキュリティダッシュボード**をクリックすると、次のページが表示されます。

- 保護が必要な仮想サーバーの総数を表示できます。**開始**をクリックして、**保護されていないアプリケーション**の詳細を表示します。
- 保護を設定できる仮想サーバーの種類は、負荷分散とコンテンツスイッチングです。

保護されたアプリケーション

統合セキュリティダッシュボードを使用して保護を設定した後、詳細を表示できます。詳細については、「保護されていないアプリケーションの保護を設定する」を参照してください。

NetScalerインスタンスで直接、またはStyleBooksを介して保護をすでに設定している場合、**保護されたアプリケーション**タブで、**プロファイル**の下に**その他**とマークされたアプリケーションを表示できます。

保護されていないアプリケーションの保護を設定する

注:

ブロックリストでサポートされる構成エンティティ（ルール）の最大数は32です。

保護されていないアプリケーションタブで、アプリケーションを選択し、**アプリケーションの保護**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリケーションを保護するには、次のいずれかのオプションを選択できます。

- WAF推奨スキャナー - このオプションを使用すると、アプリケーションでスキャンを実行できます。スキャンの特定のパラメーターに基づいて、結果はアプリケーションの保護を提案します。これらの推奨事項を適用することを検討してください。
- 保護の選択とカスタマイズ - このオプションを使用すると、さまざまなテンプレートオプションから選択したり、保護をカスタマイズして展開したりできます。
  - **OWASP Top 10** - OWASPトップ10のセキュリティリスクに対する業界標準の保護を備えた事前定義されたテンプレートです。詳細については、`https://owasp.org/www-project-top-ten/`を参照してください。
  - **CVE保護** - 既知の脆弱性カテゴリに分類された事前設定されたシグネチャルールのリストからシグネチャセットを作成できます。シグネチャパターンが受信トラフィックと一致した場合に、ログまたはブロックアクションを設定するシグネチャを選択できます。ログメッセージには脆弱性の詳細が含まれます。
  - **カスタム保護** - 要件に基づいて保護を選択し、展開します。
- 既存の保護を選択 - このオプションは、既存のアプリケーションに展開されている保護を複製します。これらの同じ保護を別のアプリケーションに展開したい場合は、このオプションを選択して、そのまま別のアプリケーションに展開できます。このオプションをテンプレートとして選択し、保護を変更してから展開することもできます。

WAF推奨スキャナー

注：

- アプリケーションに対して一度に実行できるスキャンは1つだけです。同じアプリケーションまたは別のアプリケーションで新しいスキャンを開始するには、前のスキャンが完了するまで待つ必要があります。
- **履歴の表示**をクリックして、過去のスキャンの履歴とステータスを表示できます。また、**レポートの表示**をクリックして、後で推奨事項を適用することもできます。

前提条件：

- NetScalerインスタンスは、13.0 41.28以降（セキュリティチェック用）および13.0以降（シグネチャ用）である必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プレミアムライセンスが必要です。
- ロードバランシング仮想サーバーである必要があります。

WAF推奨スキャンを開始するには、以下の情報を提供する必要があります。

1. **スキャンパラメータ**の下：

   - **ドメイン名** – アプリケーションに関連付けられている、有効でアクセス可能なIPアドレスまたは公開されているドメイン名を指定します。例：`www.example.com`。
   - **HTTP/HTTPSプロトコル** – アプリケーションのプロトコルを選択します。
   - **トラフィックタイムアウト** – スキャン中の単一リクエストに対する待機時間（秒単位）。値は0より大きい必要があります。
   - **スキャン開始URL** – スキャンを開始するアプリケーションのホームページ。例：`https://www.example.com/home`。URLは有効なIPv4アドレスである必要があります。IPアドレスがプライベートである場合、プライベートIPアドレスがNetScaler Console管理IPからアクセス可能であることを確認する必要があります。
   - **ログインURL** – 認証のためにログインデータが送信されるURL。HTMLでは、このURLは一般的にアクションURLとして知られています。
   - **認証方法** – アプリケーションでサポートされている認証方法（フォームベースまたはヘッダーベース）を選択します。

     - フォームベース認証では、ログイン資格情報を含むフォームをログインURLに送信する必要があります。これらの資格情報は、フォームフィールドとその値の形式である必要があります。その後、アプリケーションはスキャン中にセッションを維持するために使用されるセッションクッキーを共有します。
     - ヘッダーベース認証では、ヘッダーセクションに認証ヘッダーとその値が必要です。認証ヘッダーは有効な値を持つ必要があり、スキャン中にセッションを維持するために使用されます。ヘッダーベースの場合、フォームフィールドは空のままにする必要があります。

   - **リクエストメソッド** – ログインURLにフォームデータを送信する際に使用されるHTTPメソッドを選択します。許可されるリクエストメソッドは、**POST**、**GET**、**PUT**です。
   - **フォームフィールド** – ログインURLに送信するフォームデータを指定します。フォームフィールドは、フォームベース認証を選択した場合にのみ必要です。キーと値のペアで指定する必要があります。ここで、**フィールド名**がキーで、**フィールド値**が値です。パスワードを含む、ログインに必要なすべてのフォームフィールドが正しく追加されていることを確認してください。値はデータベースに保存される前に暗号化されます。複数の

© 1997–2026 Citrix Systems, Inc. All rights reserved.

フォームフィールドを追加するには、**追加**をクリックします。例：**フィールド名** – ユーザー名、**フィールド値** – admin。

- **ログアウトURL** – アクセス後にセッションを終了するURLを指定します。例：`https://www.example.com/customer/logout`。

2. 「**スキャン設定**」の下で：

   - **チェックする脆弱性** – スキャナーが検出する脆弱性を選択します。現在、これはSQLインジェクションとクロスサイトスクリプティングの違反に対して行われます。デフォルトでは、すべての違反が選択されています。脆弱性を選択すると、これらの攻撃をアプリケーション上でシミュレートし、潜在的な脆弱性を報告します。本番環境ではない環境でこの検出を有効にすることをお勧めします。他のすべての脆弱性も、アプリケーション上でこれらの攻撃をシミュレートすることなく報告されます。
   - **応答サイズ制限** – 応答サイズの最大制限。指定された値を超える応答はスキャンされません。推奨される制限は10 MB (1000000バイト) です。
   - **リクエスト同時実行数** – Webアプリケーションに並行して送信されるリクエストの総数。

3. WAFスキャン設定の構成が完了しました。**スキャン開始**をクリックしてスキャンプロセスを開始し、進行状況が完了するまで待ちます。スキャンが完了したら、**レポートの表示**をクリックします。

   スキャンレポート(/en-us/netscaler-console-service/media/scan-result.png)

4. スキャン結果ページで、**推奨事項の確認**をクリックします。

   推奨事項の確認(/en-us/netscaler-console-service/media/review-recommendation.png)

5. 保護を確認するか、他の保護を編集/追加し、**展開**をクリックします。

   保護の展開(/en-us/netscaler-console-service/media/deploy-waf-protection.png)

   セキュリティチェックを正常に適用すると：

- バージョンに応じて、StyleBooksを介してNetScalerインスタンスに構成が適用されます。
  - NetScaler 13.0の場合、`unified-appsec-protection-130` StyleBookが使用されます。
  - NetScaler 13.1の場合、`unified-appsec-protection-131` StyleBookが使用されます。
  - NetScaler 14.1の場合、`unified-appsec-protection-141` StyleBookが使用されます。
- `Appfw`プロファイルはNetScaler上に作成され、`policylabel`を使用してアプリケーションにバインドされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 推奨される署名がすでに適用されている場合、署名はappfwプロファイルにバインドされます。

注

セキュリティチェックは、NetScaler 13.0 41.28以降のバージョンでサポートされています。

Applications > Configuration > Config Packsに移動して、デフォルトのStyleBookを介してWAFプロファイルと署名が適用されていることを確認できます。

保護を選択してカスタマイズする

OWASP TOP 10

1 - IPアドレス、仮想サーバータイプ、ライセンスタイプ、アプリケーションが構成されているインスタンスなど、アプリケーションに関する情報を提供します。

2 - 選択したテンプレートを表示します。選択に応じて名前を変更できます。

3 - 保護を表示します。一部の保護には追加情報が必要です。

4 - 詳細ログタイプを表示します。次のオプションを選択できます。

- **パターン**。違反パターンのみをログに記録します。
- **パターンペイロード**。違反パターンと150バイトの追加JSONペイロードをログに記録します。
- **パターン、ペイロード、ヘッダー**。違反パターン、150バイトの追加JSONペイロード、HTTPヘッダー情報をログに記録します。

5 - モニターモードを有効にできます。モニターモードを有効にすると、トラフィックはログに記録されるだけで、緩和策はアクティブになりません。

6 - 保護を追加できます。「**保護の追加**」をクリックし、追加する保護を確認します。

7 - 「テンプレートの変更」オプションを使用して、新しいテンプレートを選択できます。

8 - 保護を編集または削除できます。

9 - 選択した保護のアナリティクスを有効にします。このオプションはデフォルトで選択されています。設定された保護のアナリティクスは、「**セキュリティ > セキュリティ違反**」で表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

保護を設定したら、「**展開**」をクリックします。

CVE保護

CVE保護を展開するには、「**CVE保護の作成**」をクリックします。「**署名セットの作成**」ページで、リストから署名を選択してログまたはブロックアクションを設定し、「**保存**」をクリックします。

- 「**保存**」をクリックすると、設定ページに追加された署名を表示できます。
- 「**保護の追加**」をクリックして、アプリケーションに保護を追加することもできます。すべての保護を設定したら、「**展開**」をクリックします。

カスタム保護

要件に基づいて保護を展開するには、「**新しい保護の作成**」をクリックします。「**保護の追加**」ページで、展開する保護を選択し、「**保存**」をクリックします。

カスタム保護(/en-us/netscaler-console-service/media/custom-protection.png)

保存をクリックした後、構成ページで選択した保護を確認し、**展開**をクリックします。

既存の保護を選択する

あるアプリケーションから別のアプリケーションへ既存の保護を展開するには、リストから既存の保護を選択します。

既存の保護(/en-us/netscaler-console-service/media/select-existing-protection.png)

保護を選択すると、既存の保護が複製され、構成ページに表示されます。要件に基づいて変更し、**展開**をクリックできます。

アプリケーションの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、攻撃に対して劇的に脆弱になっています。NetScaler Consoleを使用すると、実用的な違反の詳細を視覚化して、アプリケーションを攻撃から保護できます。単一ペインのソリューションとして、**セキュリティ** > **セキュリティ違反**に移動します。

- WAFインサイトとボットインサイトの両方で関連付けられてい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。詳細については、統合セキュリティダッシュボードを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ネットワーク、ボット、WAF**などのカテゴリに基づいて、アプリケーションのセキュリティ違反にアクセスします。
- アプリケーションを保護するための是正措置を講じます。

セキュリティ違反ページには、次のオプションがあります。

- **アプリケーション概要** – 総違反数、WAFおよびボットの総違反数、国別の違反などを含むアプリケーションの概要を表示します。詳細については、アプリケーション概要を参照してください。
- **すべての違反** – アプリケーションの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。

セットアップ

違反を表示するには、以下を確認する必要があります。

- アプリケーションで保護を設定し、分析を有効にするには、まずこれを行います。詳細については、統合セキュリティダッシュボードを参照してください。

  StyleBookまたはNetScalerインスタンスで直接保護を設定している場合は、**WAFセキュリティ違反**と**ボットセキュリティ違反**を有効にする手順に従うことができます。

  a. **インフラストラクチャ > インスタンス > NetScaler**に移動し、インスタンスタイプを選択します。例: VPX。
  b. インスタンスを選択し、**アクションの選択**リストから**分析の構成**を選択します。
  c. 仮想サーバーを選択し、**セキュリティと分析を有効にする**をクリックします。
  d. 「**Enable Analytics**」ウィンドウで、「**WAF Security Violations**」と「**Bot Security Violations**」を選択し、「**OK**」をクリックします。

- Detailed Web Transaction Settingsを構成するには。
- 「**Metrics Collector**」が有効になっている場合。詳細については、Configure Intelligent App Analyticsを参照してください。

Webトランザクション設定を有効にする

1. 「**Settings > Analytics Settings**」に移動します。

   「**Analytics Settings**」ページが表示されます。
2. 「**Enable Features for Analytics**」をクリックします。
3. 「**Detailed Web Transaction Settings**」で、「**All**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**Ok**」をクリックします。

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、セキュリティインサイトとボットインサイトの両方に関連する脅威の詳細を完全に可視化したアプリケーションが表示されます。また、合計違反数、合計WAFおよびボット違反数、国別の違反数などの情報を表示できます。

「アプリケーションの概要」(/en-us/netscaler-console-service/media/app-overview1.png)

1 – 選択した期間の合計影響アプリケーション数、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つのカスタムまたは個別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 – 違反に基づいて情報を提供します。

違反カテゴリ

WAF	BOT
Cookieハイジャック	スクレーパー
コンテンツタイプXMLの推測	スクリーンショット作成者
バッファオーバーフロー	検索エンジン
コンテンツタイプ	サービスエージェント
Cookieの一貫性	サイトモニター
CSRFフォームタグ付け	スピードテスター
URL拒否	未分類
フォームフィールドの一貫性	ウイルススキャナー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
フィールド形式	脆弱性スキャナー
最大アップロード数	DeviceFP 待機時間超過
リファラーヘッダー	無効なDeviceFP
セーフコマース	無効なCAPTCHA応答
セーフオブジェクト	ツール
HTML SQLインジェクション	CAPTCHA試行回数超過
開始URL	有効なCAPTCHA応答
クロスサイトスクリプティング	CAPTCHAクライアントミュート
XML DoS	CAPTCHA待機時間超過
XMLフォーマット	リクエストサイズ制限超過
XML WSI	レート制限超過
XML SSL	ブロックリスト（IP、サブネット、ポリシー式）
XMLアタッチメント	許可リスト（IP、サブネット、ポリシー式）
XML SOAPフォルト	ゼロピクセルリクエスト
XML検証	送信元IP
その他	ホスト
IPレピュテーション	クローラー
HTTP DOS	フィードフェッチャー
TCPスモールウィンドウ	リンクチェッカー
シグネチャ違反	マーケティング
ファイルアップロードタイプ	位置情報

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
JSONクロスサイトスクリプティング	URL
JSON SQL	
JSON DOS	
コマンドインジェクション	
ブロックキーワード	
JSONブロックキーワード	
コマンドインジェクショングラマー	

WAF違反の詳細を表示

「**上位アプリケーション**」または「**すべて表示**」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-console-service/media/waf-details.png)

注:

カスタムアプリを選択した場合、「**セキュリティ概要**」ページで統合されたアプリケーションの詳細を表示できます。リストからアプリケーションを選択して、選択したアプリケーションの詳細を表示します。

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。「**WAF**」の下に、以下が表示されます。

- アプリケーションの合計違反数、脅威インデックススコア、安全インデックススコアを示すグラフビュー。

  WAFグラフ(/en-us/netscaler-console-service/media/waf-graph.png)

  「**詳細を表示**」をクリックすると、アプリケーションファイアウォールとNetScalerシステムセキュリティの設定詳細が表示されます。

  詳細を表示(/en-us/netscaler-console-service/media/sec-violations.gif)
- 種類、重大度、適用されたアクションに基づく違反。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAFグラフの詳細(/en-us/netscaler-console-service/media/waf-violation-graph.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。クライアントIPアドレスも表示できます。

必要に応じて詳細を表示できる検索テキストボックスも使用できます。検索ボックスをクリックすると、検索候補のリストが表示されます。

- アプリケーションに影響を与えた違反。**違反の詳細**で、影響を受けた違反の詳細を表示できます。

  注

  カスタムアプリの場合、すべてのアプリケーションに適用される違反が表示されます。リストから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に影響を与えた違反を表示できます。

  各違反をクリックして、次のような詳細を表示します。

  - **発生した事象** – 合計発生回数と最終発生日時を示します。
  - **イベントの詳細** – クライアントIP、違反タイプ、クライアントIP、場所などの他の違反詳細を示すジオマップを表示します。

ボット違反の詳細を表示

ボットタブから、**上位アプリケーション**または**すべて表示**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。

注

カスタムアプリを選択した場合、統合されたアプリケーションの詳細を**セキュリティ概要**ページで表示できます。リストからアプリケーションを選択して、選択したアプリケーションの詳細を表示します。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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、良好なボットの総数、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-console-service/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-console-service/media/bot-violations-types.png)

  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するには、**ログ**をクリックします。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良好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-console-service/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。

  N/Aタイプ(/en-us/netscaler-console-service/media/na-log-bot.png)
  検索テキストボックスを使用して、要件に応じてボットの詳細を表示することもできます。検索ボックスをクリックすると、検索ボックスに検索候補のリストが表示されます。

- 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。

  注:

  カスタムアプリの場合、すべてのアプリケーションに適用される違反が表示されます。リストから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に影響を与えた違反を表示できます。

  各違反をクリックして、次のような詳細を表示します。

  - **何が起こったか** – 総発生回数と最終発生日時を示します。
  - **イベント詳細** – クライアントIPや、違反タイプ、クライアントIP、場所などの違反詳細を示すジオマップを表示します。

    ボット違反の詳細(/en-us/netscaler-console-service/media/bot-violation-details.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

WAFと**Bot**の下で、ロードバランシング仮想サーバーにバインドされているコンテンツスイッチング仮想サーバーの分析を表示できます。コンテンツスイッチング仮想サーバーをクリックし、**バインドされたロードバランシングサーバー**の下で、コンテンツスイッチング仮想サーバーにバインドされているロードバランシングサーバーのリストを表示できます。

ロードバランシングサーバーを持つコンテンツスイッチングサーバー(/en-us/netscaler-console-service/media/cs-lb-analytics.png)

イベント履歴の表示

以下の状況で、**イベント**で署名更新を表示できます。

- NetScalerインスタンスに新しい署名が追加された場合。
- NetScalerインスタンスで既存の署名が更新された場合。

署名の自動更新

NetScaler Consoleは、新しい署名更新を自動的にチェックし、管理対象のNetScalerインスタンスに適用します。

次の図は、署名がAWSクラウドから取得され、NetScalerで更新され、NetScaler Consoleで署名更新の概要が表示される方法を示しています。

イベントスケジューラ(/en-us/netscaler-console-service/media/bot-events1.png)

すべての違反

「**すべての違反**」ページには、**ネットワーク**、**WAF**、**ボット**のカテゴリに基づいて、アプリケーションセキュリティ違反の詳細が表示されます。NetScaler Consoleでセキュリティ違反を表示するには、必要なすべての設定を有効にしてください。詳細については、「設定」で利用可能な手順を参照してください。

違反カテゴリ

NetScaler Consoleでは、以下の違反を表示できます。「**違反の詳細**」で、各違反タブをクリックすると、違反の詳細を表示できます。

ネットワーク	WAF	ボット
HTTPスローロリス	コンテンツタイプXMLの推測	スクレイパー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワーク	WAF	ボット
DNSスローロリス	バッファオーバーフロー	スクリーンショット作成者
HTTPスローポスト	コンテンツタイプ	検索エンジン
NXDomainフラッド攻撃	Cookieの一貫性	サービスエージェント
HTTPデシンク攻撃	CSRFフォームタグ付け	サイトモニター
ブライヒェンバッハー攻撃	URL拒否	スピードテスター
セグメントスマック攻撃	フォームフィールドの一貫性	ツール
SYNフラッド攻撃	フィールド形式	未分類
スモールウィンドウ攻撃	リファラーヘッダー	ウイルススキャナー
	クロスサイトスクリプティング	脆弱性スキャナー
	XML DoS	DeviceFP待機時間超過
	XML形式	無効なDeviceFP
	XML WSI	無効なCAPTCHA応答
	XML SSL	CAPTCHA試行回数超過
	XML添付ファイル	有効なCaptcha応答
	XML SOAP障害	Captchaクライアントミュート
	XML検証	Captcha待機時間超過
	その他	リクエストサイズ制限超過
	IPレピュテーション	レート制限超過
	HTTP DOS	ブロックリスト (IP、サブネット、ポリシー式)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットワーク	WAF	ボット
	TCPスモールウィンドウ	許可リスト (IP、サブネット、ポリシー式)
	シグネチャ違反	ゼロピクセルリクエスト
	ファイルアップロードタイプ	送信元IP
	JSONクロスサイトスクリプティング	ホスト
	JSON SQL	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
	クッキーハイジャック	フィードフェッチャー
	ブロックキーワード	リンクチェッカー
	JSONブロックキーワード	マーケティング
	セーフコマース	
	セーフオブジェクト	
	HTML SQLインジェクション	
	開始URL	
	コマンドインジェクショングラマー	
	JSON SQLインジェクショングラマー	

セキュリティ違反ダッシュボード

セキュリティ違反ダッシュボードでは、以下を表示できます。

- すべてのNetScalerインスタンスとアプリケーションで発生した合計違反数。合計違反数は、選択した期間に基づいて表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 各カテゴリの合計違反数。

- 影響を受けたNetScalerインスタンスの合計数、影響を受けたアプリケーションの合計数、および合計発生数と影響を受けたアプリケーションに基づく上位の違反。

違反の詳細

各違反について、NetScaler Consoleは特定の期間の動作を監視し、異常な動作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。

- 合計発生回数、最終発生日時、および影響を受けるアプリケーションの合計数
- イベントの詳細では、次の情報を表示できます。
  - 影響を受けるアプリケーション。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。
  - 違反を示すグラフ。
  - 問題のトラブルシューティングを提案する**推奨されるアクション**。
  - 違反発生時刻や検出メッセージなど、その他の違反の詳細。

WAF学習

NetScaler Web App Firewall (WAF) は、SQLインジェクションやクロスサイトスクリプティングなどの悪意のある攻撃からWebアプリケーションを保護します。データ侵害を防ぎ、適切なセキュリティ保護を提供するには、脅威や攻撃に関するリアルタイムで実用的なデータをトラフィックで監視する必要があります。報告された攻撃が誤検知である場合があり、それらは例外として提供する必要があります。

NetScaler Console の学習エンジンは、WAF が Web アプリケーションの動作 (通常の活動) を学習できるようにする反復パターンフィルターです。監視に基づいて、エンジンは HTTP トラフィックに適用される各セキュリティチェックに対して、推奨されるルールまたは例外のリストを生成します。

学習エンジンを使用すると、必要な緩和策として手動で展開するよりも、緩和ルールを展開する方がはるかに簡単です。

次の図は、NetScaler Console での WAF 学習の仕組みに関する概要情報を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1 – WAFプロファイルを持つNetScalerインスタンス

2 – NetScaler Console で学習プロファイルを構成し、WAF プロファイルを追加して、緩和ルールを自動展開するか手動展開するかを選択します

3 – 管理者は NetScaler Console で緩和ルールを検証し、展開するかスキップするかを決定できます

はじめに

学習機能を展開するには、次の操作を行う必要があります。

- NetScalerインスタンスで集中学習を有効にします。NetScalerインスタンスで次のコマンドを実行します。

  ```
  set appfw settings -centralizedLearning ON
  ```

- NetScalerインスタンスのバージョンが**13.0-76.6**以降であることを確認してください。
- NetScalerアプライアンスでWeb App Firewallプロファイル（セキュリティ設定のセット）を構成します。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。

集中学習を有効にし、WAFプロファイルを構成すると、NetScaler Consoleは構成されたセキュリティチェックの例外（緩和）リストを生成します。管理者として、NetScaler Consoleで例外リストを確認し、展開するかスキップするかを決定できます。

NetScaler ConsoleのWAF学習機能を使用すると、次のことができます。

- 以下のセキュリティチェックで学習プロファイルを構成します。
  - 開始URL
  - Cookieの一貫性
  - クレジットカード

    注

    クレジットカードセキュリティチェックの場合、NetScalerインスタンスで`doSecureCreditCardLogging`を構成し、設定が**OFF**であることを確認する必要があります。

  - コンテンツタイプ
  - フォームフィールドの一貫性

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- フィールド形式
- CSRFフォームタグ付け
- HTMLクロスサイトスクリプティング
- HTML SQLインジェクション

  注

  HTML SQLインジェクションチェックの場合、NetScalerインスタンスで`set -sqlinjectionTransformSpecialChars ON`と`set -sqlinjectiontype sqlspclcharorkeywords`を構成する必要があります。

- HTMLコマンドインジェクション

  注

  NetScalerインスタンス13.0-72.12以降でのみサポートされています。

- JSON SQL

  注

  NetScalerインスタンス13.1-14.10以降でのみサポートされています。

- JSONコマンドインジェクション

  注

  NetScalerインスタンス13.1-14.10以降でのみサポートされています。

- JSON XSS

  注

  NetScalerインスタンス13.1-14.10以降でのみサポートされています。

- NetScaler Consoleで緩和ルールを確認し、必要なアクション (展開またはスキップ) を決定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- メール、Slack、ServiceNowを介して通知を受け取ります。
- **アクションサマリー**ページを使用して、緩和の詳細を表示します

NetScaler ConsoleでWAF学習を使用するには：

1. 学習プロファイルを設定する
2. 緩和ルールを管理する
3. WAF学習アクションサマリーページを使用する

WAFの推奨事項

NetScaler Web App Firewall (WAF) プロファイルとWAFシグネチャは、悪意のある攻撃からWebアプリケーションを保護します。WAFシグネチャは、既知の攻撃からWebサイトを保護するタスクを簡素化するための、特定の構成可能なルールを提供します。シグネチャは、オペレーティングシステム、Webサーバー、Webサイト、XMLベースのWebサービス、またはその他のリソースに対する既知の攻撃のコンポーネントであるパターンを表します。シグネチャを使用してアプリケーションを保護するには、適用したいルールを確認し、有効にして構成する必要があります。

同様に、データ侵害を防ぎ、アプリケーションに適切なセキュリティ保護を提供するには、セキュリティチェックを含むWAFプロファイルを作成する必要があります。NetScalerインスタンスでWAFプロファイルを作成すると、トラフィックは次のようになる可能性があります。

- 記載されているセキュリティチェックで生成される
- 記載されているセキュリティチェックで生成されない

インスタンスは他の攻撃を受けている可能性がありますが、WAFプロファイルでそのセキュリティチェックを有効にしていない可能性があります。

管理者として、Webアプリケーションを保護するために適切なシグネチャを有効にし、適切なWAFプロファイルを作成する方法を理解する必要があります。適切なシグネチャとWAFプロファイルを特定することは、一部のシナリオでは困難な作業となる場合があります。

NetScaler Console WAFレコメンデーションは、アプリケーションの脆弱性をスキャンし、次の推奨事項を生成します。

- WAFプロファイル
- WAFシグネチャ

詳細については、WAFプロファイル および WAFシグネチャ を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAFレコメンデーションデータベースは、新しい脆弱性を含めるために頻繁に更新されます。スキャンして、必要な推奨事項を有効にすることを選択できます。すべてのシグネチャとセキュリティチェックを有効にすることはできますが、誤検知が発生し、NetScalerインスタンスのパフォーマンスに影響を与える可能性があります。したがって、必要なセキュリティチェックとシグネチャのみを選択することをお勧めします。WAFレコメンデーションエンジンは、アプリケーションに対してどのシグネチャとセキュリティチェックを有効にする必要があるかも自動的に検出します。

注

NetScalerインスタンスは、セキュリティチェックの場合は **13.0 41.28以降**、シグネチャの場合は **13.0以降** である必要があります。

前提条件

アプリケーションは次のとおりです。

- プレミアムライセンスが必要です。
- ロードバランシング仮想サーバーである必要があります。

WAFスキャン設定を構成する

NetScaler Consoleで、**Security > WAF Recommendation** に移動し、**Applications** の下にある **Start Scan** をクリックして、アプリケーションのWAFスキャン設定を構成します。

WAFスキャン(/en-us/netscaler-console-service/media/waf-scan.png)

WAFレコメンデーションページで：

- **ドメイン名** – アプリケーションVIPに関連付けられている、公開アクセス可能/公開到達可能なドメイン名を指定します。例：`www.example.com`。

  注

  開始URL、ログインURL、ログアウトURLは、指定されたドメインと一致する必要があります。

- **トラフィックと開始URL** – アプリケーション（サーバー）のURL詳細を指定します。
  - **HTTP/HTTPSプロトコル** – アプリケーションのプロトコルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **トラフィックタイムアウト** – スキャン中の単一リクエストの待機時間（秒単位）。値は0より大きい必要があります。
- **開始URL** – スキャンを開始するアプリケーションのホームページ。例：`https://www.example.com/home`。URLは有効なIPv4アドレスである必要があります。IPアドレスがプライベートである場合、プライベートIPアドレスがNetScaler Console管理IPからアクセス可能であることを確認する必要があります。

  WAF構成(/en-us/netscaler-console-service/media/wre-configure-traffic.png)

- **ログインURL** – アプリケーションにアクセスするためのログイン資格情報、URL（もしあれば）を指定します。
  - **ログインURL** – 認証のためにログインデータが送信されるURL。HTMLでは、このURLは一般的にアクションURLとして知られています。
  - **認証方法** – アプリケーションでサポートされている認証方法（フォームベースまたはヘッダーベース）を選択します。
    - フォームベース認証では、ログイン資格情報とともにフォームをログインURLに送信する必要があります。これらの資格情報は、フォームフィールドとその値の形式である必要があります。その後、アプリケーションはスキャン中にセッションを維持するために使用されるセッションクッキーを共有します。
    - ヘッダーベース認証では、ヘッダーセクションに認証ヘッダーとその値が必要です。認証ヘッダーは有効な値を持つ必要があり、スキャン中にセッションを維持するために使用されます。ヘッダーベースの場合、フォームフィールドは空のままにする必要があります。
  - **リクエストメソッド** – ログインURLにフォームデータを送信する際に使用されるHTTPメソッドを選択します。許可されるリクエストメソッドはPOST、GET、PUTです。
  - **フォームフィールド** – ログインURLに送信するフォームデータを指定します。フォームフィールドは、フォームベース認証を選択した場合にのみ必要です。キーと値のペアで指定する必要があります。ここで、フィールド名がキー、フィールド値が値です。パスワードを含め、ログインが機能するために必要なすべてのフォームフィールドが正しく追加されていることを確認してください。値はデータベースに保存される前に暗号化されます。「追加」ボタンをクリックして、複数のフォームフィールドを追加できます。例：フィールド名 – ユーザー名、フィールド値 – admin。
  - **HTTPヘッダー** – ログインを成功させるためにHTTPヘッダーが必要になる場合があります。キーと値のペアで指定する必要があります。ここで、ヘッダー名がキー、ヘッダー値

© 1997–2026 Citrix Systems, Inc. All rights reserved.

が値です。「追加」ボタンをクリックして、複数のHTTPヘッダーを追加できます。最も一般的な必須HTTPヘッダーの1つはContent-Typeヘッダーです。

- **ログアウトURL** – アクセス後にセッションを終了するURLを指定します。例: `https://www.example.com/customer/logout`。

- **脆弱性** – スキャナーが検出する脆弱性を選択します。現在、これはSQLインジェクションとクロスサイトスクリプティングの違反に対して行われます。デフォルトでは、すべての違反が選択されています。脆弱性を選択した後、アプリケーションに対してこれらの攻撃をシミュレートし、潜在的な脆弱性を報告します。本番環境ではない環境でこの検出を有効にすることをお勧めします。他のすべての脆弱性も、アプリケーションに対してこれらの攻撃をシミュレートすることなく報告されます。

- **追加設定**
  - **リクエストの同時実行数** – Webアプリケーションに並行して送信されるリクエストの総数。
  - **スキャン深度** - スキャンが実行されるWebアプリケーションの深さ。たとえば、スキャン深度が2の場合、開始URLとこのURLで見つかったすべてのリンクがスキャンされます。1以上の値を指定する必要があります。
  - **応答サイズ制限** – 応答サイズの最大制限。指定された値を超える応答はスキャンされません。推奨される制限は3 MB (300000バイト) です。

WAFスキャン設定の構成が完了しました。スキャンプロセスを開始するには、**スキャン**をクリックするか、設定を保存して後でスキャンするには、**後で保存**をクリックします。

WAFスキャン推奨プロセス

スキャンを開始すると、WAF推奨エンジンは次の処理を行います。

- 提供されたURLを介して、提供されたWebアプリケーションをスキャンします。
- Webアプリケーションを検査して、Webアプリケーションで使用されているテクノロジーを検出します。
- Webアプリケーションに対するセキュリティ攻撃をシミュレートして、潜在的な脆弱性を検出します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 検出されたWebテクノロジーに基づいてシグネチャを推奨します。
- 発見された脆弱性とトラフィックの分析に基づいてセキュリティチェックを推奨します。
- Webアプリケーションの応答を分析して、より詳細な設定を生成します。

次のセキュリティチェックがサポートされています。

- バッファオーバーフロー
- フィールド形式
- クレジットカード
- Cookieの一貫性
- HTML SQLインジェクション
- HTMLクロスサイトスクリプティング
- フォームフィールドの一貫性
- CSRFフォームタグ付け

スキャンレポートの表示

スキャンが完了したら、**レポートの表示**をクリックして結果を表示します。

スキャン結果には以下が含まれます。

- **WAFレコメンデーション** – アプリケーションに推奨される署名とセキュリティチェックの合計の概要を表示できます。
- **スキャン検出** – アプリケーションで実行されたテクノロジーや違反の詳細などの情報のコレクションを表示できます。**詳細の表示**をクリックすると、検出に関する情報やスキャンのその他の詳細が表示されます。

WAFレコメンデーションの下で、**レコメンデーションの確認**をクリックして、**セキュリティチェック**と**署名**の詳細を表示します。

推奨されるセキュリティ設定は、アプリケーションに推奨されるセキュリティチェックと署名を示します。リストから推奨事項を編集し、**表示または編集**をクリックして、要件に応じて詳細を表示したり変更を編集したりできます。「デフォルトにリセット」は、行われたすべての変更をリセットし、元の推奨事項に戻します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細を確認したら、**推奨事項を適用**をクリックします。推奨事項はStyleBooksを使用して構成されます。**セキュリティチェック**タブと**シグネチャ**タブで推奨事項を個別に適用するようにしてください。

WAFの結果(/en-us/netscaler-console-service/media/wre-results.png)

まずシグネチャを適用し、次にセキュリティチェックを適用することをお勧めします。これにより、シグネチャがプロファイルに自動的にバインドされます。

シグネチャを正常に適用すると、次のようになります。

- 設定は、`appfw-import-object` StyleBookを介してNetScalerインスタンスに適用されます。
- 推奨事項が構成されたシグネチャファイルがNetScalerインスタンスにインポートされます。

注

シグネチャはNetScaler 13.0以降のバージョンでサポートされています。

セキュリティチェックの推奨事項を適用する前に、**Applications > Configuration > Config Packs**に移動し、シグネチャのconfigpackが正常に作成されていることを確認してください。

セキュリティチェックを正常に適用すると、次のようになります。

- 設定は、NetScalerのバージョンに応じて、StyleBooksを介してNetScalerインスタンスに適用されます。NetScaler 13.0では`waf-default-130` StyleBookが使用され、NetScaler 13.1では`waf-default-131` stylebookが使用されます。
- `Appfw` プロファイルはNetScaler上に作成され、`policylabel` を使用してアプリケーションにバインドされます。
- 推奨されるシグネチャがすでに適用されている場合、シグネチャはappfwプロファイルにバインドされます。

注

セキュリティチェックはNetScaler 13.0 41.28以降のバージョンでサポートされています。

推奨事項 (セキュリティチェックとシグネチャ) を適用した後、次の確認メッセージを表示できます。

WAFの確認(/en-us/netscaler-console-service/media/wre-confirmation.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications > Configuration > Config Packs に移動して、デフォルトのStyleBookを介してWAFプロファイルとシグネチャが適用されていることを確認できます。

WAF StyleBook(/en-us/netscaler-console-service/media/wre-stylebooks.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ゲートウェイ

NetScaler Consoleのゲートウェイ機能は、NetScaler Gatewayの展開全体でユーザーアクセスと仮想デスクトップエクスペリエンスの可視性を提供します。ログオンとアクセス障害のトラブルシューティング、HDX™仮想デスクトップエクスペリエンスの監視、しきい値とアラートの設定を行うことができます。

以下のトピックは、ゲートウェイ分析の監視と管理に役立ちます。

- ゲートウェイインサイト
  - Gateway Insightの問題のトラブルシューティング
- HDXインサイト
  - HDX Insightデータ収集の有効化
  - HDX Insightのしきい値の作成とアラートの設定
  - HDX Insightレポートとメトリックの表示
  - HDX Insightの問題のトラブルシューティング
- しきい値のメトリック情報

ゲートウェイインサイト

NetScaler Gatewayの展開において、ユーザーアクセス詳細の可視性は、アクセス障害のトラブルシューティングに不可欠です。ネットワーク管理者として、ユーザーがNetScaler Gatewayにログオンできない場合や、ユーザーアクティビティ、ログオン失敗の理由を知りたいと思うでしょう。しかし、通常、ユーザーが解決を要求しない限り、その情報は利用できません。

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、および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を表示できます。ユーザーのエンドポイント分析 (EPA)、認証、シングルサインオン (SSO)、およびアプリケーション起動の失敗を表示できます。また、ユーザーのアクティブセッションと終了したセッションの詳細も表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway Insightは、仮想アプリケーションのアプリケーション起動失敗の理由も可視化します。これにより、あらゆる種類のログオンまたはアプリケーション起動の失敗問題のトラブルシューティング能力が向上します。起動されたアプリケーションの数、合計およびアクティブなセッションの数、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の数を表示できます。アプリケーションのユーザー、セッション、帯域幅、および起動エラーの詳細を表示できます。

任意の時点で、NetScaler Gatewayアプライアンスに関連付けられているすべてのゲートウェイが使用し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、および帯域幅を表示できます。ゲートウェイのエンドポイント分析 (EPA)、認証、シングルサインオン、およびアプリケーション起動の失敗を表示できます。また、ゲートウェイに関連付けられているすべてのユーザーとそのログオンアクティビティの詳細も表示できます。

すべてのログメッセージはNetScaler Consoleデータベースに保存されるため、任意の期間のエラー詳細を表示できます。また、ログオン失敗の概要を表示し、ログオンプロセスのどの段階で失敗が発生したかを特定することもできます。

注意点:

- Gateway Insightは、以下の展開でサポートされています。
  - アクセスゲートウェイ
  - 統合ゲートウェイ
- NetScaler Consoleのリリースとビルドは、NetScaler Gatewayアプライアンスのリリースとビルドと同じか、それ以降である必要があります。
- Advancedライセンスを持つNetScalerインスタンスでは、1時間分のGateway Insightレポートを表示できます。1時間を超えるGateway Insightレポートを表示するには、Premiumライセンスが必要です。

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。
- 仮想ICAアプリケーションおよびデスクトップの成功したユーザーログオン、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にあるNetScaler Gatewayアプライアンスでの障害に関する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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SAML認証のGateway Insightレコードは報告されません。
- 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を使用した場合、Gateway Insightに矛盾が生じる可能性があります。
  - ローカル
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - ネイティブOTP
  - オーオース

Gateway Insightを有効にする

NetScaler GatewayアプライアンスでGateway Insightを有効にするには、まずNetScaler Gatewayアプライアンスを NetScaler Consoleに追加する必要があります。次に、VPNアプリケーションを表す仮想サーバーでAppFlowを有効にする必要があります。NetScaler Consoleへのデバイスの追加については、「インスタンスの追加」を参照してください。

注

NetScaler Consoleでエンドポイント分析 (EPA) の障害を表示するには、NetScaler Gatewayアプライアンスで AppFlow認証、承認、およびアクセス制御ユーザー名のログ記録を有効にする必要があります。

NetScaler Consoleで仮想サーバーのAppFlowを有効にする

1. **設定 > ライセンスと分析の構成** に移動します。
2. **Virtual Server Analytics Summary** で、**Configure Analytics** をクリックします。
3. **All Virtual Servers** ページで、NetScaler Gateway仮想サーバーを選択し、**Enable Security & Analytics** をクリックします。
4. **Gateway Insight** を選択します。
5. **Save** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUIを使用してNetScaler GatewayアプライアンスでAppFlowユーザー名ログ記録を有効にする

1. **Configuration > System > AppFlow® > Settings** に移動し、**Change AppFlow Settings** をクリックします。
2. **Configure AppFlow Settings** 画面で、**AAA Username** を選択し、**OK** をクリックします。

Gateway Insightレポートの表示

NetScaler Consoleでは、NetScaler Gatewayアプライアンスに関連付けられているすべてのユーザー、アプリケーション、およびゲートウェイのレポートを表示でき、特定のユーザー、アプリケーション、またはゲートウェイの詳細を表示できます。**Overview** セクションでは、EPA、SSO、認証、およびアプリケーション起動の失敗を表示できます。また、ユーザーがログオン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。

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 Consoleアナリティクスは、仮想IPアドレスベースの承認をサポートするようになりました。ユーザーは、承認されているアプリケーション（仮想サーバー）のみのすべてのインサイトのレポートを表示できるようになりました。グループとグループへのユーザーの割り当ての詳細については、「NetScaler Consoleでグループを構成する」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

1. NetScaler Consoleで、**Gateway > Gateway Insight** に移動します。
2. ユーザーの詳細を表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。「**Go**」をクリックします。
3. 失敗の詳細を表示するには、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ます。

   EPAレポート(/en-us/netscaler-console-service/media/gateway-insight-reports-failure.png)

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

NetScaler Consoleで、**Gateway > Gateway Insight**に移動し、下にスクロールしてレポートを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レポートの概要(/en-us/netscaler-console-service/media/gateway-insight-reports-summary.png)

ログオンアクティビティ(/en-us/netscaler-console-service/media/gateway-insight-reports-logon-activity.png)

ユーザー

NetScaler Gatewayアプライアンスに関連付けられているユーザーの完全なレポートを表示できます。ユーザーのEPA、認証、SSO、アプリケーション起動の失敗などを表示できます。

すべてのユーザーのアクティブセッションと終了セッションの統合ビューを視覚化することもできます。

Gateway Insightの改善点(/en-us/netscaler-console-service/media/gateway-insight-improvements.png)

管理者として、このビューを使用すると、次のことができます。

- すべてのユーザーの詳細を単一ペインの視覚化で表示
- 各ユーザーを選択してアクティブセッションと終了セッションを確認する複雑さを排除

ユーザーの詳細を表示

1. NetScaler Console で、**Gateway > Gateway Insight > Users** に移動します。
2. ユーザーの詳細を表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。**Go** をクリックします。
3. その期間中のアクティブユーザー数、アクティブセッション数、および全ユーザーによるバイト数を表示できます。

   Gateway Insight の現在(/en-us/netscaler-console-service/media/gw-now.png)

下にスクロールして、利用可能なユーザーとアクティブユーザーのリストを表示します。

アクティブユーザー(/en-us/netscaler-console-service/media/gateway-insight-reports-active-users.png)

Users または **Active Users** タブでユーザーをクリックすると、次のユーザー詳細が表示されます。

- **ユーザー詳細** - NetScaler Gateway アプライアンスに関連付けられている各ユーザーのインサイトを表示できます。**Gateway** > **Gateway Insight** > **Users** に移動し、ユーザーをクリックす

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ると、セッションモード、オペレーティングシステム、ブラウザなど、選択したユーザーのインサイトが表示されます。

ユーザー詳細(/en-us/netscaler-console-service/media/gw-user-details.png)

- **選択したゲートウェイのユーザーとアプリケーション** - **Gateway** > **Gateway Insight** > **Gateway** に移動し、ゲートウェイドメイン名をクリックすると、選択したゲートウェイに関連付けられている上位10のアプリケーションと上位10のユーザーが表示されます。

  ユーザーとアプリケーション(/en-us/netscaler-console-service/media/gw-user-app.png)

- **アプリケーションとユーザーのその他のオプションを表示** – 10を超えるアプリケーションとユーザーの場合、Applications and Users のその他アイコンをクリックすると、選択したゲートウェイに関連付けられているすべてのユーザーとアプリケーションの詳細が表示されます。
- **棒グラフをクリックして詳細を表示** – 棒グラフをクリックすると、関連する詳細を表示できます。たとえば、**Gateway > Gateway Insight > Gateway** に移動し、ゲートウェイの棒グラフをクリックすると、ゲートウェイの詳細が表示されます。

  棒グラフ(/en-us/netscaler-console-service/media/bar-graph.png)

- ユーザーの**アクティブセッション**と**終了セッション**。

  ▢

- **アクティブセッション**におけるゲートウェイドメイン名とゲートウェイIPアドレス。

  ▢

- ユーザーのログイン期間。

  ▢

- ユーザーのログアウトセッションの理由。ログアウトの理由は次のとおりです。

  - セッションがタイムアウトしました
  - 内部エラーのためログアウトしました
  - 非アクティブセッションのタイムアウトのため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

  ▢

検索バーと地理マップビュー

以下を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザー名に基づいて結果をフィルタリングできる検索バー。**Gateway > Gateway Insight > Users** に移動して、**Users** と **Active Users** の検索バーを表示します。検索バーにマウスポインターを置き、**User Name** を選択し、ユーザー名を入力して結果をフィルタリングします。

  「検索バー」(/en-us/netscaler-console-service/media/search-bar-gw.png)

- ユーザーの地理的な場所に基づいてユーザー情報を表示するジオマップ。管理者として、このジオマップを使用すると、特定の場所の総ユーザー数、総アプリケーション数、総セッション数の概要を表示できます。

  a. ジオマップを表示するには、**Gateway > Gateway Insight** に移動します。

  b. 国をクリックします。たとえば、米国。

     ジオマップには、選択した国のユーザーリスト、アクティブなセッション、終了したセッション、アプリケーションなどの詳細が表示されます。

アプリケーション

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なセッション数、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確認できます。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

1. NetScaler Consoleで、**ゲートウェイ > ゲートウェイインサイト > アプリケーション** に移動します。
2. アプリケーション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。

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なセッション数、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。

「アプリレポート」(/en-us/netscaler-console-service/media/gateway-insight-reports-apps.png)

スクロールして、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します。

「その他のアプリ」(/en-us/netscaler-console-service/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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ゲートウェイ

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、そのログオンアクティビティも表示できます。

ゲートウェイの詳細を表示

1. NetScaler Console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。

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るようになりました。

☐
スクロールダウンして、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します。

☐
Gateway Domain Name 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。

特定の場所に基づいてユーザーをフィルタリングできるゲートウェイのジオマップも表示できます。

1. **Gateway > Gateway Insight > Gateways** に移動します
2. ジオマップを表示するには、ゲートウェイドメイン名を選択します
3. 国をクリックします。たとえば、米国

   ジオマップには、選択した国のユーザーリスト、アクティブセッション、終了したセッション、アプリケーションなどの詳細が表示されます。

レポートのエクスポート

GUIに表示されるすべての詳細を含むGateway Insightレポートを、PDF、JPEG、PNG、またはCSV形式でローカルコンピューターに保存できます。また、レポートのエクスポートを、指定されたメールアドレスにさまざまな間隔でスケジュールすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

- 読み取り専用アクセス権を持つユーザーは、レポートをエクスポートできません。
- 地理マップレポートは、NetScaler Consoleにインターネット接続がある場合にのみエクスポートされます。

レポートのエクスポート

1. **ダッシュボード**タブの右ペインで、**エクスポート**ボタンをクリックします。
2. **今すぐエクスポート**の下で、必要な形式を選択し、**エクスポート**をクリックします。

エクスポートをスケジュールするには:

1. **ダッシュボード**タブの右ペインで、**エクスポート**ボタンをクリックします。
2. **エクスポートのスケジュール**の下で、詳細を指定し、**スケジュール**をクリックします。

注

レポートをスケジュールする前に、**システム** > **通知** > **メール**に移動し、**追加**をクリックしてメールサーバー設定を構成します。

メールサーバーまたはメール配布リストを追加するには:

1. **構成**タブで、**システム** > **通知** > **メール**に移動します。
2. 右ペインで、**メールサーバー**を選択してメールサーバーを追加するか、**メール配信リスト**を選択してメール配信リストを作成します。
3. 詳細を指定し、**作成**をクリックします。

Gateway Insightダッシュボード全体をエクスポートするには：

1. **ダッシュボード**タブの右ペインで、**エクスポート**ボタンをクリックします。
2. **今すぐエクスポート**の下で、**PDF**形式を選択し、**エクスポート**をクリックします。

Gateway Insightのユースケース

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に関する可視性を得る方法を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ユーザーがNetScaler Gatewayアプライアンスまたは内部Webサーバーにログオンできない

あなたはNetScaler Gateway管理者としてNetScaler Consoleを通じてNetScaler Gatewayアプライアンスを監視しており、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 Consoleでは、ログインプロセスの以下の段階でユーザーログインエラーの詳細を表示できます。

- 認証
- エンドポイント分析 (EPA)
- シングルサインオン

NetScaler Consoleでは、特定のユーザーを検索し、そのユーザーのすべての詳細を表示できます。

ユーザーを検索するには：

NetScaler Consoleで、**Gateway > Gateway Insight**に移動し、**Search for Users**テキストボックスで、検索するユーザーを指定します。

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。2段階認証を設定している場合は、認証のプライマリ、セカンダリ、または両方の段階が失敗したかどうかを確認できます。

認証失敗の詳細を表示する

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. **Overview**セクションで、認証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. **Authentication**タブをクリックします。**Failures**グラフで、任意の時点での認証エラーの数を表示できます。

同じタブのテーブルから、**Username**、**Client IP Address**、**Error Time**、**Authentication type**、**Authentication Server IP Address**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**Error Description**列にはログオン失敗の理由が表示され、**State**列には2段階認証のどの段階で失敗が発生したかが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Username列のユーザーをクリックすると、そのユーザーの認証エラーやその他の詳細が表示されます。

設定オプションを使用して、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。

EPAの失敗

認証前または認証後の段階でのEPAの失敗を表示できます。

EPA失敗の詳細を表示する

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. 概要セクションで、EPAエラーを表示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. **EPA (End Point Analysis)** タブをクリックします。**Failures**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、エラー時間、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**エラーの説明**列にはEPA障害の理由が表示され、**ポリシー名**列には障害の原因となったポリシーが表示されます。

ユーザー名列のユーザーをクリックすると、そのユーザーのEPAエラーやその他の詳細が表示されます。

設定オプションを使用して、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。

注

「clientSecurity」式がVPNセッションポリシー規則として構成されている場合、NetScaler GatewayはEPA障害を報告しません。

SSO障害

NetScaler Gatewayアプライアンスを介してアプリケーションにアクセスするユーザーの、あらゆる段階でのすべてのSSO障害を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSO障害の詳細を表示

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. 概要セクションで、SSOエラーを表示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 (シングルサインオン)**」タブをクリックします。失敗グラフで、任意の時点でのSSOエラーの数を確認できます。

下にスクロールして、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、エラー説明、リソース名**など、各SSOエラーの詳細を表示します。

ユーザー名列のユーザーをクリックすると、そのユーザーのSSOエラーやその他の詳細が表示されます。

設定オプションを使用して、テーブルの列を追加または削除できます。

2. NetScaler Gatewayに正常にログオンした後、ユーザーは仮想アプリケーションを起動できません

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、その理由を把握できます。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

1. NetScaler Consoleで、**Gateway > Gateway Insight**に移動します。
2. **概要**セクションで、SSOエラーを表示したい期間を選択します。タイムスライダーを使用して、選択した期間をさらにカスタマイズできます。**Go**をクリックします。
3. 「**アプリケーション起動**」タブをクリックします。**失敗**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。

下にスクロールして、同じタブのテーブルから、**NetScaler IPアドレス、エラー時刻、エラー説明、リソース名、Gatewayドメイン名**など、各アプリケーション起動エラーの詳細を表示します。テーブルの**エラー説明**列にはSTAサーバーのIPアドレスが表示され、**リソース名**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。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「設定」オプションを使用して、列の追加または削除を行うことで、テーブルをカスタマイズできます。

起動失敗3の画像(/en-us/netscaler-console-service/media/use-cases-app-launch-failure-errors.png)

3. 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が消費した合計バイト数と帯域幅を表示したいと考えています

新しいアプリケーションを正常に起動した後、NetScaler Consoleで、そのアプリケーションが消費した合計バイト数と帯域幅を表示できます。

アプリケーションが消費した合計バイト数と帯域幅を表示する

NetScaler Consoleで、**Gateway > Gateway Insight > Applications** に移動し、下にスクロールして、**Other Applications** タブで詳細を表示したいアプリケーションをクリックします。

帯域幅の画像(/en-us/netscaler-console-service/media/use-cases-bytes-bandwidth-consumed.png)

そのアプリケーションが消費したセッション数と合計バイト数を表示できます。

消費された帯域幅の画像(/en-us/netscaler-console-service/media/use-cases-bytes-consumed.png)

そのアプリケーションが消費した帯域幅も表示できます。

消費された帯域幅1の画像(/en-us/netscaler-console-service/media/use-cases-bandwidth-consumed.png)

4. 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一部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、障害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

1. NetScaler Consoleで、**ゲートウェイ > ゲートウェイインサイト > アプリケーション** に移動します。
2. 表示される画面で下にスクロールし、「**Other Applications**」タブで、ユーザーがログオンできなかったアプリケーションを選択します。

リソースアクセス(/en-us/netscaler-console-service/media/use-cases-resource-access.png)

表示される画面で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.

リソースアクセス1(/en-us/netscaler-console-service/media/use-cases-resource-access-users.png)

5. 異なるユーザーが異なるNetScaler Gateway展開を使用しているか、または異なるアクセスモードでNetScaler Gatewayにログオンしている可能性があります。管理者は、展開タイプとアクセスモードに関する詳細を表示できる必要があります

Gateway Insightを使用すると、ユーザーがログオンに使用したさまざまなセッションモード、クライアントの種類、および毎時ログオンしたユーザー数の概要を表示できます。ユーザーの展開が統合ゲートウェイ展開であるか、従来のNetScaler Gateway展開であるかを判断することもできます。統合ゲートウェイ展開の場合、コンテンツスイッチング仮想サーバー名とIPアドレス、およびVPN仮想サーバー名を表示できます。

セッションモード、クライアントの種類、およびログオンしたユーザー数の概要を表示

1. NetScaler Consoleで、**Gateway > Gateway Insight** に移動します。
2. 「**概要**」セクションで下にスクロールすると、「**セッションモード、オペレーティングシステム、ブラウザ**」および「**ユーザーログオンアクティビティ**」の各グラフに、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、および毎時ログオンしたユーザー数が表示されます。

セッション(/en-us/netscaler-console-service/media/use-cases-deployment-types-access-modes-summary.png)

セッション1(/en-us/netscaler-console-service/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 Console 間の接続の問題。
- NetScaler でのレコード生成。
- NetScaler Console での検証。

Gateway 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。

© 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
  ```

- 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。
- 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 Console 間の接続チェックリスト

- NetScaler で AppFlow コレクターのステータスを確認します。詳細については、「NetScaler と AppFlow コレクター間の接続ステータスを確認する方法」を参照してください。
- 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

- コマンド `nsconmsg -d stats -g ai_tot` を実行し、NetScaler で統計情報の増分を確認します。
- `nstrace` ログをキャプチャし、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。

NetScaler Console での検証

- コマンド `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` を実行してログを確認し、NetScaler Console が AppFlow レコードを受信していることを確認します。
- NetScaler インスタンスが NetScaler Console に追加されていることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway/VPN 仮想サーバーが NetScaler Console でライセンスされていることを確認します。

Gateway Insight の統計

以下の Gateway Insight 統計が利用可能です。

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled

Citrixテクニカルサポートに連絡する

迅速な解決のために、Citrixテクニカルサポートに連絡する前に、以下の情報を用意してください。

- 展開とネットワークトポロジの詳細。
- NetScaler および NetScaler Console のバージョン。
- NetScaler および NetScaler Console のテクニカルサポートバンドル。
- 問題発生時の `nstrace` キャプチャ。

既知の問題

Gateway Insight の既知の問題については、NetScaler リリースノートを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX™ インサイト

HDX Insightは、NetScalerを通過するCitrix Virtual Apps and Desktops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。リアルタイムと履歴の両方の可視性データが利用できるため、NetScaler Consoleは幅広いユースケースをサポートできます。

データが表示されるようにするには、NetScaler Gateway仮想サーバーでAppFlowを有効にする必要があります。AppFlowは、**IPFIX**プロトコルまたは**Logstream**メソッドによって配信できます。

「

注

」

ICA®ラウンドトリップ時間の計算がログに記録されるようにするには、次のポリシー設定を有効にします。

- ICAラウンドトリップ計算
- ICAラウンドトリップ計算間隔
- アイドル接続のICAラウンドトリップ計算

個々のユーザーをクリックすると、選択した期間内にユーザーが行った、アクティブまたは終了した各HDXセッションを確認できます。その他の情報には、いくつかの遅延統計とセッション中に消費された帯域幅が含まれます。また、オーディオ、プリンターマッピング、クライアントドライブマッピングなどの個々の仮想チャネルから帯域幅情報を取得することもできます。

すべてのユーザーのアクティブおよび終了したセッションの統合されたビューを視覚化することもできます。

HDX Insightの改善点(/en-us/netscaler-console-service/media/hdx-insight-improvement.png)

管理者として、このビューを使用すると、次のことができます。

- シングルペインの視覚化ですべてのユーザーの詳細を表示する
- 各ユーザーを選択してアクティブおよび終了したセッションを確認する際の複雑さを排除する

「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

」

グループを作成するときに、グループに役割を割り当てたり、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 Consoleアナリティクスは、仮想IPアドレスベースの認証をサポートするようになりました。ユーザーは、承認されているアプリケーション (仮想サーバー) のすべての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、「NetScaler Consoleでのグループの構成」を参照してください。

HDX Insight > **アプリケーション** に移動し、**起動時間** 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、**HDX Insight > ユーザー** 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管理パーティションをサポートしています。

次のシンクライアントはHDX 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

Citrix Virtual Apps and Desktopsへのアクセス中にユーザーが遅延を経験している

遅延は、サーバーネットワークの遅延、サーバーネットワークによって引き起こされるICAトラフィックの遅延、またはクライアントネットワークの遅延が原因である可能性があります。

問題の根本原因を特定するには、次のメトリックを分析します。

- WAN遅延
- DC遅延

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ホスト遅延

クライアントメトリクスを表示するには：

1. **Analytics**タブで、**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ヶ月から選択でき、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。

   クライアントメトリクス(/en-us/netscaler-console-service/media/nmas-hdxinsight-analytics-1.png)
4. **Current Application Sessions**テーブルで、**RTT**値にマウスを重ねて、ホスト遅延、DC遅延、WAN遅延の値をメモします。
5. **Current Application 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。

   現在のアプリケーションセッション(/en-us/netscaler-console-service/media/nmas-hdxinsight-analytics-2.png)

概要：

この例では、**DC Latency**は751ミリ秒、**WAN latency**は52ミリ秒、**Host Delays**は6秒です。これは、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、ユーザーが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 Apps™またはDesktopsでアプリケーションを起動する際にユーザーが遅延を経験している

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るもの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

ユーザーメトリックを表示するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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遅延、DC遅延、およびRTT値に注目します。
4. **Current Application Sessions** テーブルで、ホスト遅延が高いことに注目します。

概要：

この例では、**DC遅延**は1ミリ秒、**WAN遅延**は12ミリ秒ですが、**ホスト遅延**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、ホストサーバー上のアプリケーションエラーを示しています。

注

NetScaler Consoleソフトウェアバージョン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隣のテーブルに表示されます。

HDX Insight のジオマップ

NetScaler Console のジオマップ機能は、Web アプリケーションの利用状況を異なる地理的場所で地図上に表示します。管理者として、この情報を使用してアプリケーションの使用傾向を把握し、キャパシティプランニングに役立てることができます。

ジオマップは、国、州、都市に固有の以下のメトリックに関する情報を提供します。

- 総ヒット数: アプリケーションがアクセスされた合計回数。
- 帯域幅: クライアント要求の処理中に消費された合計帯域幅
- 応答時間: クライアント要求への応答を送信するのにかかった平均時間。

ジオマップは、次のような複数のユースケースに対応するために使用できる情報を提供します。

- アプリケーションにアクセスするクライアントの数が最も多い地域
- 応答時間が最も長い地域
- 最も帯域幅を消費する地域

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console は、**Web insight** を有効にすると、プライベート IP アドレスまたはパブリック IP アドレスのジオマップを**自動的に有効にします**。

プライベート IP ブロックの作成

NetScaler Console は、クライアントのプライベート IP アドレスが NetScaler Console サーバーに追加されると、クライアントの場所を認識できます。たとえば、クライアントの IP アドレスが都市 A に関連付けられたプライベート IP アドレスブロックの範囲内にある場合、NetScaler Console は、そのクライアントのトラフィックが都市 A から発信されていると認識します。

IP ブロックを作成するには:

1. NetScaler Console で、**Settings > Analytics Settings > IP Blocks** に移動し、**Add** をクリックします。
2. 「**IPブロックの作成**」ページで、次のパラメータを指定します。
   - **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。
   - **都市**。地域に基づいて都市が自動入力されますが、都市を選択することもできます。
   - **都市の緯度**と**都市の経度**。選択した都市に基づいて、緯度と経度が自動入力されます。
3. **作成**をクリックして完了します。

パブリックIPブロック

クライアントがパブリックIPアドレスを使用している場合、NetScaler Consoleはクライアントの場所を認識することもできます。NetScaler Console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、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 Consoleは、特定の地理的位置のジオマップを表示するためにインターネット接続を必要とします。GeoMapを.pdf、.png、または.jpg形式でエクスポートするためにもインターネット接続が必要です。

ジオマップ(/en-us/netscaler-console-service/media/mas-web-insight-geomap.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このダッシュボードのレポートをエクスポートするには:

このページのレポートをエクスポートするには、このページの右上にある **Export** アイコンをクリックします。**Export** ページでは、次のいずれかを実行できます。

1. **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。
2. **Schedule Export** タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、メールまたはSlackメッセージでレポートを送信します。

注

- **毎週**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いることを確認してください。

データセンターのジオマップを構成するには:

Infrastructure タブで、**Sites** > **Private IP Blocks** に移動し、特定の場所のジオマップを構成します。

ユースケース

ABC社には2つの支社があり、1つはサンタクララに、もう1つはインドにあるシナリオを考えてみましょう。

サンタクララのユーザーは、SClara.x.com 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時の間に、サンタクララのユーザーはSClara.x.comに接続してVPNトラフィックにアクセスします。ほとんどのユーザーが同じNetScaler Gatewayにアクセスするため、VPNへの接続に遅延が発生し、一部のユーザーはSClara.x.comの代わりにIndia.x.comに接続します。

トラフィックを分析するNetScaler管理者は、ジオマップ機能を使用してサンタクララオフィスのトラフィックを表示できます。マップは、サンタクララオフィスの応答時間が高いことを示しています。これは、サンタクララオフィスにはユーザーがVPNトラフィックにアクセスできるNetScaler Gatewayアプライアンスが1つしかないためです。したがって、管理者は別のNetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gatewayをインストールして、ユーザーがVPNにアクセスするためのローカルNetScaler Gatewayアプライアンスを2つ持つように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、HDX Insight用にNetScaler Consoleで設定されたしきい値はトリガーされません。

このダッシュボードのレポートをエクスポートするには:

このページのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページで、次のいずれかを実行できます。

1. **今すぐエクスポート**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。
2. **エクスポートをスケジュール**タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、メールまたはSlackメッセージでレポートを送信します。

注

- **毎週**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いることを確認してください。

HDX™ Insight データ収集を有効にする

HDX Insight は、NetScaler アプライアンスを通過する ICA トラフィックに対するエンドツーエンドの可視性を提供することで、管理者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。

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表示できます。

NetScaler インスタンス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。このトピックには、次の詳細が含まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 透過モードで展開された NetScaler インスタンスの監視のためのデータ収集の有効化
- シングルホップモードで展開された NetScaler Gateway アプライアンスのためのデータ収集の有効化
- ダブルホップモードで展開された NetScaler Gateway アプライアンスのためのデータ収集の有効化
- LAN ユーザーモードで展開された NetScaler の監視のためのデータ収集の有効化

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がシングルホップモードで展開されている場合、NetScaler Gatewayはネットワークのエッジに位置し、ICA接続をデスクトップ配信インフラストラクチャにプロキシします。この展開は最も単純で一般的な展開です。このモードは、外部ユーザーが組織内の内部ネットワークにアクセスしようとした場合にセキュリティを提供します。シングルホップモードでは、ユーザーは仮想プライベートネットワーク（VPN）を介してNetScalerアプライアンスにアクセスします。

レポートの収集を開始するには、NetScaler GatewayアプライアンスをNetScaler Consoleインベントリに追加し、NetScaler ConsoleでAppFlowを有効にする必要があります。次の図は、シングルホップモードで展開されたNetScaler Consoleを示しています。

シングルホップ(/en-us/netscaler-console-service/media/single-hop-2.png)

NetScaler ConsoleからAppFlow機能を有効にする

1. **インフラストラクチャ** > **インスタンス** に移動し、分析を有効にするNetScalerインスタンスを選択します。
2. **アクションの選択** リストから、**分析の構成** を選択します。
3. 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. **Web Insight** 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、以下のコマンドがバックグラウンドで実行され始めます。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

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アプライアンス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 Consoleインベントリに追加した後、データ収集のためにAppFlowを有効にする必要があります。データ収集の有効化は、デバイスとモードによって異なります。その場合、各NetScalerアプライアンスにNetScaler ConsoleをAppFlowコレクターとして追加し、アプライアンスを通過するすべてのICAトラフィックまたは特定のICAトラフィックを収集するためのAppFlowポリシーを構成する必要があります。

注

- NetScaler Console構成ユーティリティを使用して、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 Consoleのネットワーク展開を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、次を実行します。

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NetScaler Insight CenterをAppFlowコレクターとして追加します。

```
add appflow collector <name> -IPAddress <ip_addr>
```

例:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

注

NetScalerアプライアンスで構成されているAppFlowコレクターを表示するには、**show appflow collector**コマンドを使用します。

4. AppFlow®アクションを作成し、コレクターをそのアクションに関連付けます。

```
add appflow action <name> -collectors <string> ...
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
```

8. 設定を保存します。

```
save ns config
```

© 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。

管理者として、NetScaler Consoleを使用して、以下を分析できます。

- ICA接続が通過するホップ数 (NetScaler Gatewayアプライアンス)
- 各TCP接続の遅延に関する詳細と、クライアントが認識する合計ICA®遅延に対してそれがどのように機能するか

次の図は、最初のDMZにあるNetScaler ConsoleとNetScaler Gatewayが同じサブネットに展開されていることを示しています。

ダブルホップ(/en-us/netscaler-console-service/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を通過できるようにし、サーバーファームへのユーザー接続を完了させます。

NetScaler Consoleは、最初のDMZにあるNetScaler Gatewayアプライアンスに属するサブネット、または2番目のDMZにあるNetScaler Gatewayアプライアンスに属するサブネットのいずれかに展開できます。

ダブルホップモードでは、NetScaler Consoleは、一方のアプライアンスからTCPレコードを、もう一方のアプライアンスからICAレコードを収集します。NetScaler Gatewayアプライアンスを NetScaler Consoleインベントリに追加し、データ収集を有効にすると、各アプライアンスはホップ数と接続チェーンIDを追跡することでレポートをエクスポートします。

NetScaler ConsoleがどのNetScaler Gatewayアプライアンスがレコードをエクスポートしているかを識別できるように、各アプライアンスにはホップ数が指定され、各接続には接続チェーンIDが指定されます。ホップ数は、クライアントからサーバーへのトラフィックが通過する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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleは、ホップ数と接続チェーンIDを使用して、両方のNetScaler Gatewayアプライアンスからのデータを関連付け、レポートを生成します。

このモードで展開されたNetScaler Gatewayアプライアンスを監視するには、まずNetScaler GatewayをNetScaler Consoleインベントリに追加し、NetScaler ConsoleでAppFlowを有効にし、その後、NetScaler Consoleダッシュボードでレポートを表示する必要があります。

NetScaler Consoleでのデータ収集の有効化

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 NetScaler Console を有効にすると、収集される詳細は冗長になります。この状況を回避するには、最初の NetScaler Gateway アプライアンスで TCP 用の AppFlow を有効にし、次に 2 番目のアプライアンスで ICA 用の AppFlow を有効にする必要があります。そうすることで、一方のアプライアンスは ICA AppFlow レコードをエクスポートし、もう一方のアプライアンスは TCP AppFlow レコードをエクスポートします。これにより、ICA トラフィックの解析にかかる処理時間も節約されます。

NetScaler Console から AppFlow 機能を有効にするには：

1. **Infrastructure** > **Instances** に移動し、分析を有効にする NetScaler インスタンスを選択します。
2. **Select Action** リストから、**Configure Analytics** を選択します。
3. 仮想サーバーを選択し、**Enable Security & Analytics** をクリックします。
4. Web **Insight** を選択します
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 Console にエクスポートするには、NetScaler Gateway アプライアンスで次の設定を構成する必要があります。

- 最初の DMZ と 2 番目の DMZ にある NetScaler Gateway アプライアンスの仮想サーバーが相互に通信するように構成します。
- 2 番目の DMZ にある NetScaler Gateway 仮想サーバーを、最初の DMZ にある NetScaler Gateway 仮想サーバーにバインドします。
- 2 番目の DMZ にある NetScaler Gateway でダブルホップを有効にします。
- 2 番目の DMZ にある NetScaler Gateway 仮想サーバーで認証を無効にします。
- いずれかの NetScaler Gateway アプライアンスで ICA レコードをエクスポートするように有効にします

© 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てNetScaler Gatewayを構成する:

1. 最初のDMZにあるNetScaler Gateway仮想サーバーが、2番目のDMZにあるNetScaler Gateway仮想サーバーと通信するように構成します。

   VPNネクストホップサーバーを追加 \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure** (ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

2. 2番目のDMZにあるNetScaler Gateway仮想サーバーを、最初のDMZにあるNetScaler Gateway仮想サーバーにバインドします。最初のDMZにあるNetScaler Gatewayで次のコマンドを実行します。

   VPN仮想サーバーをバインド \<name\> **-nextHopServer** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. 2番目のDMZにあるNetScaler Gatewayでダブルホップと AppFlowを有効にします。

   set vpn vserver \<name\> \[**- doubleHop** (有効 |無効)\] \[**- appflowLog** (有効 |無効)\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

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アプライアンスが TCPレコードをエクスポートするように有効にします。

   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アプライアンスが ICAレコードをエクスポートするように有効にします。

   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 \[**-connectionChaining** (ENABLED|DISABLED)\]

   ```
   set appflow param -connectionChaining ENABLED
   ```

構成ユーティリティを使用したNetScaler Gatewayの構成:

1. 最初のDMZにあるNetScaler Gatewayを、2番目のDMZにあるNetScaler Gatewayと通信するように構成し、2番目のDMZにあるNetScaler Gatewayを最初のDMZにあるNetScaler Gatewayにバインドします。

   a. **Configuration**タブで**NetScaler Gateway**を展開し、**Virtual Servers**をクリックします。
   b. 右側のペインで仮想サーバーをダブルクリックし、Advancedグループで**Published Applications**を展開します。
   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**のチェックを外します。

4. いずれかのNetScaler Gatewayアプライアンスで TCPレコードをエクスポートできるようにします。

a. 「**Configuration**」タブで「**NetScaler Gateway**」を展開し、「**Virtual Servers**」をクリックします。
b. 右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. 他のNetScaler Gatewayアプライアンスで ICAレコードのエクスポートを有効にします。

a. 「**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。

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**」の順に移動します。
b. 右側のペインの「**Settings**」グループで、「**Change Appflow Settings**」をクリックします。
c. 「**Connection Chaining**」を選択し、「**OK**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LANユーザーモードで展開されたNetScalerを監視するためのデータ収集を有効にする

Citrix Virtual AppまたはDesktopアプリケーションにアクセスする外部ユーザーは、NetScaler Gatewayで認証する必要があります。ただし、内部ユーザーはNetScaler Gatewayにリダイレクトされる必要がない場合があります。また、透過モード展開では、管理者はルーティングポリシーを手動で適用して、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するには、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。キャッシュリダイレクト仮想サーバーは、NetScaler Gatewayアプライアンス上でSOCKSプロキシとして機能します。

次の図は、**LANユーザーモード**で展開されたNetScaler Consoleを示しています。

LAN(/en-us/netscaler-console-service/media/lan.png)

注

NetScaler Gatewayアプライアンスはエージェントに到達できる必要があります。

このモードで展開されたNetScalerアプライアンスを監視するには、まずNetScalerアプライアンスをNetScaler Insightインベントリに追加し、AppFlowを有効にしてから、ダッシュボードでレポートを表示します。

NetScalerアプライアンスをNetScaler Consoleインベントリに追加した後、データ収集のためにAppFlowを有効にする必要があります。

注

- NetScaler Console構成ユーティリティを使用して、LANユーザーモードで展開されたNetScalerでデータ収集を有効にすることはできません。
- コマンドとその使用方法の詳細については、「コマンドリファレンス」を参照してください。
- ポリシー式に関する情報については、「ポリシーと式」を参照してください。

コマンドラインインターフェイスを使用してNetScalerアプライアンスでデータ収集を構成するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コマンドプロンプトで、次を実行します。

1. NetScaler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を適用す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アプライアンスでNetScaler ConsoleをAppFlowコレクターとして追加します。

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
```

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. AppFlow®アクションを作成し、コレクターをそのアクションに関連付けます。

```
add appflow action** \<name\> **-collectors** \<string\> ...
```

例:

```
add appflow action act -collectors MyInsight
```

5. トラフィックを生成するためのルールを指定するAppFlowポリシーを作成します。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

例:

```
add appflow policy pol true act
```

6. AppFlowポリシーをグローバルバインドポイントにバインドします。

```
bind appflow global** \<policyname\> \<priority\> **-type** \<type\>
```

例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

注

type の値は、ICA® トラフィックに適用するために 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set appflow param -flowRecordInterval 60
```

8. 設定を保存します。

```
save ns config
```

HDX™ Insight のしきい値を作成し、アラートを設定する

NetScaler Console の HDX Insight を使用すると、NetScaler インスタンスを通過する HDX トラフィックを監視できます。NetScaler Console では、Insight トラフィックの監視に使用されるさまざまなカウンターにしきい値を設定できます。また、NetScaler Console でルールを設定し、アラートを作成することもできます。

HDX トラフィックタイプは、アプリケーション、デスクトップ、ゲートウェイ、ライセンス、ユーザーなど、さまざまなエンティティに関連付けられています。各エンティティには、それぞれ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、ヒット数、アプリケーションによって消費される帯域幅、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 遅延、DC 遅延、ICA® RTT、およびユーザーによって消費される帯域幅に関連付けることができます。

NetScaler Console の HDX Insight のしきい値管理では、設定されたしきい値が侵害された場合に、事前にルールを作成し、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では、しきい値グループを地理的位置に関連付けることもできます。

NetScaler Console でアラートが生成されるのは、設定されたしきい値グループ内のすべてのルールが侵害された場合のみです。たとえば、合計セッション起動数とアプリケーション起動数の両方でアプリケーションを1つのしきい値グループとして監視できます。両方のルールが侵害された場合にのみアラートが生成されます。これにより、エンティティに対してより現実的なしきい値を設定できます。

いくつかの例を以下に示します。

- 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ミリ秒である必要があります

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- しきい値ルール2：ユーザー（エンティティ）のWAN遅延（メトリック）は\<= 100ミリ秒である必要があります

しきい値グループの例は次のとおりです：{しきい値ルール1 + しきい値ルール2}

ルールを作成するには、まず監視するエンティティを選択する必要があります。次に、ルール作成時にメトリックを選択します。たとえば、アプリケーションエンティティを選択し、**合計セッション起動数またはアプリ起動数**を選択できます。エンティティとメトリックのすべての組み合わせに対して1つのルールを作成できます。提供されている比較演算子（\>、\<、\>=、および\<=）を使用し、各メトリックのしきい値を入力します。

注

単一のグループで複数のエンティティを監視したくない場合は、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 Console はしきい値侵害を示すイベントを生成し、イベントごとに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。アラートをNetScaler Consoleに表示するか、電子メールまたはその両方で受信するか、モバイルデバイスでSMSとして受信するかを有効にできます。最後の2つのアクションについては、NetScaler Consoleで電子メールサーバーまたはSMSサーバーを設定する必要があります。

しきい値グループは、ユーザーエンティティの地理固有の監視のために地理的位置にバインドすることもできます。

使用例

ABC Inc.はグローバル企業であり、50か国以上にオフィスを構えています。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GSLBベースのリダイレクトを使用して、世界中のどこからでもCitrix Virtual Apps and Desktopsにアクセスしています。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プリとデスクトップの配信を最適化するために、すべてのオフィスのユーザーエクスペリエンスを追跡したいと考えています。Ericはまた、ICA RTT、遅延などのユーザーエクスペリエンスメトリックをチェックし、逸脱をプロアクティブに提起したいと考えています。

ABC Inc.のユーザーは分散した場所にいます。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、これらの場所ではメトリックと対応するしきい値も異なります。たとえば、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データセンターに近い場所のICA RTTは5〜10ミリ秒であるのに対し、遠隔地の同じものは約100ミリ秒になることがあります。

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域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、もしあれば容量の問題に根本原因を絞り込むこともできます。Ericは、HDX InsightポートフォリオメトリックのすべてのすべてのCitrix Virtual Apps and Desktopsを手動で確認する複雑さを心配することなく、逸脱をプロアクティブに追跡できるようになりました。

NetScaler Consoleを使用してHDX Insightのしきい値ルールグループを作成し、アラートを設定する

1. NetScaler Console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 Consoleがアラートを生成するイベントを作成するための名前を入力します。

    b. **トラフィックの種類**。リストから を選択します。

    c. **エンティティ**。リスト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の種類ごとに異なります。

    d. **参照キー**。参照キーは、選択したトラフィックの種類とエンティティに基づいて自動的に生成されます。

    e. **期間**。リストから、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。

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。

    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、個々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。

4. **ユーザーエンティティの地理位置情報タグ付けの設定:**

© 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。

5. **しきい値を有効にする**をクリックして、NetScaler Consoleがエンティティの監視を開始できるようにします。
6. オプションで、メールやSlack通知などのアクションを設定します。
7. しきい値ルールグループを作成するには、**作成**をクリックします。

HDX™ Insight レポートとメトリクスを表示

HDX Insight は、NetScaler インスタンス上の HDX トラフィックに関連するレポートとメトリクスを完全に可視化します。

選択したエンティティの HDX メトリクスを表示できます。ビューには、次のエンティティカテゴリが含まれます。

- **ユーザー**: 選択した時間間隔内に Citrix Virtual Apps and Desktops にアクセスす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。
- **ゲートウェイ仮想サーバー**: すべての仮想サーバーのレポートを表示します。
- **デスクトップ**: 選択した期間に使用されたデスクトップのレポートを表示します。
- **ライセンス**: 指定された時間枠内で使用された SSL VPN ライセンスの総数に関するレポートを表示します。

注:

14.1-51.x 以降のリリースでは、VPN 仮想サーバーレベルでアクティブなセッション、デスクトップ、起動されたアプリケーションなどの主要なメトリクスを監視できます。すべての仮想サーバーのリストは、**Gateway > HDX Insight > Gateway Virtual Servers** で表示できます。

このドキュメントには以下が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザービューのレポートとメトリクス
- アプリケーションビューのレポートとメトリクス
- デスクトップビューのレポートとメトリクス
- インスタンスビューレポートとメトリクス(/ja-jp/netscaler-console-service/analytics/hdx-insight/instance-view-reports-and-metrics.html)
- ライセンスビューレポートとメトリクス(/ja-jp/netscaler-console-service/analytics/hdx-insight/license-view-reports-and-metrics.html)

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。「**Gateway**」>「**HDX Insight**」>「**Applications**」の順に移動します。

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アプリケーションのレポートが表示されます。

明示的に言及されていない限り、すべてのメトリック/レポートには、選択した期間に対応する値が表示されます。

折れ線グラフ

メトリック	説明
セッション	指定された時間間隔におけるセッションの総数。
起動時間	アプリケーションの起動にかかる平均時間。

アプリケーションサマリーレポート

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
起動時間	Citrix Virtual Appの起動にかかった平均時間。

アクティブアプリケーションレポート

メトリック	説明
名前	Citrix Virtual Appの名前。
状態	アプリケーションの状態を表示します: 緑 - アクティブ、赤 - 非アクティブ
アクティブなセッション数	指定された時間間隔でこのアプリを使用しているアクティブなユーザーセッションの数。
アクティブなアプリ数	このアプリケーションのアクティブなセッション数。

アクティブなアプリケーション(/en-us/netscaler-console-service/media/hdx-active-applications.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*がアプリケーション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。

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-console-service/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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
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。
間隔あたりの帯域幅	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	セッション開始時刻。
アップタイム	セッション期間。
クライアントIPアドレス	エンドユーザーIP。
サーバーIPアドレス	バックエンド/Citrix Virtual AppサーバーのIPアドレス。
NetScaler IPアドレス	NetScaler管理IP (NSIP)。
クライアントタイプ	Citrix Workspace タイプ - Citrix Windows クライアント。
クライアントバージョン	Citrix Workspace 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
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フェイルオーバー回数	HAフェイルオーバーが発生した回数。
終了理由	セッション終了の理由を表示します。例えば、ICAセッションタイムアウト、ユーザーによるセッション終了など。
ICA RTT	ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションやデスクトップを操作する際に、ユーザーが経験する画面の遅延です。
WAN遅延	ネットワークのクライアント側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。

© 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。
クライアント側ゼロウィンドウサイズイベント	このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。
クライアント側の高速RTO	NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。
サーバー側のゼロウィンドウサイズイベント	このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。
サーバー側の高速RTO	NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
ユーザー名	この特定のCitrix Virtual Appにアクセスしているユーザーのユーザー名。
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	定義されたしきい値の違反が設定された時間間隔で発生した場合の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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
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。

現在のセッションレポート(/en-us/netscaler-console-service/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. **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 AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作しているときにユーザーが経験する画面の遅延です。
WAN遅延	ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
サーバー側のゼロウィンドウサイズイベント	ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまで。
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。
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。
クライアント側ゼロウィンドウサイズイベント	このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。

折れ線グラフ(/en-us/netscaler-console-service/media/hdx-line-chart-2.png)

ユーザー棒グラフ

この**ユーザー**棒グラフは、この特定のアプリにログインしているユーザーを表します。

ユーザーグラフ(/en-us/netscaler-console-service/media/hdx-user-bar-graph.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Desktop に焦点を当てています。**Gateway** > **HDX™ Insight** > **Desktop** の順に移動します。

概要ビュー

概要ビューには、選択したタイムライン中にログインしたすべての Citrix Virtual Desktops™ のレポートが表示されます。

明示的に記載されていない限り、以下のすべてのメトリクス/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。
アクティブなアプリ	この数値は、アクティブな Citrix Virtual App セッションの数を示します。
ICA RTT	ICA RTT は、Citrix Virtual App または Desktop でホストされているアプリケーションまたはデスクトップを操作しているときにユーザーが経験する画面の遅延です。
WAN 遅延	ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまで。
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。
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
	がシームレスでなくなるわけではありませんが、再送信による高い帯域幅使用率を示します。
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-console-service/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 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からバックエンドサーバーまでの遅延。

© 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。
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。

サマリーレポート(/en-us/netscaler-console-service/media/hdx-dekstop-summary-report.png)

しきい値レポート

しきい値レポートは、選択した期間に*エンティティ*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。

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. **Gateway > HDX Insight > Desktop**に移動します。
2. **Desktop Summary Report**から特定の**Desktop**を選択します。

折れ線グラフ

メトリック	説明
アクティブセッション	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。

© 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要した1秒あたりの合計バイト数。
サーバー側再送信	NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側の再送信	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、再送信による帯域幅の使用率が高いことを示します。
クライアント側の高速RTO	NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。
サーバー側の高速RTO	NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
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、デスクトップ起動数と帯域幅でソートできます。

メトリック	説明
名前	シトリックス バーチャル デスクトップの名前。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
デスクトップ起動数	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 からバックエンドサーバーまでの遅延です。
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 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(/en-us/netscaler-console-service/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	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。

© 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によって消費された帯域幅。
間隔あたりのバイト数	セッションがその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。
NetScaler IPアドレス	NetScaler管理IP (NSIP)。
クライアントの種類	シトリックス ワークスペース タイプ - シトリックス ウィンドウズ クライアント
クライアントバージョン	Citrix Workspace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。
受け入れられたUSBインスタンスの数	受け入れられたUSBインスタンスの数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
拒否されたUSBインスタンスの数	拒否されたUSBインスタンスの数。
停止されたUSBインスタンスの数	停止されたUSBインスタンスの数。
クライアントホスト名	クライアントのホスト名。
HAフェイルオーバー数	HAフェイルオーバーが発生した回数。
終了理由	セッション終了の理由を表示します。たとえば、ICAセッションタイムアウト、ユーザーによるセッション終了などです。
ICA RTT	ICA RTTは、Citrix Virtual Apps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にならない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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
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	このカウンタは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。
サーバー側高速RTO	NetScalerとバックエンドサーバー間の接続で再送信タイムアウトが発生した回数。
VDIイメージ名	ユーザーが接続しているCitrix Virtual Desktopの名前
図	

非アクティブなセッション(/en-us/netscaler-console-service/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は、特定の選択されたユーザーのセッションのレポートを提供します。

選択したユーザーのセッションのメトリ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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
セッションの再接続	この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。
ACRカウント	この数値は、アクティブなCitrix Virtual App セッションの数を示します。
ICA RTT	ICA RTTは、Citrix Virtual 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からバックエンドサーバーへの遅延です。
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数。
クライアント側再送信	NetScalerとエンドユーザー間の接続で再送信されたパケット数。このメトリックの値が高いからといって、ユーザーエクスペリエンスがシームレスでなくなるわけではありませんが、再送信による高い帯域幅利用率を示します。
クライアント側高速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る帯域幅。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
サーバー側ゼロウィンドウサイズイベント	このカウンターは、サーバーがゼロTCPウィンドウをアドバタイズした回数を示します。
クライアント側のゼロウィンドウサイズイベント	このカウンターは、クライアントがゼロTCPウィンドウをアドバタイズした回数を示します。

折れ線グラフ(/en-us/netscaler-console-service/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	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	特定の時間間隔中にセッションによって消費されたバイト数。
開始時刻	セッション開始時刻。
稼働時間	セッション継続時間。
クライアントIPアドレス	エンドユーザーIP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
サーバーIPアドレス	バックエンド/シトリックス バーチャル アプリケーション 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 クライアント
クライアントバージョン	Citrix Workspace バージョン。
MSI	ブール値 (はい/いいえ)。セッションがマルチストリーム ICA であるかどうかを示します。
セッションの再接続	セッションが再接続された回数。
ACR カウント	クライアントが切断されたセッションにユーザーを自動的に再接続した合計回数。
ユーザーアクセスタイプ	ICA セッションのアクセスモードを表示します。例: NetScaler Gateway ユーザー/透過モード。
国	セッションが確立された国。
地域	セッションが確立された地域。
都市	セッションが確立された都市。
USBステータス	アクティブ/非アクティブ - 緑/赤。
承認されたUSBインスタンスの数	承認されたUSBインスタンスの数。
拒否されたUSBインスタンスの数	拒否されたUSBインスタンスの数。
停止されたUSBインスタンスの数	停止されたUSBインスタンスの数。
クライアントホスト名	クライアントのホスト名。
HAフェイルオーバー数	HAフェイルオーバーが発生した回数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
終了理由	セッション終了の理由を表示します。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 ウィンドウを通知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 ンドウを通知した回数を示します。
サーバー側高速RTO	NetScalerとバックエンドサーバー間の接続で 再送信タイムアウトが発生した回数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
VDIイメージ名	ユーザーが接続しているCitrix Virtual Desktopの名前

非アクティブセッション(/en-us/netscaler-console-service/media/hdx-user-dekstop-active-inactive.png)

ユーザービュー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 AppまたはDesktopユーザーごとに表示されます。

Gateway > **HDX™ Insight** > **Users** に移動します。

概要ビュー

概要ビューには、選択したタイムライン中にログインしたすべてのユーザーのレポートが表示されます。このビューのすべてのメトリクス/レポートは、特に指定がない限り、選択した期間に対応する値を表示します。

選択した期間を変更するには：

1. 期間リストまたはタイムスライダーを使用して、目的の時間間隔を設定します。
2. **Go** をクリックします。

折れ線グラフ

メトリクス	説明
アクティブセッション	この数値は、アクティブなCitrix Virtual Apps and Desktopsセッションの数を示します。
アクティブなアプリ	この数値は、アクティブなCitrix Virtual Appセッションの数を示します。
ICA RTT	ICA RTTは、Citrix Virtual AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作しているときにユーザーが経験する画面の遅延です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
WAN遅延	ネットワークのクライアント側によって引き起こされる遅延。つまり、NetScalerからエンドユーザーまでの遅延です。
DC遅延	ネットワークのサーバー側によって引き起こされる遅延。つまり、NetScalerからバックエンドサーバーまでの遅延です。
帯域幅	選択された時間間隔中にエンドツーエンドの通信にかかった1秒あたりの合計ビット数。
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。

折れ線グラフ(/en-us/netscaler-console-service/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。

© 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	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、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を操作しているとき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	選択した時間間隔中にエンドツーエンド通信に要した合計ビット/秒。
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にならないという意味ではありませんが、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	説明
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。
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。
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。

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。メトリックを帯域幅または合計バイト数で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/総ビッ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-console-service/media/hdx-user-agents.png)

しきい値違反数

しきい値違反数メトリックは、選択した期間内に違反したしきい値の数を表します。

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、地域をクリックするだけで、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、さらに都市や州ごとの情報を表示するためにドリルダウンできます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightのワールドマップで以下の詳細を表示できます。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WAN遅延
- DC遅延
- 帯域幅
- 合計バイト数

ワールドマップ(/en-us/netscaler-console-service/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に関する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. **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。
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る帯域幅。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
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るバイト数。
開始時刻	セッション開始時刻。
稼働時間	セッション期間。
クライアントIPアドレス	エンドユーザーIP。
サーバーIPアドレス	バックエンド/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	ワークスペースタイプ - Citrix Windows Client
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。
セッション再接続数	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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
拒否されたUSBインスタンスの数	拒否されたUSBインスタンスの数。
停止されたUSBインスタンスの数	停止されたUSBインスタンスの数。
クライアントホスト名	クライアントのホスト名です。
HAフェイルオーバー数	HAフェイルオーバーが発生した回数。
終了理由	セッション終了の理由を表示します。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 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。
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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	説明
クライアント側の高速RTO	NetScalerとエンドユーザー間の接続で再送信タイムアウトが発生した回数。
サーバー側の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。

HDX INSIGHTにおけるEDTのサポート

NetScaler Consoleは、HDX Insightの分析を表示するために、現在、Enlightened Data Transport (EDT) をサポートしています。つまり、NetScaler ConsoleはUDPとTCPの両方のプロトコルをサポートしています。NetScaler GatewayのEDTサポートにより、Citrix Workspaceを実行しているユーザーに対して、仮想デスクトップのセッション内ユーザーエクスペリエンスが高精細に保証されます。

HDX Insightは、アクティブセッションレポートの一部として、EDTセッションと非EDTセッションの数を表示するようになりました。ユーザーテーブルには、システム内のすべてのユーザーの詳細レポートが表示されます。このテーブルには、WAN遅延、DC遅延、再送信、RTOなどのメトリックが表示されますが、これらのメトリックの一部は、現在TCPスタックから計算されているため、EDTセッションを持つユーザーには利用できません。したがって、それらは「NA」と表示されます。

- 新しいドーナツチャートが導入され、ユーザーが消費した帯域幅と、ユーザーが使用するプロトコルの種類に基づいた合計バイト数を確認できるようになりました。

NETSCALER CONSOLE 12.0以降で利用可能なHDX INSIGHTメトリック

L7 クライアント側遅延	ICAクライアントとNETSCALERインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCITRIX以外のデバイスが存在する場合に役立ちます。
L7 サーバー側遅延	NetScalerデバイスとCitrix Virtual App間で観測された平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 クライアント側遅延	ICAクライアントとNETSCALERインスタンス間で観測された平均L7遅延。このメトリックは、配信パスにCITRIX以外のデバイスが存在する場合に役立ちます。
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。

デスクトップユーザー

この表は、特定のユーザーのCitrix Virtual Desktopセッションに関する洞察を提供します。これらのメトリックは、デスクトップ起動回数と帯域幅でソートできます。

メトリック	説明
名前	シトリックス バーチャル デスクトップ の名前。
デスクトップ起動回数	デスクトップが起動された回数。
帯域幅	選択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秒あたりの合計ビット数。
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する際に、ユーザーが経験する画面の遅延です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリケーション

アクティブ、セッション起動総数、アプリ起動総数、起動期間でソートされたアプリを表す棒グラフです。

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、各ICA仮想チャネルによって消費される全体的な帯域幅または総ビット数をドーナツチャートの形式で表します。メトリックを帯域幅または総ビット数で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、各エンドポイントによって消費される全体的な帯域幅/総ビット数をドーナツチャートの形式で表します。メトリックを帯域幅または総ビット数でソートすることもできます。

ユーザーセッションごとの表示

ユーザーごとのセッションビューでは、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.

メトリクス	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 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。
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。

© 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。

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、1つまたは複数の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 Consoleにログオンします。
2. **Gateway** > **HDX™ Insight** > **Instances** の順に移動します。

インスタンスサマリービュー

このビューは、NetScaler Consoleに追加されたすべてのNetScalerインスタンスのレポートを表示するため、サマリービューと呼ばれます。

明示的に言及されていない限り、これら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あります。

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、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。
セッション起動の合計数	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合計数。
アプリケーションの合計数	指定された時間間隔で起動された一意のアプリケーションの合計数。
タイプ	該当なし

インスタンスサマリーレポート(/en-us/netscaler-console-service/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、選択した期間にインスタンスとして*エンティティ*が選択されている場合に、違反したしきい値の数を表します。詳細については、「しきい値とアラートの作成方法」を参照してください。

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。このフローは、サポートされていないCitrix Virtual AppまたはDesktopバージョン、サポートされていないワークスペース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、許可リストの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、「NetScalerチェックリストにおけるHDX/ICAトラフィックのレコード生成の問題」を参照してください。

ワールドビュー

HDX Insightのワールドマップビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者はシステムのワールドビューを持ち、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、都市や州ごとの情報

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を表示するためにドリルダウンできます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightのワールドマップでは以下の詳細を表示でき、各メトリックの密度はヒートマップ形式で表示されます。

- ICA RTT
- WAN遅延
- DC遅延
- 帯域幅
- 合計バイト数

インスタンスごとのビュー

インスタンスごとのビューは、特定の選択されたNetScalerインスタンスの詳細なエンドユーザーエクスペリエンスレポートを提供します。

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。
合計アプリ数	指定された時間間隔に起動された一意のアプリケーションの総数。

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、または起動時間に基づいて、上位5つのアプリケーションを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー棒グラフ

ユーザー棒グラフは、以下の基準に基づいて上位5人のユーザーを表示します

- 帯域幅
- WAN遅延
- DC遅延
- ICA RTT

ユーザー棒グラフ(/en-us/netscaler-console-service/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 デスクトップ名。
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。
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 AppまたはDesktopでホストされているアプリケーションまたはデスクトップを操作しているときにユーザーが経験する画面の遅延です。

デスクトップユーザーレポート(/en-us/netscaler-console-service/media/hdx-dekstop-user.png)

ワールドビュー

HDX Insightのワールドマップビューでは、管理者は地理的な観点から過去およびアクティブなユーザーの詳細を表示できます。管理者は、地域をクリックすることで、システムのワールド

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、さらにドリルダウンして都市および州ごとの情報を表示できます。NetScaler Consoleバージョン12.0以降では、地理的な場所から接続しているユーザーにドリルダウンできます。

HDX Insightの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。**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セッションや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、しきい値を超過した回数を表します。

© 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、問題は次のいずれかにある可能性があります。トラブルシューティングについては、それぞれのセクションのチェックリストを参照してください。

- HDX Insight の構成。
- NetScaler と NetScaler Console 間の接続。
- NetScaler での HDX/ICA トラフィックのレコード生成。
- NetScaler Console でのレコードの入力。

HDX Insight 構成チェックリスト

- NetScaler で AppFlow 機能が有効になっていることを確認します。詳細については、「AppFlow の有効化」を参照してください。
- NetScaler の実行中の構成で HDX Insight 構成を確認します。

  HDX Insight 構成を確認するには、`show running | grep -i <appflow_policy>` コマンドを実行します。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 REQUEST
  ```

  透過モードの場合、バインドタイプは ICA_REQ_DEFAULT である必要があります。例:

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- シングルホップ/Access Gateway またはダブルホップ展開の場合、HDX Insight AppFlow ポリシーが HDX/ICA トラフィックが流れる VPN 仮想サーバーにバインドされていることを確認してください。
- 透過モードまたは LAN ユーザーモードの場合、ICA® ポート 1494 および 2598 が設定されていることを確認してください。
- NetScaler GatewayまたはVPN仮想サーバーの`appflowlog`パラメータが、Access Gatewayまたはダブルホップ展開で有効になっていることを確認します。詳細については、仮想サーバーのAppFlowを有効にするを参照してください。
- ダブルホップNetScalerで「Connection Chaining」が有効になっていることを確認します。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ことを確認します。詳細については、NetScaler高可用性ペアでのセッション信頼性を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerとNetScaler Console間の接続チェックリスト

- 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。
- HDX Insight AppFlow®ポリシーのヒットを確認します。

  コマンド`show appflow policy <policy_name>`を実行して、AppFlowポリシーのヒットを確認します。

  GUIで**System > AppFlow > Policies**に移動して、AppFlowポリシーのヒットを確認することもできます。
- 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におけるHDX/ICAトラフィックのレコード生成チェックリスト

ログ検証のためにコマンド`tail -f /var/log/ns.log | grep -i "default ICA Message"`を実行します。生成されたログに基づいて、この情報をトラブルシューティングに利用できます。

- ログ: **ICA接続の解析をスキップしました - このホストではHDX Insightはサポートされていません**

  原因: サポートされていないCitrix Virtual Apps and Desktopsのバージョン

  回避策: Citrix Virtual Apps and Desktopsサーバーをサポートされているバージョンにアップグレードします。
- ログ: **クライアントタイプ0x53を受信しました、サポートされていません**

  原因: サポートされていないバージョンのCitrix Workspaceアプリ

  解決策: Citrix Workspaceアプリ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。
- 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: **Missing EUEM ICA RTT**

  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: **Skip code**

  スキップコードに以下のいずれかの値が表示された場合、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のに十分なバイトがありません

© 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
105	NS_ICA_ERR_INVALID_CHANNEL	無効なICAチャネル番号
106	NS_ICA_ERR_INVALID_DECODER	チャネルに指定されたデコーダーが無効です
107	NS_ICA_ERR_INVALID_TW_PARAM	Thinwireチャネルに指定されたパラメータ数が無効です
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未満の場合を示します
121	NS_ICA_ERR_CGP_INVALID_CMD	無効なCGPコマンドが検出されました
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	チャネル上のバイト数が不足しています
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL、またはSEAMLESSチャネル上の不正なデータ
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	クライアントから無効なデータ長を受信しました
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が検出されました

© 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の無効化エラー
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。不正なレシーバーで発生します。
135	NS_ICA_ERR_INVALID_SIGNATURE	不正なICA署名またはマジック文字列
136	NS_ICA_ERR_PARSE_RAW	ICAハンドシェイクパケットの解析中にエラーが発生しました
137	NS_ICA_ERR_INCOMPLETE_PKT	ハンドシェイクで不完全なパケットを受信しました
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICAフレームが大きすぎます。1,460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	サポートされている制限を超えて分割されているため、CGPコマンドを処理できません
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	許可リストにないため、このワークスペース（クライアント）のICA解析をスキップしました
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	クライアントの再接続クッキーの解析状態を検出できません
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	クライアント再接続後に無効な再接続クッキーの長さが検出されました
145	NS_ICA_ERR_INVALID_RECONNECT_ID	クライアントの再接続クッキーが必要な制約を満たしていません
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	クライアントから無効なワークスペースバージョン文字列が受信されました
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	クライアントから無効な製品IDが受信されました
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	展開後のチャネル長が無効です
149	NS_ICA_ERR_SPECIAL_THINWIRE	解凍エラー
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	シームレスコマンドに十分なバイト数が見つかりませんでした
151	NS_ICA_ERR_EUEM_INSUFFBYTE	EUEMコマンドに十分なバイト数が見つかりませんでした
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	シームレスチャネルの解析に無効なイベントです

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スキップコード	エラーメッセージ	エラーの原因
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRLチャネル解析の無効なイベント
154	NS_ICA_ERR_EUEM_INVALID_EVENT	EUEMチャネル解析の無効なイベント
155	NS_ICA_ERR_USB_INVALID_EVENT	USBチャネル解析の無効なイベント
156	NS_ICA_ERR_PURE_INVALID_EVENT	ピュアチャネル解析の無効なイベント
157	NS_ICA_ERR_VCP_INVALID_EVENT	仮想チャネル解析の無効なイベント
158	NS_ICA_ERR_ICAP_INVALID_EVENT	ICAデータ解析の無効なイベント
159	NS_ICA_ERR_CGPP_INVALID_EVENT	CGPデータ解析の無効なイベント
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	基本暗号化における暗号化コマンドの無効な状態
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	基本暗号化における無効な暗号化コマンド
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	RC5暗号化における暗号化コマンドの無効な状態
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	RC5暗号化における無効な暗号コマンド
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5暗号化/復号化エラー
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5暗号化/復号化エラー
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDAはReducer Version 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
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	WorkspaceはReducer Version 3をサポートしていません
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICAハンドシェイクで予期しないバイト数
169	NS_ICA_ERR_HIGHER_RECONSEQ	再接続後のピアからのCGP再開シーケンス番号が高い
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ACRの詳細を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セッション終了の詳細を解析中にエラーが発生しました
175	NS_ICA_ERR_NON_NSAP_SN	Insightチャネルのサポートがないため、サービスノードでのICA解析をスキップしました
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAPはクライアントでサポートされていません
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAPはVDAでサポートされていません
178	NS_ICA_ERR_NSAP_NEG_FAIL	NSAPデータネゴシエーション中のエラー

© 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
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
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無効化中のエラー

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。次の表に、ICA解析の様々なカウンターを示します。 カウンターの詳細を表示するには、コマンド `nsconmsg –g hdx –d statswt0` を実行します。

HDXカウンター名	目的	カテゴリ（統計/エラー/診断）
hdx_tot_ica_conn	NSによって検出された純粋なICA接続の総数を示します。クライアントPCB上の	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シグネチャに基づく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接続の総数を示します（セッション信頼性ON）。クライアントPCB上のCGPシグネチャに基づく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対応接続の総数を示します	統計
hdx_tot_skip_conn	無効なICAまたはCGP署名が原因で、パーサーによってスキップされたICA接続の数を示します。	統計
hdx_dbg_active_conn	その時点でのアクティブなEDT/CGP/ICA接続の総数。	統計
hdx_dbg_active_nsap_conn	その時点でのアクティブなEDT/CGP/ICA NSAP接続の総数。	統計
hdx_dbg_skip_appflow_disabled	AppFlowの無効化により、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	透過ユーザーアクセスの総数	統計/診断
hdx_dbg_ag_user	Access Gatewayユーザーアクセスの合計数	統計/診断
hdx_dbg_lan_user	LANユーザーモードアクセスの合計数	統計/診断

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDXカウンター名	目的	カテゴリ（統計/エラー/診断）
hdx_basic_enc	基本暗号化を使用しているICA接続の数を示します	統計/診断
hdx_advanced_enc	高度なRC5ベースの暗号化を使用しているICA接続の数を示します	統計/診断
hdx_dbg_reconnected_session	NetScalerエラーなしでクライアントからの再接続リクエストの合計数	統計/診断
hdx_dbg_host_rejected_ns_reconnect	クライアントによって再接続要求が拒否されたホストの総数	統計/診断
hdx_euem_available	エンドユーザーエクスペリエンス監視チャネルが利用可能な接続の数を示します。エンドユーザーエクスペリエンス監視チャネルは、ICA RTTなどの統計情報を収集するために必要です。	統計/診断
hdx_err_disabled_sr	`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が機能しません。	エラー
hdx_err_skip_no_msi	XA/XDサーバーにMSI機能がありません。これは古いサーバーバージョンを示しており、HDX Insightはこの接続をスキップします。	エラー
hdx_err_skip_old_server	サポートされていない古いサーバーバージョン	エラー
hdx_err_clnt_not_whitelist	クライアントレシーバーが許可リストにないため、HDX	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）
	Insightはこの接続をスキップします	
hdx_sm_ica_cam_channel_disabled	SmartAccessポリシーによって無効にされたNS_ICA_CAM_CHANNELの合計数	診断
hdx_sm_ica_usb_channel_disabled	SmartAccessポリシーによって無効にされたNS_ICA_USB_CHANNELの合計数	診断
hdx_sm_ica_clip_channel_disabled	SmartAccessポリシーによって無効にされたNS_ICA_CLIP_CHANNELの合計数	診断
hdx_sm_ica_ccm_channel_disabled	SmartAccessポリシーによって無効にされたNS_ICA_CCM_CHANNELの合計数	診断
hdx_sm_ica_cdm_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_CDM_CHANNELの総数	診断
hdx_sm_ica_com1_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_COM1_CHANNELの総数	診断
hdx_sm_ica_com2_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_COM2_CHANNELの総数	診断
hdx_sm_ica_cpm_channel_disabled	SmartAccessポリシーによって無効化された	診断

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDXカウンター名	目的	カテゴリ（統計/エラー/診断）
	NS_ICA_CPM_CHANNELの総数	
hdx_sm_ica_lpt1_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_LPT1_CHANNELの総数	診断
hdx_sm_ica_lpt2_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_LPT2_CHANNELの総数	診断
dx_dbg_sm_ica_msi_disabled	SmartAccessポリシーによってMSIが無効化されたケースの総数	診断
hdx_sm_ica_file_channel_disabled	SmartAccessポリシーによって無効化されたNS_ICA_FILE_CHANNELの総数	診断
hdx_dbg_usb_accept_device	承認された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	停止したUSBデバイスの総数	診断
hdx_dbg_usb_stop_device_response	停止したUSBデバイスからの応答総数	診断
hdx_dbg_usb_device_gone	消失したUSBデバイスの総数	診断
hdx_dbg_usb_device_stopped	停止したUSBデバイスの総数	診断

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nstraceの検証

NetScalerから出力されるすべてのAppFlowレコードを確認するには、CFLOWプロトコルをチェックします。

NetScaler Consoleチェックリスト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、ログを確認して、NetScaler ConsoleがAppFlowレコードを受信していることを確認します。
- NetScalerインスタンスがNetScaler Consoleに追加されていることを確認します。
- NetScaler Gateway/VPN仮想サーバーがNetScaler Consoleでライセンスされていることを検証します。
- 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とNetScaler Consoleのバージョン。
- Citrix Virtual Apps and Desktopsサーバーのバージョン。
- クライアントワークスペースのバージョン。
- 問題発生時のアクティブなICAセッション数。
- NetScalerコマンドプロンプトで `show techsupport` コマンドを実行して取得したテクニカルサポートバンドル。
- NetScaler Console用に取得したテクニカルサポートバンドル。
- すべてのNetScalerで取得されたパケットトレース。 パケットトレースを開始するには、`start nstrace -size 0'` と入力します。 パケットトレースを停止するには、`stop nstrace` と入力します。
- `show arp` コマンドを実行して、システムのARPテーブルのエントリを収集します。

既知の問題

HDX Insightの既知の問題については、NetScalerのリリースノートを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

しきい値のメトリクス情報

しきい値を作成し、その値が侵害されたときに通知を受け取ることができます。一般的な展開では、しきい値を次のように設定できます。

- さまざまなアプリケーションメトリクスを追跡する
- 計画を容易にする
- アプリケーションのメトリクス値が設定されたしきい値を超えたときに通知を受け取る

しきい値を設定するには：

1. **設定 > 分析設定 > しきい値** に移動します。
2. **Thresholds** ページで、**Add** をクリックします。

Web

メトリクス	エンティティ	説明
アプリケーション	ヒット数	仮想サーバー（アプリケーション）によって受信された総ヒット数
	帯域幅 (MB)	仮想サーバー (アプリケーション) が消費した総帯域幅
	応答時間 (ms)	仮想サーバーが応答するのにかかった時間
クライアント	リクエスト	クライアントが受信した総リクエスト
	レンダリング時間 (ms)	クライアントがサーバー応答をレンダリングするのにかかった時間
	クライアントネットワーク遅延	クライアントネットワークからのリクエストにかかった時間
デバイス	ヒット数	デバイスが受信した総ヒット数。例: ノートパソコン、携帯電話

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	エンティティ	説明
	帯域幅 (MB)	デバイスが消費した総帯域幅
ドメイン	ヒット数	ネットワークドメインが受信したヒットの総数
	帯域幅 (MB)	ネットワークドメインが消費した総帯域幅
	応答時間 (ms)	ネットワークドメインがリクエストに応答するのにかかった時間
オペレーティングシステム	ヒット数	オペレーティングシステムが受信したヒットの総数
	帯域幅 (MB)	オペレーティングシステムが消費した総帯域幅
	レンダリング時間 (ms)	オペレーティングシステムがサーバー応答をレンダリングするのにかかった時間
リクエストメソッド	ヒット数	リクエストメソッドが受信したリクエストの総数。例: GET、POST
	帯域幅 (MB)	リクエストメソッドが消費した合計帯域幅
レスポンスステータス	ヒット数	レスポンスコードで受信したヒットの総数
	帯域幅 (MB)	レスポンスコードが消費した合計帯域幅
サーバー	ヒット数	サーバーが受信したリクエスト/ヒットの総数
	帯域幅 (MB)	サーバーが消費した合計帯域幅

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリクス	エンティティ	説明
	サーバーネットワーク遅延 (ms)	サーバーネットワークからのリクエストにかかる時間
	サーバー処理時間 (ms)	サーバーがリクエストに応答するのにかかる時間
URL	ヒット数	URLが受信したヒットの合計数。例: www.Citrix.com
	ロード時間 (ms)	サーバーからURLがロードされるのにかかる時間
	レンダリング時間 (ms)	URLがレンダリングおよび表示されるのにかかる時間
ユーザーエージェント	ヒット数	ユーザーエージェントが受信したリクエストの合計数。例: Chromeウェブブラウザ
	帯域幅 (MB)	ユーザーエージェントによって消費された合計帯域幅
	レンダリング時間 (ms)	ユーザーエージェントがサーバー応答をレンダリングするのにかかった時間

セキュリティ

メトリック	エンティティ	説明
アプリケーション	脅威インデックス	アプリケーションに対する攻撃の重要度を示す1桁の評価システム。アプリケーションに対する攻撃が重要であるほど、そのアプリケーションの脅威インデックスは高くなります。値は1から7の範囲です。
	安全性インデックス	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メトリック	エンティティ	説明
		に、NetScalerインスタンスをどれだけ安全に構成したかを示す1桁の評価システム。アプリケーションのセキュリティリスクが低いほど、安全性インデックスは高くなります。値は1から7の範囲です。

APPANALYTICS

メトリック	エンティティ	説明
アプリケーション	AppScore	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し、応答性の観点からアプリケーションが適切に機能しているかどうかを示します。値は0から80の範囲です。

HDX™

HDX のしきい値については、HDX Insight のしきい値を作成し、アラートを設定するを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インフラストラクチャ

NetScaler Consoleのインフラストラクチャ機能を使用すると、NetScalerインスタンスを監視および管理できます。インフラストラクチャの健全性を分析し、インスタンスとイベントを管理し、SSL証明書を処理し、構成ジョブとアップグレードジョブを実行し、ネットワーク全体でインスタンスをプロビジョニングできます。

次のトピックは、インフラストラクチャの監視と管理に役立ちます。

- インフラストラクチャ分析
- インスタンス管理
- イベント
- SSLダッシュボード
- 構成
- アップグレードジョブ
- ネットワーク機能
- ネットワークレポート
- プロビジョニング
- オーケストレーション

インフラストラクチャ分析

ネットワーク管理者にとって重要な目標の1つは、NetScalerインスタンスを監視することです。NetScalerインスタンスは、それを通じてアクセスされるアプリケーションやデスクトップの使用状況とパフォーマンスに関する興味深い洞察を提供します。管理者はNetScalerインスタンスを監視し、各NetScalerインスタンスによって処理されるアプリケーションフローを分析する必要があります。管理者はまた、構成、セットアップ、接続、証明書、およびアプリケーションの使用状況やパフォーマンスにおけるその他の影響に関する潜在的な問題を修正できる必要があります。たとえば、アプリケーショントラフィックパターンの突然の変化は、SSLプロトコルの無効化のようなSSL構成の変更が原因である可能性があります。管理者は、以下のことを確実にするために、これらのデータポイント間の相関関係を迅速に特定できる必要があります。

- アプリケーションの可用性が最適な状態であること
- リソース消費、ハードウェア、容量、または構成変更に関する問題がないこと

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 未使用のインベントリがないこと
- 有効期限切れの証明書がないこと

インフラストラクチャ分析機能は、複数のデータソースを関連付け、インスタンスの健全性を定義する測定可能なスコア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、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。

NetScaler Consoleのインフラストラクチャ分析

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、表形式またはサークルパックの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特定するのにも役立ちます。

インスタンススコア

インスタンススコアは、NetScalerインスタンスの健全性を示します。スコアが100の場合、問題のない完全に健全なインスタンスであることを意味します。インスタンススコアは、インスタンス上の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、スコアは、事前定義された「監視期間」に対して、その時間枠で検出されたすべてのインジケーターに基づいて定期的に計算されます。現在、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カテゴリのいずれかに属するアクティビティ（イベントまたは問題）として定義できます。

- システムリソースインジケーター
- 重大イベントインジケーター
- SSL構成インジケーター
- 設定偏差インジケーター

健全性インジケーターの説明

- システムリソースインジケーター

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以下は、NetScalerインスタンスで発生する可能性があり、NetScaler Consoleによって監視される重要なシステムリソースの問題です。

- **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。
- **高いメモリ使用率**。NetScalerインスタンスでメモリ使用率が上限しきい値を超えました。
- **高いディスク使用率**。NetScalerインスタンスでディスク使用率が上限しきい値を超えました。
- **ディスクエラー**。NetScalerインスタンスがインストールされているハイパーバイザーのハードディスク0またはハードディスク1にエラーがあります。
- **電源障害**。NetScalerインスタンスへの電源供給が失敗したか、切断されました。
- **SSLカード障害**。インスタンスにインストールされているSSLカードが故障しました。
- **フラッシュエラー**。NetScalerインスタンスでコンパクトフラッシュエラーが検出されました。
- **NIC破棄**。NetScalerインスタンスでNICカードによって破棄されたパケットが上限しきい値を超えました。

これらのシステムリソースエラーの詳細については、「インスタンスダッシュボード」を参照してください。

- 重要なイベントインジケーター

  以下の重要なイベントは、NetScaler Consoleのイベント管理機能で、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NetScalerインスタンス間の構成同期がセカンダリサーバーで失敗しました。
  - **HAハートビートなし**。高可用性構成のNetScalerインスタンスのペアにおけるプライマリサーバーが、セカンダリサーバーからハートビートを受信していません。
  - **HAセカンダリ状態不良**。高可用性構成のNetScalerインスタンスのペアにおけるセカンダリサーバーが、ダウン、不明、またはセカンダリ維持状態です。
  - **HAバージョン不一致**。高可用性構成のNetScalerインスタンスのペアにインストールされているNetScalerソフトウェアイメージのバージョンが一致しません。
  - **クラスター同期失敗**。クラスターモードのNetScalerインスタンス間の構成同期が失敗しました。
  - **クラスターバージョン不一致**。クラスターモードのNetScalerインスタンスにインストールされているNetScalerソフトウェアイメージのバージョンが一致しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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。

  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 Console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**。NetScalerインスタンスにインストールされているSSL証明書の期限が切れました。
  - **SSL証明書の期限が間近**。NetScalerインスタンスにインストールされているSSL証明書が、今後1週間以内に期限切れになります。
  - **推奨されないアルゴリズム**。NetScalerインスタンスにインストールされているSSL証明書の署名アルゴリズムが、NetScalerの標準に準拠していません。

SSL証明書の詳細については、SSLダッシュボード を参照してください。

- 構成の逸脱インジケーター
  - **構成ドリフトテンプレート**。特定のインスタンスで監査したい特定の構成で作成した監査テンプレートから、構成にドリフト（未保存の変更）があります。
  - **構成ドリフトのデフォルト**。デフォルトの構成ファイルから、構成にドリフト（未保存の変更）があります。

構成の逸脱と、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。

NetScalerのキャパシティ問題を表示する

NetScalerインスタンスが利用可能なキャパシティのほとんどを消費すると、クライアントトラフィックの処理中にパケットドロップが発生する可能性があります。このようなNetScalerのキャパシティ問題を理解することで、NetScalerのパフォーマンスを安定させるために、追加のライセ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ンスを積極的に割り当てることができます。詳細については、NetScalerインスタンスのキャパシティ問題を表示する を参照してください。

ヘルスインジケーターの値

インジケーターは、その値に基づいて、高優先度インジケーターと低優先度インジケーターに次のように分類されます。

同じグループ内のヘルスインジケーターには、異なる重みが割り当てられています。あるインジケーターは、別のインジケーターよりもインスタンススコアの低下に大きく寄与する可能性があります。たとえば、高いメモリ使用量は、高いディスク使用量、高いCPU使用量、NIC破棄よりもインスタンススコアを大きく低下させます。インスタンスで検出されるインジケーターの数が多いほど、インスタンススコアは低くなります。

インジケーターの値は、以下のルールに基づいて計算されます。インジケーターは、以下の3つのいずれかの方法で検出されたと見なされます。

1. **アクティビティに基づく**。たとえば、インスタンスで電源障害が発生すると、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は増加します。
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いて**。ここでは、インジケーターは2つの方法でトリガーされます。
    - 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。その場合、インスタンススコアに部分的なペナルティが課されます。
    - 値が高しきい値を超えた場合。その場合、インスタンススコアに完全なペナルティが課されます。
    - 値が低しきい値を下回った場合、インスタンススコアにペナルティは課されません。

たとえば、CPU使用率はシステムリソースインジケーターであり、使用率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ます。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インフラストラクチャ分析は、**サークルパック**形式または**表形式**で表示できます。これら2つの形式を切り替えることができます。

- 表形式ビューでは、検索バーにホスト名またはIPアドレスを入力してインスタンスを検索できます。
- デフォルトでは、インフラストラクチャ分析ページにはページの右側にサマリーパネルが表示されます。
- **設定**アイコンをクリックして、**設定**パネルを表示します。
- どちらの表示形式でも、サマリーパネルには、ネットワーク内のすべてのインスタンスの詳細が表示されます。

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表示します。これらは多くの場合、より小さなインスタンスグループが同じカテゴリの他のグループと類似した色で表示されるか、より大きなグループ内にネストされている階層を示します。サークルパックは階層データセットを表し、階層内の異なるレベルとそれらがどのように相互作用するかを示します。

サークルパック(/en-us/netscaler-console-service/media/circle-pack.png)

インスタンスサークル

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。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。いくつかの問題が検出されており、レビューが必要です。
- **赤** - インスタンススコアが50未満。そのインスタンスで複数の問題が検出されているため、インスタンスは危機的な状態にあります。

インスタンスサークル(/en-us/netscaler-console-service/media/infra-analytics-3.png)

サイズ。これらの色付きの円のサイズは、そのインスタンスに構成されている仮想サーバーの数を示します。円が大きいほど、仮想サーバーの数が多いことを示します。

各インスタンスサークル（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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスサークル(/en-us/netscaler-console-service/media/infra-analytics-4.png)

グループ化されたインスタンスサークル

Circle Packは当初、以下の基準に基づいて、グループ化、ネスト、または別の円の中にパックされたインスタンスサークル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
- NetScalerインスタンスの仮想モデルまたは物理モデル
- インスタンスにインストールされているNetScalerイメージのバージョン

次の図は、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。

グループ化されたインスタンスの円(/en-us/netscaler-console-service/media/infra-analytics-5.png)

これらすべてのネストされた円は、2つの最も外側の円によって囲まれています。外側の2つの円は、NetScaler Consoleによって監視されるイベントの4つのカテゴリ（システムリソース、クリティカルイベント、SSL構成、構成偏差）と、それに寄与する健全性インジケータを表しています。

クラスター化されたインスタンスの円

NetScaler Consoleは多くのインスタンスを監視します。これらのインスタンスの監視とメンテナンスを容易にするために、Infrastructure Analyticsでは2つのレベルで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NetScalerインスタンスがデプロイされています。まず、NetScalerインスタンスをタイプ別にグループ化し、次にすべてのインスタンスをグループ化されているサイト別にグループ化できます。これにより、管理しているサイトに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。

クラスター化されたインスタンス(/en-us/netscaler-console-service/media/infra-analytics-6.png)

クラスター化されたインスタンス(/en-us/netscaler-console-service/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-console-service/media/infra-analytics-7.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

タイプとバージョン:

タイプ(/en-us/netscaler-console-service/media/infra-analytics-8.png)

サイトとバージョン:

バージョン(/en-us/netscaler-console-service/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(/en-us/netscaler-console-service/media/circle-pack-how-to.png)

そのインスタンスで発生したイベントに応じて、外側の円には、それらの健全性インジケーターのみが強調表示されます。たとえば、Circle Pack の次の2つの画像は、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 の使用方法(/en-us/netscaler-console-service/media/infra-analytics-10.png)

健全性インジケーターをクリックして、そのリスクインジケーターを報告したインスタンスの数に関する詳細情報を取得することもできます。たとえば、`Not recommended Algo` をクリックして、そのリスクインジケーターの概要レポートを表示します。

Circle Pack の使用方法(/en-us/netscaler-console-service/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詳細が表形式で表示されます。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。

検索バー

検索バーにマウスポインターを置き、次の検索属性を選択して結果をフィルタリングします。

- ホスト名
- IPアドレス
- タイプ
- バージョン
- サイト

検索結果は、サークルビューとテーブルビューの両方で機能します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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クリティカルな状態のインスタンスに効率的かつ迅速に焦点を当てるのに役立ちます。このパネルは、概要、インスタンス情報、トラフィックプロファイルの3つのタブに分かれています。このパネルで行った変更は、サークルパック形式と表形式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インジケーターに基づいてインスタンスを監視できます。ここで監視できるインジケーターは次のとおりです。

- CPU使用率
- メモリ使用率
- ディスク使用率
- システム障害
- 重大イベント
- SSL証明書の有効期限切れ

これらのインジケーターの詳細については、「*NetScalerインスタンスのヘルスインジケーター*」を参照してください。

以下の例は、「**概要**」パネルを操作して、エラーを報告しているインスタンスを分離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：

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を表示するには、「**レビュー**」チェックボックスを選択します。

「**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。いずれかの棒グラフにマウスポインターを合わせます。グラフの下部にある凡例には、使用範囲とその範囲内のインスタンス数が表示されます。棒グラフをクリックして、その範囲内のすべてのインスタンスを表示することもできます。

例2：割り当てられたメモリの10%から20%を消費しているインスタンスを表示する：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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29個のインスタンスが動作していることが示されます。

これらのヒストグラムで複数の範囲を選択することもできます。

例3：複数の範囲でディスク領域を消費しているインスタンスを表示する：

0%から10%のディスク領域を消費したインスタンスを表示するには、次の図に示すように、マウスポインターを2つの範囲にドラッグします。

注：

選択を解除するには、「X」をクリックします。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：

「**SSL証明書の有効期限**」セクションで、3つのインスタンスを表示するには、「**期限切れ**」チェックボックスを選択します。

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。

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、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。棒グラフを選択して、その範囲のインスタンスを表示します。

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、23から40のTCP接続をサポートし、1秒あたり最大100のSSLトランザクションを処理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、次のことができます。

- インフラストラクチャ分析のデフォルトビューを設定します。
- 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します。
- インスタンスメトリックを選択し、しきい値を設定し、インスタンススコアを計算するためにそれらのメトリックに重みを割り当てます。
- 必要な問題を選択し、設定されたしきい値を超えた問題の通知を有効にし、選択された問題のみの通知を受け取ります。

表示

- **デフォルトビュー**。分析ページのデフォルトビューとして、**Circle Pack** または表形式を選択します。選択した形式は、NetScaler Console でページにアクセスするたびに表示されるものです。
- **Circle Pack - インスタンスサイズ**。インスタンス円のサイズを、仮想サーバーの数またはアクティブな仮想サーバーの数のいずれかに設定できます。
- **Circle Pack - クラスター化の基準**。インスタンス円の2レベル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円」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンススコア計算のメトリックを選択し、重みをカスタマイズする

インスタンスメトリックを選択し、しきい値を設定し、インスタンススコアを計算するためにそれらのメトリックに重みを割り当てることができます。デフォルトでは、すべてのメトリックが選択され、各メトリックにデフォルトの重みが割り当てられます。要件に応じてメトリックを選択し、インスタンススコアの計算を決定するために適切な重みを割り当てることができます。

設定アイコンをクリックし、**スコアインジケーター設定**タブを選択して、次の操作を行います。

- 必要なメトリックを選択し、しきい値を追加する
- メトリックに重みを割り当てる。

しきい値を設定し、重みを割り当てたら、**保存**をクリックします。インスタンススコアは、選択されたメトリックとその重みに基づいてのみ更新されます。

スコアしきい値(/en-us/netscaler-console-service/media/infra-analytics-19.png)

通知を構成する

必要な問題を選択し、構成されたしきい値を超過した問題に対して通知を有効にし、選択した問題のみ通知を受け取ることができます。この機能強化により、監視したい選択した問題のみ通知を受け取ることができます。

> **注:**
>
> デフォルトでは、すべてのカテゴリの問題が選択されています。しきい値を構成できる問題に対してのみ通知を有効にできます。

1. **設定**アイコンをクリックし、**スコアインジケーター設定**タブを選択します。
2. 通知を受け取りたい問題を選択します。
3. **システムリソース**および**キャパシティ**カテゴリの問題については、**通知**を有効にします。

   通知(/en-us/netscaler-console-service/media/enable-notification.png)
4. **保存**をクリックします。

   > **注:**
   >
   > **通知**タブで少なくとも1つのプロファイルを構成していることを確認する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ダッシュボードでデータを視覚化する方法

Infrastructure Analytics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。これをより詳しく理解するために、ExampleCompanyのネットワーク管理者であるChrisのケースを考えてみましょう。

Chrisは彼の組織で多くの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、彼はそれらを綿密に監視する必要があります。彼は、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取る必要がありました。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見つけるために、より多くの時間を費やす必要がありました。彼はInfrastructure Analytics機能を使用して、すべてのインスタンスの健全性を視覚的に確認しています。

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トラフィックを監視する:

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す。彼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、そのためそのインスタンスが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ります。

例2 - 設定変更を監視する:

Chrisはまた、別のインスタンスが「Review」状態であり、最近設定の逸脱があったことにも気づきます。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す。彼はまた、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す。彼はこのレポートをエクスポートし、さらに調査するよう管理者に送ります。

Infrastructure Analytics でインスタンスの詳細を表示する

1. **インフラストラクチャ > インフラストラクチャ アナリティクス** 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

テーブルビューからIPアドレスをクリックすることもできます。

- **ホスト名** – NetScaler インスタンスに割り当てられたホスト名を示します
- **IPアドレス** – NetScaler インスタンスのIPアドレスを示します
- **スコア** – NetScaler インスタンスのスコアと、Critical、Good、Fair などのステータスを示します
- **可用性** – NetScaler インスタンスの現在のステータス（**Up**、**Down**、**Out of service** など）を示します。
- **最大寄与** – NetScaler インスタンスが最大のエラー数を記録している問題カテゴリを示します。
- **CPU使用率** – インスタンスによって使用されている現在のCPU使用率（%）を示します
- **メモリ使用率** – インスタンスによって使用されている現在のメモリ使用率（%）を示します
- **ディスク使用率** – インスタンスによって使用されている現在のディスク使用率（%）を示します
- **システム障害** – インスタンスシステムのエラーの合計数を示します
- **重大イベント** – NetScalerインスタンスが最大数のイベントを持つイベントカテゴリを示します
- **SSL有効期限** – NetScalerインスタンスにインストールされているSSL証明書の現在のステータスを示します
- **タイプ** – VPX、SDX、MPX、CPXなどのNetScalerインスタンスタイプを示します
- **展開** – NetScalerインスタンスがスタンドアロンインスタンスとして展開されているか、HAペアとして展開されているかを示します
- **モデル** – NetScalerインスタンスのモデル番号を示します
- **バージョン** – NetScalerインスタンスのバージョンとビルド番号を示します
- **スループット** – NetScalerインスタンスからの現在のネットワークスループットを示します
- **HTTPSリクエスト/秒** – NetScalerインスタンスが受信した現在のHTTPSリクエスト/秒を示します
- **TCP接続** – 確立された現在のTCP接続を示します
- **SSLトランザクション** – NetScalerインスタンスによって処理された現在のSSLトランザクションを示します
- **サイト** – NetScalerインスタンスが展開されているサイトの名前を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

IPアドレスをクリックし、表示されるページで「**インスタンスの詳細**」をクリックして、インスタンスの詳細を表示します。

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詳細。

- **機能** – デフォルトでは、ライセンスされていない機能が表示されます。**ライセンスされた機能**をクリックして、ライセンスされている機能を表示します。

- **モード** – デフォルトでは、インスタンスで無効になっているすべてのモードが表示されます。**有効なモードを表示**をクリックして、インスタンスで有効になっているモードを表示します。

インスタンスダッシュボードには、以下の詳細を確認できるインスタンスの概要が表示されます。

- **インスタンススコア**

  1 – 選択した期間の現在のNetScalerインスタンススコアを示します。最終スコアは**100から合計ペナルティを引いた値**として計算されます。グラフには、選択した期間のスコア範囲が表示されます。

  2 – **稼働中**、**停止中**、**サービス停止中**など、NetScalerインスタンスの現在のステータスを示します。

  3 – NetScalerインスタンスが稼働している期間を示します。

  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。**有効**または**無効**をクリックして、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）などの詳細を表示します。

  5 – リストから期間を選択して、インスタンスの詳細を表示します。

  6 – NetScalerインスタンスの合計問題数と問題カテゴリを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **主要メトリック**

  各タブをクリックして詳細を表示します。各メトリックでは、選択した期間の平均値と差分値を表示できます。

  次の画像はHTTPS Req/Secの例で、選択された期間は1時間です。値**692**は1ヶ月間のHTTPS Req/Secの平均値であり、値**20**は差分値です。グラフでは、最初の値が**139**で、最後の値が**119**です。差分値は**139 – 119 = 20**です。

  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使用率。
  - **スループット** – 選択した期間に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平均HTTPSリクエスト数。
  - **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平均TCP接続数。
  - **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。

問題カテゴリ	説明	問題
システムリソース	CPU、メモリ、ディスク使用量など、NetScalerシステムリソースに関連するすべての問題を表示します。	- 高いCPU使用率
		- 高いメモリ使用率
		- 高いディスク使用率
		- SSLカードの障害

© 1997–2026 Citrix Systems, Inc. All rights reserved.

問題カテゴリ	説明	問題
		- 電源障害
		- ディスクエラー
		- フラッシュエラー
		- NIC破棄
SSL設定	NetScalerインスタンス上のSSL設定に関連するすべての問題を表示します。	- SSL証明書の期限切れ
		- 推奨されない発行者
		- 推奨されないアルゴリズム
		- 推奨されない鍵強度
構成の逸脱	NetScalerインスタンスに適用された構成ジョブに関連するすべての問題を表示します。	- 構成ドリフト
		- 実行中とテンプレートの比較
重大なイベント	HAペアおよびクラスターで構成されたNetScalerインスタンスに関連するすべての重大なイベントを表示します。	- クラスタープロパゲーションの失敗
		- 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の不正なセカンダリ状態
		- HAハートビートなし

© 1997–2026 Citrix Systems, Inc. All rights reserved.

問題カテゴリ	説明	問題
		- HA同期の失敗
		- HAバージョンの不一致
容量の問題	NetScalerの容量の問題を表示します。NetScaler Consoleは、NetScalerインスタンスから5分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンターの増分が存在する場合に表示します。問題は、以下の容量パラメータに基づいて分類されます。	- スループット制限に達しました
		- PE CPU制限に達しました
		- PPS制限に達しました
		- SSLスループットレート制限
		- SSL TPSレート制限
ネットワーク	インスタンスで発生する運用上の問題を表示します。	詳細については、「新しいインジケーターによる強化されたインフラストラクチャ分析」を参照してください。

各タブをクリックして、問題を分析し、トラブルシューティングします。たとえば、選択した期間にインスタンスで次のエラーが発生したとします。

- **Current**タブには、現在インスタンススコアに影響を与えている問題が表示されます。
- 「**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスのキャパシティ問題を表示する

NetScalerインスタンスが利用可能なキャパシティのほとんどを消費すると、クライアントトラフィックの処理中にパケットドロップが発生する可能性があります。この問題は、NetScalerインスタンスのパフォーマンス低下を引き起こします。このようなNetScalerのキャパシティ問題を理解することで、NetScalerのパフォーマンスを安定させるために、追加のライセンスを事前に割り当てることができます。

サークルパックビューでは、NetScalerインスタンスのキャパシティ問題が存在する場合に表示できます。

NetScalerのキャパシティ問題を表示するには、,

1. **インフラストラクチャ > インフラストラクチャ分析**に移動します。
2. サークルパックビューを選択します。

> **注:**
>
> **インフラストラクチャ分析**では、サークルパックビューと表形式ビューに、過去1時間に発生したイベントと問題が表示されます。

次の図は、選択したインスタンスにキャパシティ問題が存在することを示しています。

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されるアクションを表示

NetScaler Console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. **Infrastructure > Infrastructure Analytics**で、表形式ビューを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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-console-service/media/instance-details.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される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されるアクション(/en-us/netscaler-console-service/media/adc-capacity-issues-drill-down.gif)

NetScaler Consoleは、NetScalerインスタンスから5分ごとにこれらのイベントをポーリングし、パケットドロップまたはレート制限カウンターの増分が存在する場合に表示します。

NetScaler Consoleは、定義された容量しきい値に基づいてインスタンススコアを計算します。

- **低しきい値** – 1パケットドロップまたはレート制限カウンターの増分
- **高しきい値** – 10000パケットドロップまたはレート制限カウンターの増分

したがって、NetScalerインスタンスが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、**設定 > 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強化されたインフラストラクチャ分析

NetScaler Console の **インフラストラクチャ分析** を使用すると、次のことができます。

- NetScaler インスタンスで発生する新しい一連の運用上の問題を表示します。
- エラーメッセージを表示し、問題をトラブルシューティングするための推奨事項を確認します。

管理者として、問題の根本原因分析を迅速に特定できます。

注:

ルールインジケーターは、以下ではサポートされていません。

- クラスターモードで構成された NetScaler インスタンス。
- 管理パーティションで構成された NetScaler インスタンス。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console で、**インフラストラクチャ > インフラストラクチャ分析** に移動して、次のインジケーターを表示します。

インフラストラクチャ分析のインジケーター名	説明
ポート割り当ての失敗	NetScaler が SNIP を使用して新しいサーバー接続と通信し、その SNIP で利用可能なポートがすべて使い果たされたときに検出します。推奨されるアクションは、同じサブネットに別の SNIP を追加することです。
セッションの蓄積	NetScalerのメモリがSSLセッションによって占有されていることを検出します。
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ることを検出します。
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かどうかを検出します。
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かどうかを検出します。
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を検出します。NetScalerはこの攻撃をすでに軽減しているため、このアラートは情報提供のみを目的としています。
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	サイト名の不一致が原因で GSLB 構成の同期に失敗した場合に検出します。
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。

© 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
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 キータイプの使用により、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。
レイヤー 2 ループ	ネットワーク内のレイヤー 2 ループの存在を検出します。
タグ付き VLAN の不一致	タグ付き VLAN パケットがタグなしインターフェイスで受信された場合に検出します。

表形式ビュー

Infrastructure Analytics の表形式ビューオプションを使用して、異常を表示することもできます。**Infrastructure > Infrastructure Analytics** に移動し、

をクリックして、すべての管理対象インスタンスを表示します。

をクリックして詳細を展開します。

異常の詳細を表示

たとえば、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アドレスの競合に対して表示されている異常をクリックします。

- **詳細** - 検出された異常を示します
- **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トラブルシューティング手順を示します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンス管理

インスタンスとは、NetScaler Console を使用して管理、監視、トラブルシューティングできる Citrix 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 Console に追加します。インスタンスは、NetScaler Console のセットアップ時、または後で追加できます。インスタンスを NetScaler Console に追加すると、継続的にポーリングされ、後で問題の解決やレポートデータとして使用できる情報が収集されます。

インスタンスは、静的グループまたはプライベート IP ブロックとしてグループ化できます。インスタンスの静的グループは、構成ジョブなどの特定のタスクを実行する場合に役立ちます。プライベート IP ブロックは、地理的な場所に基づいてインスタンスをグループ化します。

インスタンスを追加する

インスタンスは、NetScaler Console サーバーを初めてセットアップするとき、または後で追加できます。インスタンスを追加するには、各 NetScaler インスタンスのホスト名または IP アドレス、あるいは IP アドレスの範囲を指定する必要があります。

NetScaler Console にインスタンスを追加する方法については、「NetScaler Console へのインスタンスの追加」を参照してください。

インスタンスを NetScaler Console サーバーに追加すると、サーバーは暗黙的に自身をインスタンスのトラップ宛先として追加し、インスタンスのインベントリを収集します。詳細については、「NetScaler Console がインスタンスを検出する方法」を参照してください。

インスタンスを追加した後、 > に移動し、インスタンスカテゴリを選択して削除できます。次に、削除するインスタンスを選択し、 をクリックします。

インスタンスダッシュボードの使用方法

NetScaler Console のインスタンスごとのダッシュボードには、選択したインスタンスのデータが表形式とグラフ形式で表示されます。ポーリングプロセス中にインスタンスから収集されたデータがダッシュボードに表示されます。

デフォルトでは、管理対象インスタンスは毎分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 呼び出しを使用して継続的に収集されます。管理者は、収集されたすべてのデータを単一のページで表示し、インスタンスの問題を特定し、それらを修正するための即時アクションを実行できます。

特定のインスタンスのダッシュボードを表示するには、 > > に移動します。NetScaler ページで、インスタンスタイプを選択し、表示するインスタンスを選択して をクリックします。

© 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、担当者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の 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 および 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。
- **ネットワーク機能**。ネットワーク機能ダッシュボードを使用すると、選択したNetScalerインスタンスに構成されているエンティティの状態を監視できます。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する仮想サーバーのグラフを表示できます。
- **ネットワーク使用状況**。ネットワーク使用状況タブで、選択したインスタンスのネットワークパフォーマンスデータを表示できます。1時間、1日、1週間、または1か月間のレポートを表示できます。タイムラインスライダー機能を使用して、生成されるネットワークレポートの期間をカスタマイズできます。デフォルトでは8つのレポートのみが表示されますが、画面右下隅にある「プラス」アイコンをクリックすると、別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方法

ネットワーク管理者として、地理的に分散された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正確に把握することは容易ではありません。

NetScaler Consoleのジオマップは、サイトのグラフィカルな表示を提供し、地理別にネットワーク監視エクスペリエンスを分類します。ジオマップを使用すると、場所別にネットワークインスタンスの分布を視覚化し、ネットワークの問題を監視できます。

以下のセクションでは、NetScaler Consoleでデータセンターを監視する方法について説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleでのグローバルに分散されたサイトの監視

NetScaler Consoleサイトは、特定の地理的場所にあるCitrix Application Delivery Controller (NetScaler) インスタンスの論理的なグループ化です。たとえば、あるサイトがAmazon Web Services (AWS) に割り当てられ、別のサイトがAzureに割り当てられる場合があります。さらに別のサイトは、テナントのオンプレミスでホストされます。NetScaler Consoleは、すべてのサイトに接続されているすべてのNetScalerインスタンスを管理および監視します。NetScaler Consoleを使用して、管理対象インスタンスから発生するsyslog、AppFlow、SNMP、およびその他のデータを監視および収集できます。

NetScaler Consoleのジオマップは、サイトのグラフィカルな表示を提供します。ジオマップは、地理別にネットワーク監視エクスペリエンスを分類します。ジオマップを使用すると、場所別にネットワークインスタンスの分布を視覚化し、すべてのネットワークの問題を監視できます。メニューの**Infrastructure**をクリックすると、世界地図上に作成されたサイトの視覚的な表示として**Instances Dashboard**が表示されます。

ユースケース

大手携帯電話会社であるExampleCompanyは、リソースとアプリケーションのホスティングをプライベートサービスプロバイダーに依存していました。同社はすでに2つのサイトを持っていました。1つは米国のミネアポリスに、もう1つはオーストラリアのアリススプリングスにあります。この画像では、2つのマーカーが既存の2つのサイトを表していることがわかります。

サイトマーカー(/en-us/netscaler-console-service/media/nmaservice-global-datacenters-1.png)

マーカーは、サイト上の以下のコンポーネントの数も表示します。

- **インスタンス**: 利用可能なインスタンスの数を示します。
- **アプリケーション**: ホストされているアプリケーションの数を示します。
- **仮想サーバー**: 利用可能な仮想サーバーの数を示します。
- **重大なイベント**: インスタンスで発生した重大なイベントの数を示します。
- **主要イベント**: インスタンスで発生した主要イベントの数を示します。

サイトコンポーネントの図(/en-us/netscaler-console-service/media/nmaservice-global-datacenters-2.png)

Applications をクリックして、各サイトで作成されたすべてのカスタムアプリケーションを表示します。

Details をクリックして、各サイトに追加されたNetScalerインスタンスのリストを表示します。詳細を表示するには、タブをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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
  - NetScalerインスタンスのタイプ
  - 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イベントと重要なイベントのリストを表示します。
- **証明書** タブ: このタブで以下を表示します。
  - すべてのインスタンスの証明書のリスト
  - 有効期限ステータス
  - 重要な情報と、使用中の証明書数による上位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。

Geomap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を決定しました。

管理者として、まずサイトを作成し、次にNetScaler ConsoleにNetScalerインスタンスを追加する必要があります。また、インスタンスをサイトに追加し、エージェントを追加して、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。そうすると、NetScaler ConsoleはNetScalerインスタンスとエージェントが属するサイトを認識します。

NetScalerインスタンスの追加の詳細については、「インスタンスの追加」を参照してください。

サイトの作成

NetScaler Consoleでインスタンスを追加する前にサイトを作成します。ロケーション情報を提供することで、サイトを正確に特定できます。

サイトを作成するには：

1. **Infrastructure > Instances > Site**に移動します。「**Add**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Select Cloud**タブで、**Site type**を選択します。**Data Center**または**Branch**タイプのサイトを作成できます。

   Data Centerサイトタイプの場合は、リストから**Type**を選択します。

   - プライベート
   - AWS
   - Azure (アジュール)
   - グーグルクラウド
   - ヴイエムウェア ブイセンター

3. 「**次へ**」をクリックします。
4. 「**リージョンの選択**」タブで、次の詳細を入力します。

   - サイト名
   - 市区町村
   - 郵便番号
   - リージョン
   - 国
   - 緯度
   - 経度

   または、**場所を検索**に場所を入力し、**場所を取得**をクリックしてサイトを正確に特定できます。市区町村、郵便番号、リージョン、国、緯度、経度の各フィールドが自動的に入力されます。

5. 「**完了**」をクリックします。

注記:

概説されている手順は、以下に適用されます。

- ブランチサイトタイプ。
- プライベートタイプのデータセンターサイトタイプ。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- クラウドプロバイダータイプでフェッチオプションが選択されていない場合。

クラウドプロバイダータイプのサイトを作成する

クラウドプロバイダータイプでサイトを作成し、**フェッチ**オプションを有効または無効にするかを選択できます。デフォルトでは、**フェッチ**オプションは選択されていません。

フェッチオプションは、AWS、Azure、Google Cloudプラットフォームでのみ利用可能です。

特定のクラウドプロバイダー向けにサイトを作成するための詳細な手順については、以下のセクションを参照してください。

1. AWSでサイトを作成する
2. Azureでサイトを作成する
3. Google Cloudでサイトを作成する
4. VMware vCenterでサイトを作成する

サイトを編集する

既存のサイトを変更するには：

1. サイトを選択し、**編集**をクリックします。
2. **サイトの構成**ページで、**サイトの種類**を更新できます。たとえば、以前に**ブランチ**を選択していた場合、**データセンター**に更新できます。
3. サイトの種類に応じて、**種類**を変更できます。たとえば、リストから種類をプライベートデータセンターからパブリッククラウドに変更できます。

サイトを削除する

1. サイトを削除するには、サイトを選択し、**削除**をクリックします。
2. 確認ページで、**はい**をクリックします。

インスタンスを追加してサイトを選択するには：

サイトを作成したら、NetScaler Consoleにインスタンスを追加する必要があります。以前に作成したサイトを選択することも、サイトを作成してインスタンスを関連付けることもできます。

1. NetScaler Consoleで、**インフラストラクチャ > インスタンス > NetScaler**に移動します。
2. **VPX**を選択し、**追加**をクリックします。
3. **NetScaler VPXの追加**ページで、IPアドレスを入力し、リストからプロファイルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. リストからサイトを選択します。**サイト**フィールドの横にある**追加**ボタンをクリックしてサイトを作成するか、**編集**ボタ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-console-service/media/nmaservice-global-datacenters-5.png)
6. エージェントを選択したら、そのエージェントをサイトに関連付ける必要があります。この手順により、エージェントをサイトにバインドできます。エージェントを選択し、**Attach Site** をクリックします。

   エージェントをサイトに関連付ける(/en-us/netscaler-console-service/media/nmaservice-global-datacenters-6.png)

   a. リストからサイトを選択し、**Save** をクリックします。
7. オプションで、**Tags** のキーと値のフィールドを入力できます。
8. **OK** をクリックします。

また、**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。

エージェントをサイトに関連付けるには:

1. NetScaler Console で、**Infrastructure > Instances > Agents** に移動します。
2. エージェントを選択し、**Attach Site** をクリックします。
3. サイトを関連付けて、**Save** をクリックします。

NetScaler Console は、バンガロールサイトに追加された NetScaler インスタンスと、他の2つのサイトのインスタンスも監視し始めます。

このダッシュボードのレポートをエクスポートするには:

このページのレポートをエクスポートするには、このページの右上にある **Export** アイコンをクリックします。**Export** ページで、次のいずれかを実行できます。

1. **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。
2. **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。

© 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。
- 「**毎月**の繰り返し」を選択した場合は、レポートをスケジュールするすべての日をコンマで区切って入力してください。

タグを作成してインスタンスに割り当てる方法

NetScaler Consoleでは、NetScalerインスタンスにタグを関連付けることができるようになりました。タグは、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**: 英国にある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、英国にあるすべてのインスタンスを検索および監視するのに役立ちます。
- **ユースケース 2**: ステージング環境にあるインスタンスを検索したいとします。ここでは、キーを「Purpose」、値を「Staging_NS」とするタグを作成できます。このタグは、ステージング環境で使用されているすべてのインスタンスを、クライアントリクエストが実行されているインスタンスから分離するのに役立ちます。
- **ユースケース 3**: 英国のスウィンドン地域にあり、David T.が所有するNetScalerインスタンスのリストを見つけたい状況を考えてみましょう。これらすべての要件に対してタグを作成し、これらの条件を満たすすべてのインスタンスに割り当てることができます。

NetScaler VPXインスタンスにタグを割り当てるには:

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler**に移動します。
2. **VPX**タブを選択します。
3. 必要なVPXインスタンスを選択します。
4. **タグ**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、次の画像は、作成されたいくつかのキーワードとその値を示しています。独自のキーワードを追加し、各キーワードに値を入力できます。

キーと値の画像(/en-us/netscaler-console-service/media/instance-tags.png)

キーと値の画像-2(/en-us/netscaler-console-service/media/instance-tags-example1.png)

「+」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。

- カンマで区切ることで、キーワードに複数の値を追加できます。

  たとえば、管理者の役割を同僚のGreg T.に割り当てるとします。彼の名前をカンマで区切って追加できます。複数の名前を追加すると、いずれかの名前または両方の名前で検索するのに役立ちます。NetScaler Consoleは、カンマで区切られた値を2つの異なる値として認識します。

- タグに基づいてインスタンスを検索する方法の詳細については、タグとプロパティの値を使用してインスタンスを検索する方法を参照してください。

5. **OK**をクリックします。

> **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。作成するタグの数に制限はありません。

タグとプロパティの値を使用してインスタンスを検索する方法

NetScaler Consoleが多数のNetScalerインスタンスを管理している状況があるかもしれません。管理者として、特定のパラメータに基づいてインスタンスインベントリを検索する柔軟性を求めるかもしれません。NetScaler Consoleは現在、検索フィールドで定義したパラメータに基づいてNetScalerインスタンスのサブセットを検索するための改善された検索機能を提供しています。インスタンスは、タグとプロパティという2つの基準に基づいて検索できます。

- **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、ユーザーがNetScalerインスタンスに割り当てることができる用語またはキーワードです。NetScalerインスタンスにタグを関連付けることができるようになりました。これらのタグは、NetScalerインスタンスをより適切に識別し、検索するために使用できます。
- **プロパティ**。NetScaler Consoleに追加された各NetScalerインスタンスには、そのインスタンスに関連付けられたいくつかのデフォルトパラメータまたはプロパティがあります。たとえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、あなたが所有するインスタンスも検索できます。「Owner」タグを作成し、そのタグに「David T」という値を割り当てることができます。タグの作成と割り当て方法の詳細については、「タグを作成してインスタンスに割り当てる方法」を参照してください。

タグとプロパティを組み合わせて、独自の検索条件を作成できます。

NetScaler VPXインスタンスを検索するには

1. NetScaler Consoleで、**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**タブを選択します。
3. 検索フィールドをクリックします。タグまたはプロパティを使用するか、両方を組み合わせて検索式を作成できます。

   次の例は、検索式を効率的に使用してインスタンスを検索する方法を示しています。

   a. **タグ**オプションを選択し、**所有者**を選択します。「David T」を選択します。

   NetScaler Consoleは、検索式で正規表現とワイルドカード文字をサポートしています。

   a. 検索条件をさらに拡張するために、正規表現を使用できます。たとえば、DavidまたはStephen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、値は「\|」式で区切って入力できます。

      所有者タグ(/en-us/netscaler-console-service/media/instance-search-tags-properties-3.png)

   b. 1つ以上の文字を置き換えたり表現したりするために、ワイルドカード文字を使用することもできます。たとえば、「David」と「Dave P」が所有するすべてのインスタンスを検索するには、`Dav*`と入力します。

      正規表現とワイルドカード文字(/en-us/netscaler-console-service/media/instance-search-tags-properties-4.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

正規表現とワイルドカード文字、およびそれらの使用方法の詳細については、検索バーの「情報」アイコンをクリックしてください。

NetScaler® Console を介した GeoIP DB の一元的な更新

NetScaler Console を使用すると、管理者は MaxMind から GeoIP DB (地理位置情報データベース) ファイルを NetScaler Console 経由で直接アップロードできます。GeoIP DB ファイルを管理対象の NetScaler インスタンスにすぐにプッシュするか、後で更新をスケジュールすることができます。これらのファイルは、GSLB やセキュリティポリシーで一般的に使用される、正確な IP-場所マッピングに不可欠です。

この機能強化により、更新履歴の追跡も可能になり、更新が成功したか失敗したかを確認できます。また、以前にアップロードまたはプッシュされた GeoIP DB バージョンを NetScaler Console から表示、削除、またはダウンロードできます。この機能強化により、NetScaler Console での GeoIP DB ファイルの手動更新、バージョン管理、および自動更新ワークフローも導入され、GSLB サービスに影響を与えることなくシームレスな GeoIP DB 更新が可能になります。

以前は、NetScaler には NetScaler 上で GeoIP DB 更新を管理するための一元的なメカニズムがありませんでした。管理者は各デバイスで手動で更新を実行する必要があり、これは時間と手間がかかり、エラーが発生しやすく、本番環境では中断を伴うものでした。

この機能強化には、次の利点があります。

- **自動化**: 更新プロセスは自動化されており、計画されたダウンタイムなしで実行されるため、運用上のオーバーヘッドが削減されます。
- **効果的なスケーラビリティ**: 複数の NetScaler インスタンスにわたる更新の管理は効率的で、簡単に拡張できます。
- **バージョン管理**: 問題が発生した場合、履歴バージョンを追跡し、古い GeoIP DB ファイルをアップロードして同期できます。

制限事項

- **MaxMind に限定された形式変換のサポート**: 自動形式変換は MaxMind ファイルのみでサポートされています。他のベンダーの場合、ファイルはすでにサポートされている形式である必要があります。
- **削除の制限**: アクティブに使用中のファイルを削除することはできません。削除する前に、アクティブな依存関係がないことを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console を介した GeoIP DB の一元的な更新の構成

前提条件

- GeoIP DB ファイルを使用するために必要な有効な MaxMind ライセンスがあることを確認してください。
- 他のベンダーのファイル形式を使用している場合は、ファイルがサポートされている形式であることを確認してください。

MaxMindまたはその他のベンダーからGeoIP DBファイルをアップロードするには、次の手順を実行します。

1. **Infrastructure > GeoIP DB Sync** に移動し、**Get Started** をクリックします。

2. 次のいずれかのオプションを選択します。

   - **Local**: ローカルシステムからファイルをアップロードできます。
   - **Appliance**: NetScaler Consoleに既に存在するファイルを選択できます。

   注記:

   - GeoIP DBファイルを初めてアップロードする場合、**Appliance** オプションは表示されません。ファイルが既にアップロードされている場合にのみ、その後のアップロード時に **Appliance** オプションが表示されます。
   - MaxMindファイルをアップロードすると、NetScaler Consoleサービスはアップロード中にファイルをNetScalerが推奨する形式に自動的に変換します。他のプロバイダーからファイルをアップロードする場合、そのファイルはCSV形式である必要があり、NetScalerが推奨する次のフィールド順序（IP範囲、国コード、地域、都市）に従う必要があります。

3. ファイルをアップロードした後、次のいずれかのアクションを選択します。

   - **Sync Now:** 同期設定ダイアログにすぐに進みます。
   - **Create Schedule:** ターゲットエンティティにファイルを展開する将来の日付と時刻を選択します。

4. **Sync Now** をクリックした場合、次のいずれかの展開モードを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Sync all:** GeoIP DBファイルをすべてのNetScalerインスタンス、エージェント、およびNetScaler Consoleに自動的に配布します。
- **カスタマイズ:** ターゲットを手動で選択します。
  - **NetScaler Consoleを選択:** 現在ログインしているNetScaler Consoleを表示します。
  - **NetScalerインスタンスを選択:** グループドロップダウンメニューまたはキー:値検索を使用して、特定のインスタンスをフィルタリングして識別します。
  - **エージェントを選択:** 利用可能なエージェントのリストを表示します。

同期開始をクリックする前に、プロンプトに答えてください: *「現在のファイルにはIPv6が含まれていますか？」*。GeoIPファイルにIPv6アドレスブロックが含まれている場合に*のみ*、**はい**を選択してください。この設定は、各ターゲットエンティティがデータを解析する方法を決定します。

5. **GeoIP DB同期**ページで進行状況と結果を監視します。**最終同期概要**パネルには、次のメトリックが表示されます。
   - **選択されたエンティティの合計:** ターゲットとなるすべてのNetScaler Consoleインスタンスとエージェントの合計数。
   - **同期保留中:** キューに入れられているが、まだ開始されていないエンティティ。
   - **同期進行中:** ファイルをアクティブに受信しているエンティティ。
   - **同期成功:** エラーなしで完了したエンティティ。
   - **同期失敗:** エラーが発生したエンティティ。
   - **全体的な同期完了率:** 正常に完了した選択されたエンティティの割合。

   エンティティ別同期ステータスを展開して、IPアドレス、ホスト名、タイプ、状態、バージョン、同期ステータスを一覧表示するデバイスごとのテーブルを表示します。フィルターバーを使用して、任意のフィールド（例: **同期ステータス: 完了**）で結果を絞り込みます。

6. 要件に基づいて、**GeoIP DB同期**ページから次のいずれかのアクションを実行します。
   - **新しいファイルを選択:** ローカルシステムからGeoIP DBファイルをアップロードするか、NetScaler Consoleからすでにアップロードされているファイルを選択します。
   - **ファイル情報を表示:** 以前にアップロードされたファイルを確認します。問題が発生した場合は、過去のバージョンを追跡し、古いGeoIP DBファイルをアップロードして同期できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アクティブなスケジュール:** まだ実行されていない、今後のスケジュールされた同期ジョブを表示します。
- **履歴スケジュール:** 完了したGeoIP DB同期操作を表示します。各エントリには、エンティティスコープ（例：**2つのNetScalerインスタンス、1つのエージェント、およびNetScaler Console**）、実行タイムスタンプ、および使用されたGeoIPファイルが表示されます。任意のエントリをクリックすると、NetScaler Consoleインスタンスとエージェントごとの同期結果（ステータス、開始時刻、終了時刻）を含むジョブの詳細全体が表示されます。

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 (NetScaler) インスタンスで管理パーティションを設定できます。これにより、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に、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割り当てることができます。

NetScaler Consoleは、管理者が所有するすべてのパーティションを単一のコンソールからシームレスに管理する方法を提供します。これらのパーティションは、他のパーティション設定を中断することなく管理できます。

複数のユーザーが異なる管理パーティションを管理できるようにするには、グループを作成し、それらのグループにユーザーとパーティションを割り当てる必要があります。グループまたはユーザーの作成の詳細については、およびを参照してください。

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。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ている管理パーティションがシステムに自動的に追加されます。各管理パーティションは、NetScaler Consoleのインスタンスとして扱われます。

管理パーティションを表示する

2つのNetScaler VPXインスタンスがあり、各インスタンスに2つの管理パーティションが構成されているとします。たとえば、NetScalerインスタンス10.xx.xx.100にはpartition-1とpartition-2があり、10.xx.xx.101インスタンスにはfirst-partitionとsecond-partitionがあります。

管理パーティションを表示するには、次の手順を実行します。

1. **Infrastructure > Instances > NetScaler** に移動します。
2. **VPX** タブで、**Partitions** をクリックします。

たとえば、次の条件でグループを作成する場合：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **設定 > ユーザーとロール > グループの作成 > 承認設定 > インスタンスの選択** で、「10.xx.xx.100-partition-1」と「10.xx.xx.101-first-partition」インスタンスを選択します。
- 「User1」をグループに割り当てます。

User1は、グループに追加されたパーティションのみを表示および管理できます。ただし、グループに追加されていないパーティションは、同じインスタンスに属していても、ユーザーに対して制限されます。

この例では、10.xx.xx.100-partition-2と10.xx.xx.101-second-partitionは、ユーザーが割り当てられているグループにインスタンスが追加されていないため、制限されています。

別のユーザーに管理者パーティション 10.xx.xx.100-partition-2 と 10.xx.xx.101-second-partition を管理させたい場合は、次の条件でグループを作成します。

- 「**Authorization Settings**」タブで、10.xx.xx.100-partition-2 および 10.xx.xx.101-second-partition インスタンスを選択します。
- 必要なユーザーをグループに割り当てます。

このグループにより、割り当てられたユーザーは選択した管理者パーティションを表示および管理できます。

リビジョン履歴の差分を表示する

管理者パーティションの**リビジョン履歴の差分**を使用すると、パーティション化されたNetScalerインスタンスの最新の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/保存済みの構成と構成リビジョンを比較したりできます。構成の差分に加えて、修正構成も表示されます。すべての修正コマンドをローカルフォルダにエクスポートして、構成を修正できます。

リビジョン履歴の差分を表示するには：

1. **Infrastructure > Configuration > Configuration Audit** に移動します。Configuration Audit ダッシュボードにはさまざまなレポートが表示されます。ドーナツチャートの中央に表示されている数字をクリックします。

2. パーティション化されたNetScalerインスタンスを選択します。
3. 「Action」ボックスから、「**Revision History Diff**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**Revision History Diff**」ページで、比較したいファイルを選択します。たとえば、「Saved Configuration」と「Configuration Revision-2」を比較し、「**Show configuration difference**」をクリックします。

   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表示できます。以下は、5つの保存済み構成を持つ管理者パーティションの例です。

   修正構成コマンドを表示し、これらの修正コマンドをローカルフォルダーにエクスポートすることもできます。これらの修正コマンドは、構成を目的の状態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（比較に使用されている構成ファイル）。

管理者パーティションとインスタンスに保存されている構成は異なります。次の例では、10.xx.xx.20インスタンスには5つの保存された構成があり、このインスタンスの管理者パーティションには3つの異なる保存された構成があります。

テンプレートと実行中の差分を表示する

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。構成の差分に加えて、修正構成も表示されます。すべての修正コマンドをローカルフォルダーにエクスポートして、構成を修正することもできます。

1. **Infrastructure > Configuration > Configuration Audit**に移動します。構成監査ダッシュボードには、さまざまなレポートが表示されます。ドーナツチャートの中央に表示されている数字をクリックします。

2. **監査レポート**ページで、「テンプレートと実行中の差分」列の下にある**差分が存在**ハイパーリンクをクリックします。

   監査テンプレートと実行中の構成の間に差分がある場合、その差分はハイパーリンクとして表示されます。差分がある場合は、ハイパーリンクをクリックして差分を表示します。構成の差分に加えて、修正構成も表示されます。すべての修正コマンドをローカルフォルダーにエクスポートして、構成を修正することもできます。

このダッシュボードのレポートをエクスポートするには:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このページのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページで、次のいずれかを実行できます。

1. **今すぐエクスポート**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。
2. **エクスポートのスケジュール**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。

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するようにしてください。
- 「**毎月**の繰り返し」を選択した場合は、レポートをスケジュールするすべての日をコンマで区切って入力するようにしてください。

NetScalerインスタンスのバックアップと復元

Citrix Application Delivery Controller (NetScaler) インスタンスの現在の状態をバックアップし、後でバックアップファイルを使用してNetScalerインスタンスを同じ状態に復元できます。インスタンスをアップグレードする前、または予防措置として、常にインスタンスをバックアップする必要があります。安定したシステムのバックアップがあれば、不安定になった場合に安定した時点に復元できます。NetScalerインスタンスでバックアップと復元を実行する方法は複数あります。GUI、CLIを使用してNetScaler構成を手動でバックアップおよび復元することも、NetScaler Consoleを使用して自動バックアップと手動復元を実行することもできます。NetScaler Consoleは、NITROコールとSecure Shell (SSH) およびSecure Copy (SCP) プロトコルを使用して、管理対象のNetScalerインスタンスの現在の状態をバックアップします。

NetScaler Consoleは、以下のNetScalerインスタンスタイプの完全なバックアップを作成し、復元します。

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

詳細については、「NetScalerインスタンスのバックアップと復元」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

- NetScaler Console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/tenants/<specify-the-tenant-name>/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最大3つのバックアップファイルを保存できます。

NetScalerインスタンスをバックアップおよび復元するには、まずNetScaler Consoleでバックアップ設定を構成する必要があります。設定を構成した後、単一のNetScalerインスタンスまたは複数のインスタンスを選択し、これらのインスタンス内の構成ファイルのバックアップを作成できます。必要に応じて、これらのバックアップファイルを使用してNetScalerインスタンスを復元することもできます。

NetScaler Consoleを使用して、選択したNetScalerインスタンスのバックアップを作成する

選択したNetScalerインスタンスまたは複数のインスタンスをバックアップする場合は、このタスクを実行します。

1. NetScaler Consoleで、**Infrastructure > Instances**に移動します。**Instances**の下で、画面に表示するインスタンスのタイプ（例：VPX）を選択します。
2. バックアップするインスタンスを選択します。
   - MPX、VPX、およびBLXインスタンスの場合は、**Select Action**リストから**Backup/Restore**を選択します。
   - SDXインスタンスの場合は、**Backup/Restore**をクリックします。
3. **Backup Files**ページで、**Back Up**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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します。パスワードを入力するか、以前にInstance Backup Settingsページで指定したグローバルパスワードを使用できます。
5. **Continue**をクリックします。

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、まずバックアップファイルをNetScaler Consoleサーバーにアップロードしてから、復元操作を実行する必要があります。

NetScaler Consoleバックアップファイルを転送するには：

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**Backup/Restore**を選択します。
3. バックアップファイルを選択し、**Transfer**をクリックします。

   Transfer Backup Fileページが表示されます。次のパラメータを指定します。

   a. **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。
   b. **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。
   c. **ポート** – ファイルが転送されるシステムのポート番号。
   d. **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。
   e. **ディレクトリパス** – バックアップファイルが新しいシステムに転送される場所。
   f. 「**OK**」をクリックします。

注：

NetScaler Consoleサービスからのバックアップファイルは、エージェントを介して外部サーバーに送信されます。多数のエージェントがある場合、NetScalerバックアップファイルは、そのNetScalerインスタンスを追加するために使用されたのと同じエージェントを介して送信されます。エージェントに関連付けられているインスタンスの詳細については、「**Infrastructure > NetScaler > Agents**」に移動してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleを使用してNetScalerインスタンスを復元する

注：

HAペアにNetScalerインスタンスがある場合は、次の点に注意する必要があります。

- バックアップファイルが作成されたのと同じインスタンスを復元します。たとえば、HAペアのプライマリインスタンスからバックアップが取得されたシナリオを考えてみましょう。復元プロセス中に、たとえそれがプライマリインスタンスでなくなったとしても、同じインスタンスを復元していることを確認してください。
- プライマリNetScalerインスタンスで復元プロセスを開始すると、プライマリインスタンスにアクセスできなくなり、セカンダリインスタンスは**STAYSECONDARY**に変更されます。プライマリインスタンスでの復元プロセスが完了すると、セカンダリNetScalerインスタンスは**STAYSECONDARY**から**ENABLED**モードに変わり、再びHAペアの一部になります。復元プロセスが完了するまで、プライマリインスタンスでダウンタイムが発生する可能性があります。

以前に作成したバックアップファイルを使用してNetScalerインスタンスを復元するには、このタスクを実行します。

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、復元する設定を含むバックアップファイルを選択し、**Restore** をクリックします。

注:

外部から転送されたバックアップファイルをアップロードするには、**Upload** ボタンを使用します。

NetScaler Console を使用して NetScaler SDX アプライアンスを復元する

NetScaler Console では、NetScaler SDX アプライアンスのバックアップには以下が含まれます。

- 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 証明書のポーリング設定 (XML 形式)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SVM db ファイル
- SDX 上に存在するデバイスの NetScaler 設定ファイル
- 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する必要があります。アプライアンスの復元中に、現在の構成全体が削除されます。

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、復元プロセスを開始する前に、ライセンスを追加し、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内の設定と一致するように構成してください。

バックアップされたNetScaler SDXプラットフォームバリアントが、復元しようとしているものと同じであることを確認してください。異なるプラットフォームバリアントから復元することはできません。

注:

SDX RMAアプライアンスを復元する前に、バックアップされたバージョンがRMAバージョンと同じか、それ以降であることを確認してください。

バックアップファイルからSDXアプライアンスを復元するには：

1. NetScaler Console GUIで、**Infrastructure > Instances > NetScaler** 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。そのため、SDXアプライアンスを復元する前に、バックアップファイルを再パッケージ化する必要があります。

   バックアップファイルを再パッケージ化すると、SDXアプライアンスを復元するためにすべてのバックアップファイルがまとめられます。再パッケージ化されたバックアップファイルは、SDXアプライアンスの正常な復元を保証します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

このダッシュボードのレポートをエクスポートする

このページのレポートをエクスポートするには、このページの右上にある「**エクスポート**」アイコンをクリックします。「**エクスポート**」ページで、次のいずれかを実行できます。

1. 「**今すぐエクスポート**」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するには。
2. 「**エクスポートをスケジュール**」タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、メールまたはSlackメッセージでレポートを送信するには。

注意

- 「**毎週**」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**」の繰り返しを選択した場合、レポートをスケジュールしたい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。

セカンダリNetScalerインスタンスへのフェールオーバーを強制する

たとえば、プライマリCitrix Application Delivery Controller (NetScaler) インスタンスを交換またはアップグレードする必要がある場合、フェールオーバーを強制したいことがあります。プライマリインスタンスまたはセカンダリインスタンスのいずれかからフェールオーバーを強制できます。プライマリインスタンスでフェールオーバーを強制すると、プライマリがセカンダリになり、セカンダリがプライマリになります。強制フェールオーバーは、プライマリインスタンスがセカンダリインスタンスがUPであることを判断できる場合にのみ可能です。

強制フェールオーバーは伝播または同期されません。強制フェールオーバー後の同期ステータスを表示するには、インスタンスのステータスを表示できます。

強制フェールオーバーは、次のいずれかの状況で失敗します。

- スタンドアロンシステムでフェールオーバーを強制する。
- セカンダリインスタンスが無効または非アクティブである。セカンダリインスタンスが非アクティブ状態の場合、フェールオーバーを強制するには、その状態がUPになるまで待つ必要があります。
- セカンダリインスタンスがセカンダリのままになるように構成されている。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

強制フェールオーバーコマンドを実行したときに潜在的な問題が検出された場合、NetScalerインスタンスは警告メッセージを表示します。メッセージには、警告をトリガーした情報が含まれており、続行する前に確認を求めます。

プライマリインスタンスまたはセカンダリインスタンスでフェールオーバーを強制できます。

NetScaler Consoleを使用してセカンダリNetScalerインスタンスへのフェールオーバーを強制するには：

1. NetScaler Consoleで、**Infrastructure > Instances** に移動します。**VPX** タブに移動し、インスタンスを選択します。
2. 選択したインスタンスタイプの下にリストされているインスタンスから、HAセットアップのインスタンスを選択します。
3. **Action** ボックスから、**Force Failover** を選択します。
4. 強制フェールオーバーアクションを確認するには、**Yes** をクリックします。

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

高可用性 (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。

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なく、プライマリノードで障害が検出された場合でもセカンダリノードのままであってほしいとします。

セカンダリノードをセカンダリのままにするように強制すると、プライマリノードがダウンしてもセカンダリのままになります。また、HAペア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は参加しません。ノードのステータスはSTAYSECONDARYと表示されます。

注

システムをセカンダリのままにするように強制しても、強制プロセスは伝播または同期されません。コマンドを実行したノードのみに影響します。

NetScaler Consoleを使用してセカンダリNetScalerインスタンスをセカンダリのままにするように設定するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**インフラストラクチャ > インスタンス**に移動し、インスタンスタイプ (VPX) の下の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. **アクション**ボックスから、**セカンダリのままにする**を選択します。
4. **はい**をクリックして、「セカンダリのままにする」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 Consoleに追加する必要があります。インスタンスを正常に追加したら、インスタンスファミリーに基づいてインスタンスグループを作成します。インスタンスのグループを作成すると、グループ化されたインスタンスに対して一度にアップグレード、バックアップ、または復元を行うことができます。

インスタンスビューを使用すると、すべての管理対象インスタンスとそれに関連付けられたグループを表示できるため、マッピングされていないインスタンスを簡単に識別できます。マッピングされていないインスタンスをグループに割り当てることができます。

NetScaler Consoleを使用してインスタンスグループを作成するには

1. NetScaler Consoleで、**インフラストラクチャ > インスタンス > インスタンスグループ**に移動し、**追加**をクリックします。
2. インスタンスグループに名前を指定し、**インスタンスファミリー**リストから**NetScaler**を選択します。
3. **カテゴリ**で、**デフォルト**オプションを選択します。
4. **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、グループ化するインスタンスを選択し、**選択**をクリックします。

   テーブルには、選択されたインスタンスとその詳細が一覧表示されます。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、**削除**をクリックします。
5. **作成**をクリックします。

マッピングされていないインスタンスを識別してグループに追加するには

1. **インフラストラクチャ > インスタンス > インスタンスグループ > インスタンスビュー**に移動します。
2. 1つまたは複数のマッピングされていないインスタンスを選択します。
3. **インスタンスグループの追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. リストから必要な**インスタンスグループ**を選択します。インターフェイスには以下も表示されます。

   - 利用可能なインスタンスグループ。
   - 各グループにすでにマッピングされているインスタンス。これにより、重複または誤った割り当てを防ぐことができます。

5. **保存**をクリックします。選択したインスタンスは、選択したグループに割り当てられます。

グローバルサーバー負荷分散サイトグループ

ADCインスタンスの継続的な可用性と災害復旧を確保したい場合は、GSLBサイトグループを設定できます。これにより、クライアント要求を最も近いサイトまたは最もパフォーマンスの高いサイトに、あるいは障害発生時には稼働中のサイトに誘導することで、サイト間の負荷を分散します。

GSLBサイトグループでは、ADCインスタンスの設定オブジェクトが互いに上書きしようとすることがあります。これは競合状態につながります。このような問題に対処するには、GSLBサイトグループでのプライマリノードの選択を制御する必要があります。プライマリノードの設定は、残りのADCインスタンスに適用されます。NetScaler Consoleでは、GSLBサイトグループを作成し、次の操作を実行できます。

- 選択したADCインスタンスの中からプライマリノードを選択します。
- 選択したプライマリノードがダウンした場合に備えて、プライマリノード選択の優先順位を設定します。

GSLBサイトグループは、**インフラストラクチャ > インスタンス > GSLBサイトグループ**で表示できます。

GSLBサイトグループを作成する

ADCインスタンスを含むGSLBサイトグループを作成するには、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 > GSLBサイトグループ**に移動します。
2. **追加**をクリックします。
3. GSLBサイトグループの名前を指定します。
4. GSLBサイトグループに追加するインスタンスを選択します。これらのインスタンスは、グループ内のサイトとして機能します。
5. 少なくとも1つのサイトを選択し、**アクティブサイトにする**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

優先度 `1` に設定されたインスタンスがプライマリノードになります。アクティブサイトの優先順位を並べ替えることができます。優先順位の低いインスタンスを選択し、**優先順位を上げる**をクリックします。

6. **作成**をクリックします。

Infrastructure > Network Functions > GSLB で、GUIはGSLBサイトグループのプライマリADCノードからのエンティティのみを表示します。

NetScalerエージェント用の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、要求されたデータを管理情報ベース (MIB) で検索し、そのデータをSNMPマネージャーに送信します。

NetScalerエージェントに照会するためにSNMPマネージャーを追加できます。マネージャーはSNMP V2およびV3に準拠しています。1つ以上のSNMPマネージャーを指定した場合、NetScalerエージェントは指定されたSNMPマネージャー以外のホストからのSNMPクエリを受け入れません。

SNMP v2マネージャーを追加する

NetScalerエージェント用のSNMP v2マネージャーを追加するには：

1. **Infrastructure > Instances > 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。
4. **Create** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SNMP v3マネージャーを追加する

NetScalerエージェントにSNMP v3マネージャーを追加するには、次の手順を実行します。

1. **Infrastructure > Instances > 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ユーザーを追加する

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 > Instances > Agents** に移動し、NetScalerエージェントを選択して、**Select Action > Manage SNMP** をクリックします。
2. **SNMP > SNMP User** タブで、**Add** をクリックします。
3. **Create SNMP User** ページで、次の詳細を追加します。
   - **Name**。ユーザー名を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 > Instances > Agents** に移動し、NetScalerエージェントを選択して、**Select Action > Manage SNMP** をクリックします。
2. **SNMP > SNMP User** タブで、**Add** をクリックします。
3. **Create SNMP 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の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設定できます。

4. **Create** をクリックします。

   SNMPビューの画像(/en-us/netscaler-console-service/media/snmp-create-view.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDX 上での NetScaler VPX インスタンスのプロビジョニング

NetScaler Console 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、NetScaler Console はそれ以上の NetScaler インスタンスのプロビジョニングを許可しません。

開始する前に、VPX インスタンスをプロビジョニングする場所として NetScaler Console に SDX インスタンスを追加していることを確認してください。

VPX インスタンスをプロビジョニングするには、次の手順を実行します。

1. 「**Infrastructure > Instances > NetScaler**」に移動します。
2. 「**SDX**」タブで、VPX インスタンスをプロビジョニングする SDX インスタンスを選択します。
3. 「**Select Action**」で、「**Provision VPX**」を選択します。

ステップ 1 - VPX インスタンスを追加する

NetScaler Console は、SDX アプライアンスで VPX インスタンスを構成するために次の情報を使用します。

- 「**名前**」 - NetScaler インスタンスに名前を指定します。
- SDX と VPX 間の通信ネットワークを確立します。そのためには、リストから必要なオプションを選択します。
    - 「**内部ネットワーク経由で管理**」 - このオプションは、NetScaler Console と VPX インスタンス間の通信のために内部ネットワークを確立します。
    - 「**IP アドレス**」 - NetScaler VPX インスタンスを管理するために、**IPv4** または **IPv6** アドレス、あるいはその両方を選択できます。VPX インスタンスは、管理 IP (NetScaler IP とも呼ばれます) を 1 つしか持つことができません。NetScaler IP アドレスを削除することはできません。

      選択したオプションについて、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 NetScaler Console 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。次のいずれかのオプションを使用して XVA ファイルを選択します。
    - **ローカル** - ローカルマシンからXVAファイルを選択します。
    - **アプライアンス** - NetScaler Consoleのファイルブラウザから XVAファイルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **管理者プロファイル** - このプロファイルは、VPXインスタンスをプロビジョニングするためのアクセスを提供します。このプロファイルを使用すると、NetScaler Consoleはインスタンスから構成データを取得します。プロファイルを追加する必要がある場合は、**追加**をクリックします。
- **エージェント** - インスタンスを関連付けるエージェントを選択します。
- **サイト** - インスタンスを追加するサイトを選択します。

VPXインスタンスを追加する(/en-us/netscaler-console-service/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**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-Instance Add-On Pack) 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-console-service/media/license-allocation.png)

SDX 12.0 57.19バージョン以降、暗号容量を管理するインターフェイスが変更されました。詳細については、「暗号容量の管理」を参照してください。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**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

  」

  インスタンスに設定できる最大スループットは180 Gbpsです。

リソースを割り当てる(/en-us/netscaler-console-service/media/resource-allocation.png)

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一覧表示するNetScalerインスタンスのプロビジョニングの表を参照してください。

ステップ 4 - インスタンス管理の追加

VPXインスタンスの管理者ユーザーを作成できます。これを行うには、「**インスタンス管理**」セクションで「**インスタンス管理の追加**」を選択します。

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です。このユーザーはスーパーユーザーアクセス権を持っていますが、VLANやインターフェースを設定するためのネットワークコマンドへのアクセス権はありません。
- **パスワード**: ユーザー名のパスワードを指定します。
- **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です。このオプションはデフォルトで選択されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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** - 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。詳細については、「NetScalerインスタンスでのL2モードの許可」を参照してください。

  注

  インスタンスのL2モードを無効にする場合は、そのインスタンスにログオンしてL2モードを無効にする必要があります。そうしないと、インスタンスを再起動した後に他のすべてのNetScalerモードが無効になる可能性があります。

- **0/1** - **VLANタグ**で、管理インターフェースのVLAN IDを指定します。
- **0/2** - **VLANタグ**で、管理インターフェースのVLAN IDを指定します。

デフォルトでは、インターフェース**0/1**と**0/2**が選択されています。

データインターフェースで、**追加**をクリックしてデータインターフェースを追加し、以下を指定します。

- **インターフェース** - リストからインターフェースを選択します。

  注記

  インスタンスに追加するインターフェースのインターフェースIDは、SDXアプライアンス上の物理インターフェースの番号付けと必ずしも対応しません。

  例えば、インスタンス1に関連付ける最初のインターフェースがSDXインターフェース1/4である場合、そのインスタンスでインターフェース設定を表示すると、インターフェース1/1として表示されます。このインターフェースは、インスタンス1に関連付けた最初のインターフェースであることを示します。

- **許可されたVLAN** - NetScalerインスタンスに関連付けることができるVLAN IDのリストを指定します。
- **MACアドレスモード** - インスタンスにMACアドレスを割り当てます。次のいずれかのオプションから選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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。ベースMACアドレスの設定については、「インターフェースへのMACアドレスの割り当て」を参照してください。

- **VMAC設定 (仮想MACを構成するためのIPv4およびIPv6 VRID)**
  - **VRID IPv4** - VMACを識別するIPv4 VRID。指定可能な値：1～255。詳細については、「インターフェースでのVMACの構成」を参照してください。
  - VRID IPv6 - VMACを識別するIPv6 VRID。指定可能な値：1～255。詳細については、「インターフェースでのVMACの構成」を参照してください。

「**追加**」をクリックします。

ステップ6 - 管理VLAN設定を指定します

管理サービスとVPXインスタンスの管理アドレス（NSIP）は同じサブネットワーク内にあり、通信は管理インターフェースを介して行われます。

管理サービスとインスタンスが異なるサブネットワークにある場合は、VPXインスタンスをプロビジョニングするときに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。

デプロイメントで、VPXインスタンスのプロビジョニング中にNSIPが選択されたインターフェイスからのみアクセス可能である必要がある場合は、**NSVLAN**を選択します。これにより、NSIPは他のインターフェイスからはアクセスできなくなります。

- HAハートビートは、NSVLANの一部であるインターフェ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。
- **NSVLAN**が選択されていない場合、VPXインスタンスの `clear config full` コマンドはVLAN構成を削除します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VLANの管理](/en-us/netscaler-console-service/media/manage-vlan-settings.png)

完了をクリックして、VPXインスタンスをプロビジョニングします。

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。

プロビジョニングされたVPXインスタンスを表示](/en-us/netscaler-console-service/media/provisioned-vpx-on-sdx.png)

複数のNetScalerインスタンスを再検出する

NetScaler Consoleのセットアップで、複数のCitrix Application Delivery Controller (NetScaler) インスタンス (VPX、MPX、SDX、BLX、CPX) を再検出できます。インスタンスを再検出すると、それらのインスタンスの最新の状態と構成を表示できます。NetScaler Consoleサーバーは、すべてのADCインスタンスを再検出し、インスタンスが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. **Infrastructure > Instances > NetScaler** に移動します。インスタンスタブ (VPX、MPX、SDX、BLX、CPX) を選択し、再検出するインスタンスを選択します。
2. **Action** ボックスで、**Rediscover** をクリックします。複数のVPXインスタンスを再検出することもできます。
3. Rediscover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、**Yes** をクリックします。

   画面には、各インスタンスの再検出の進行状況が表示されます。

ポーリングの概要

ポーリングは、NetScaler ConsoleがNetScalerインスタンスから特定の情報を収集するプロセスです。組織のために、世界中に複数のNetScalerインスタンスを設定している場合があります。NetScaler Consoleを通じてインスタンスを監視するには、NetScaler Consoleは、すべての管理対象NetScalerインスタンスから、CPU使用率、メモリ使用率、SSL証明書、ライセンス機能、ライセンスの種類などの特定の情報を収集する必要があります。NetScaler Consoleと管理対象インスタンスの間で行われるポーリングには、次の種類があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- インスタンスポーリング
- インベントリポーリング
- パフォーマンスデータ収集
- インスタンスバックアップポーリング
- 構成監査ポーリング
- SSL証明書ポーリング
- エンティティポーリング

NetScaler Consoleは、NITROコール、Secure Shell (SSH)、Secure Copy (SCP) などのプロトコルを使用して、NetScalerインスタンスから情報をポーリングします。

NetScaler Consoleが管理対象インスタンスとエンティティをポーリングする方法

NetScaler Consoleは、デフォルトで定期的に自動的にポーリングします。また、NetScaler Consoleでは、いくつかのポーリングタイプに対してポーリング間隔を設定したり、必要に応じて手動でポーリングしたりすることもできます。

次の表に、ポーリングの種類、ポーリング間隔、使用されるプロトコルなどの詳細を示します。

ポーリングの種類	ポーリング間隔	ポーリング情報	使用プロトコル	ポーリング間隔の設定
インスタンスのポーリング	5分ごと（デフォルト）	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。	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

© 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	使用プロトコル	ポーリング間隔の設定
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）	管理対象のNetScalerインスタンスの現在の状態のバックアップファイル	NITROコール、SSH、およびSCP	はい。**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）	NetScalerインスタンスで発生する構成変更（例：実行中の構成と保存された構成）	SSH、SCP、およびNITROコール	はい。**Infrastructure > Configuration > Configuration Audit**に移動します。構成監査ページで、**Settings**をクリックし、構成監査ポーリングのポーリング間隔を設定します。
				構成監査を手動でポーリングし、インスタンスのすべての構成監査をNetScaler Consoleに即座に追加できます。これを行うには、**Infrastructure >**

© 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	使用プロトコル	ポーリング間隔の設定
				Configuration > **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コールとSCP	はい。**Infrastructure** > **SSL Dashboard** に移動します。SSL Dashboard ページで、**Settings** をクリックしてポーリング間隔を設定します。
				SSL証明書を手動でポーリングし、インスタンスのすべての証明書をNetScaler Consoleに即座に追加できます。これを行うには、**Infrastructure** > **SSL Dashboard** に

© 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	使用プロトコル	ポーリング間隔の設定
				移動し、**Poll Now** をクリックします。**Poll Now** ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
エンティティポーリング				
すべてのインスタンス	720分ごと（デフォルト）	インスタンスに構成されているすべてのエンティティ。エンティティとは、NetScalerインスタンスにアタッチされているポリシー、仮想サーバー、サービス、またはアクションのいずれかです。エンティティポーリングを有効にするには、「NetScaler Console機能の有効化または無効化」を参照してください。	NITROコール	はい。30分から1440分の間で設定できます。設定するには、**Infrastructure > Network Functions** に移動します。Networks Functionページで、**Settings** をクリックしてポーリング間隔を設定します。
				エンティティを手動でポーリングし、インスタ

© 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	使用プロトコル	ポーリング間隔の設定
				ンスのすべてのエンティティをNetScaler Consoleに即座に追加できます。これを行うには、**Infrastructure > Network Functions** に移動し、**Poll Now** をクリックします。**Poll Now** ページでは、ネットワーク内のすべてのインスタンスまたは選択したインスタンスをポーリングできます。
選択したNetScalerインスタンス	15分ごと（デフォルト）	デフォルトのポーリングサイクルがトリガーされる前に変更が加えられたNetScalerインスタンスのみをポーリングします。	NITROコール	はい。5分から60分の間で設定できます。**Infrastructure > Network Functions** に移動し、**Settings** をクリックして、**Delay time for Network Functions** テキストボックスで時間を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

ポーリングに加えて、管理対象のNetScalerインスタンスによって生成されたイベントは、インスタンスに送信されるSNMPトラップを介してNetScaler Consoleによって受信されます。たとえば、システム障害や構成の変更があった場合にイベントが生成されます。

インスタンスのバックアップ中、SSLファイル、CA証明書ファイル、NetScalerテンプレート、データベース情報などがNetScaler Consoleにダウンロードされます。構成監査中、ns.confファイルはダウンロードされ、ファイルシステムに保存されます。管理対象のNetScalerインスタンスから収集されたすべての情報は、データベース内に内部的に保存されます。

インスタンスをポーリングするさまざまな方法

NetScaler Consoleが管理対象インスタンスに対して実行するポーリングのさまざまな方法は次のとおりです。

- インスタンスのグローバルポーリング
- インスタンスの手動ポーリング
- エンティティの手動ポーリング

インスタンスのグローバルポーリング

NetScaler Consoleは、お客様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60分ですが、**Infrastructure > Network Functions > Settings** に移動して、要件に応じて間隔を設定できます。

インスタンスの手動ポーリング

NetScaler Consoleが多数のエンティティを管理している場合、レポートの生成にポーリングサイクルが長くかかり、空白の画面が表示されたり、システムが以前のデータを表示したままになったりする可能性があります。

NetScaler Consoleでは、自動ポーリングが行われない最小ポーリング間隔期間があります。新しいNetScalerインスタンスを追加したり、エンティティが更新されたりした場合、NetScaler Consoleは次のポーリングが行われるまで、新しいインスタンスやエンティティへの更新を認識しません。また、その後の操作のために仮想IPアドレスのリストをすぐに取得する方法はありません。最小ポーリング間隔期間が経過するまで待つ必要があります。新しく追加されたインスタンスを発見するために手動でポーリングを行うことはできますが、これによりNetScalerネットワーク全体がポーリングされ、ネットワークに大きな負荷がかかります。ネットワーク全体をポーリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ングする代わりに、NetScaler Consoleでは、いつでも選択したインスタンスとエンティティのみをポーリングできるようになりました。

NetScaler Consoleは、1日の決まった時間に情報を収集するために、管理対象インスタンスを自動的にポーリングします。選択されたポーリングにより、NetScaler Consoleがこれらの選択されたインスタンスにバインドされているエンティティの最新ステータスを表示するために必要な更新時間が短縮されます。

NetScaler Consoleで特定のインスタンスをポーリングするには:

1. NetScaler Consoleで、**インフラストラクチャ > ネットワーク機能**に移動します。
2. **ネットワーク機能**ページで、右上隅にある**今すぐポーリング**をクリックします。
3. 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用意されています。

    a. **すべてのインスタンス**タブ - **ポーリング開始**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. **ポーリング開始**をクリックします。

    NetScaler Consoleは手動ポーリングを開始し、すべてのエンティティを追加します。

エンティティの手動ポーリング

NetScaler Consoleでは、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。この場合、更新された1つのエンティティのステータスを知るために、インスタンス全体をポーリングする必要はありません。エンティティを選択してポーリングすると、NetScaler Consoleはそのエンティティのみをポーリングし、NetScaler Console GUIのステータスを更新します。

仮想サーバーが**DOWN**状態である例を考えてみましょう。次の自動ポーリングが行われる前に、その仮想サーバーのステータスが**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、正しいステータスが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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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した場合、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 Console で特定のエンティティをポーリングするには：

例えば、このタスクはロードバランシング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。

1. NetScaler Console で、**インフラストラクチャ > ネットワーク機能 > 負荷分散 > 仮想サーバー**に移動します。
2. ステータスが「**DOWN**」と表示されている仮想サーバーを選択し、「**Poll Now**」をクリックします。仮想サーバーのステータスが「**UP**」に変わります。

インスタンスの管理を解除する

NetScaler Consoleとネットワーク内のインスタンス間の情報交換を停止したい場合は、インスタンスの管理を解除できます。

インスタンスの管理を解除するには：

1. **インフラストラクチャ > インスタンス > NetScaler** に移動します。
2. NetScalerインスタンスタブ（例：VPX）を選択します。
3. 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**管理解除**を選択するか、インスタンスを選択して**アクション**リストから**管理解除**を選択します。

   選択したインスタンスのステータスが**サービス停止中**に変わります。

   インスタンスはNetScaler Consoleによって管理されなくなり、NetScaler Consoleとのデータ交換も行われなくなります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスへのルートをトレースする

NetScaler Consoleからインスタンスへのパケットのルートをトレースすることで、インスタンスに到達するために必要なホップ数などの情報を見つけることができます。トレーシングルートは、送信元から宛先へのパケットのパスをトレースします。ルート内の各エンティティのホスト名とIPアドレスとともに、ネットワークホップのリストを表示します。

トレーシングルートは、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、トレーシングルートは問題がどこにあるかを示します。

インスタンスのルートをトレースするには:

1. **インフラストラクチャ > インスタンス > NetScaler** に移動します。
2. NetScalerインスタンスタブ（例: VPX）を選択します。
3. 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、**アクション**リストから**TraceRoute**をクリックします。

   TraceRouteメッセージボックスには、インスタンスへのルートと、各ホップで消費された時間（ミリ秒単位）が表示されます。

NetScalerが所有するIPアドレスの表示

NetScaler Console GUIから直接、NetScalerインスタンスに設定されているIPアドレスを表示できます。設定の変更やその他の操作は、NetScalerインスタンス上でのみ実行できることに注意してください。

NetScalerが所有するIPアドレスを表示するには、**Infrastructure > Instances > NetScaler Owned IPs**に移動します。

この機能は、NetScalerインスタンスに設定されているIPv4アドレスとIPv6アドレスの両方を表示します。IPアドレスの種類は次のとおりです。

- NetScaler IPアドレス
- サブネットIPアドレス
- 仮想IPアドレス
- ADNSサービスIPアドレス
- GSLB IPアドレス
- クラスターIPアドレス
- マップされたIPアドレス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理対象IPアドレス(/en-us/netscaler-console-service/media/netscaler-owned-ips.png)

NetScalerが所有するIPアドレスのエクスポート

NetScalerが所有するIPアドレスをエクスポートするには、次の手順を実行します。

1. **Infrastructure > Instances > NetScaler Owned IPs**に移動します。
2. 「**NetScaler Owned IPs**」ページで、右上隅にあるエクスポートアイコンをクリックします。
3. 「**Export Reports**」ページで、「**Export Now**」をクリックします。
4. 「**Export Now**」ページで、エクスポートオプションを選択します。

   「**Snapshot**」エクスポートの場合:

   a. エクスポートファイル形式として、PDF、JPG、またはPNGを選択します。

      スナップショットのエクスポート(/en-us/netscaler-console-service/media/export-now-snapshot.png)

   「**Tabular**」エクスポートの場合:

   a. エクスポートファイル形式として、PDFまたはCSVを選択します。
   b. リストからエクスポートするデータレコードの数を選択します。

      表形式のエクスポート(/en-us/netscaler-console-service/media/export-now-tabular.png)

5. 「**Export**」をクリックします。

NetScalerが所有するIPアドレスのエクスポートをスケジュールする

NetScalerが所有するIPアドレスのエクスポートをスケジュールするには、次の手順に従います。

1. 「**Infrastructure > Instances > NetScaler Owned IPs**」に移動します。
2. 「**NetScaler Owned IPs**」ページで、右上隅にあるエクスポートアイコンをクリックします。
3. 「**レポートのエクスポート**」ページで、「**エクスポートのスケジュール**」をクリックします。
4. 「**エクスポートのスケジュール**」ページで、次の詳細を入力します。

   a. 件名と説明を入力します。
   b. エクスポートタイプを選択します。

      スナップショットエクスポートタイプの場合:

      - エクスポートファイル形式 (PDF、JPG、PNG) を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表形式エクスポートタイプの場合:

- エクスポートファイル形式 (PDF または CSV) を選択します。
- リストからエクスポートするデータレコードの数を選択します。

c. 繰り返し (毎日、毎週、毎月) を選択します。

d. エクスポート時間を選択します。

e. エクスポートされたIPアドレスの送信方法 (メール、Slack、またはその両方) を選択します。

メールの場合:

- 「**メール**」を選択し、NetScalerが所有するIPアドレスのリストを送信するメール配信リストを選択します。
  - メール配信リストを追加するには、「**追加**」をクリックし、メールサーバーの詳細を指定します。
  - メール配信リストを編集するには、**編集**をクリックします。
  - メール配信リストが機能していることを確認するには、**テスト**をクリックします。これにより、選択したメール配信リストにテストメールが送信されます。

Slackの場合:

- **Slack**を選択し、NetScalerが所有するIPアドレスのリストを送信するSlackプロファイルリストを選択します。
  - Slackプロファイルを追加するには、**追加**をクリックし、Slackチャネルの**プロファイル名**、**チャネル名**、および**トークン**を指定します。
  - 既存のSlackチャネルを編集するには、**編集**をクリックします。

5. エクスポートをスケジュールするには、**スケジュール**をクリックします。

エクスポートのスケジュール(/en-us/netscaler-console-service/media/schedule-export.png)

スケジュールされると、エクスポートスケジュールは**エクスポートレポート**ページに表示され、スケジュールを選択して編集または削除操作を実行できます。

エクスポート操作のスケジュール(/en-us/netscaler-console-service/media/schedule-export-operations.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler MPXまたはVPXのrootパスワードを変更する方法

セキュリティ上の理由またはパスワードローテーションポリシーの遵守のため、NetScalerアプライアンスのrootパスワードを定期的に変更する必要があります。

このドキュメントでは、NetScaler Consoleクラウドを通じて管理されるNetScaler MPXおよびVPXアプライアンスのrootパスワードを変更するために必要な手順について説明します。

NetScalerのパスワードを変更する場合は、NetScalerに関連付けられているNetScaler Console管理者プロファイルを変更する必要があります。NetScaler Console管理者プロファイルは、NetScalerアプライアンスとのREST API、SSH、SCP、またはSNMPベースの通信のためのNetScaler資格情報を保持します。管理者プロファイルを通じて、NetScaler ConsoleはNetScaler MPXおよびVPXアプライアンスを管理します。

構成ジョブ機能を使用してパスワードを変更する

NetScaler Consoleの構成ジョブ機能を使用すると、繰り返しのパスワード変更プロセスを簡素化し、個々のインスタンスにアクセスすることなく、NetScalerアプライアンスに変更を適用できます。

パスワードを変更するには、次の手順に従います。

- ステップ1. 構成テンプレートを作成します。
- ステップ2. 構成ジョブを作成します。
- ステップ3. 管理者プロファイルを作成し、変更します。

注:

> NetScalerアプライアンスが他のツールでも管理されている場合は、それらのツールの資格情報も変更する必要があります。

構成テンプレートを作成する

1. NetScaler Console のグラフィカルユーザーインターフェースから、**Infrastructure > Configuration > Configuration Templates** に移動します。
2. **Add**を選択します。SSHコマンド `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$` を入力して構成テンプレートを作成します。

   「コマンドの選択」(/en-us/netscaler-console-service/media/change-adc-root-password-2.png)
3. $ROOT_USER_NAME$ 変数を選択し、**タイプとしてテキストフィールド**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 任意で、ルートユーザー名のデフォルト値を指定します。**完了**を選択して変数設定を保存します。

   「変数設定の保存」(/en-us/netscaler-console-service/media/change-adc-root-password-3.png)

5. $ROOT_USER_PASSWORD$ 変数を選択し、**タイプとしてパスワードフィールド**を選択します。**完了**を選択して変数設定を保存します。
6. **OK**を選択して構成テンプレートを保存します。
7. 新しい構成テンプレートは、**構成テンプレート**の下に表示されます。

構成ジョブの作成

1. NetScaler Console GUIから、**インフラストラクチャ > 構成ジョブ**に移動します。
2. **ジョブの作成**を選択し、新しい構成テンプレートの「+」アイコンをクリックします。**次へ**を選択します。

   「構成ジョブの作成」(/en-us/netscaler-console-service/media/change-adc-root-password-8.png)

3. パスワードを変更する必要があるNetScalerインスタンスを選択します。

   「インスタンスの選択」(/en-us/netscaler-console-service/media/change-adc-root-password-9.png)

4. **インスタンスの選択**ペインで、インスタンスを選択し、**次へ**をクリックします。
5. **変数値を指定**ペインで、ユーザー名とパスワードの値を指定し、**次へ**をクリックします。
6. 「**ジョブプレビュー**」で、NetScaler ConsoleがNetScalerインスタンスで実行する実際のCLIコマンドを確認します。プレビューが問題なければ、「**次へ**」をクリックします。

7. 「**実行**」ペインで、ジョブをすぐに実行するか、後でスケジュールするかを選択できます。また、選択したすべてのインスタンスでジョブを並行して実行するか、順次実行するかを選択することもできます。実行の詳細を指定したら、「完了」を選択します。
8. 構成ジョブは、実行が成功したか失敗したかを示します。
9. 「**ジョブ**」を選択し、「**詳細**」をクリックします。実行の詳細には、個々のインスタンスレベルでのステータスが表示されます。

管理者プロファイルの変更

NetScalerのパスワードを変更した後、インスタンスの管理者プロファイルを追加および変更する必要があります。次の手順に従います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**インフラストラクチャ > インスタンス > NetScaler**」に移動します。
2. 「**プロファイル**」をクリックして、すべての管理者プロファイルを表示します。
3. 「**追加**」を選択して管理者プロファイルを作成し、新しいNetScaler資格情報を指定します。

4. 新しく作成されたプロファイルは、「**管理者プロファイル**」の下に表示されます。
5. 「**ネットワーク > インスタンス > NetScaler**」に移動します。パスワードが変更されたNetScalerインスタンスを選択し、「**編集**」を選択します。
6. 新しく作成されたプロファイル名を選択し、「**OK**」をクリックします。

7. インスタンスを再度選択し、右クリックして、「**Rediscover**」を選択します。

   インスタンスを再検出(/en-us/netscaler-console-service/media/change-adc-root-password-16a.png)

パスワードの変更に成功しました。

SDXアプライアンスのパスワード変更については、「NetScaler SDXのrootパスワードを変更する方法」を参照してください。

NetScaler SDX nsroot パスワードを変更する方法

セキュリティ上の理由またはパスワードローテーションポリシーの遵守のため、NetScalerアプライアンスのnsrootパスワードを変更する必要がある場合があります。

このドキュメントでは、NetScaler Consoleクラウドを介して管理されるNetScaler SDXアプライアンスのnsrootパスワードを変更するために必要な手順について説明します。

NetScalerのパスワードを変更した場合、NetScalerに関連付けられているNetScaler Consoleの管理者プロファイルを変更する必要があります。NetScaler Consoleの管理者プロファイルは、NetScalerアプライアンスとのREST API、SSH、SCP、またはSNMPベースの通信のためのNetScaler資格情報を保持します。管理者プロファイルを通じて、NetScaler ConsoleはNetScaler SDXアプライアンスを管理します。

パスワードの変更

パスワードを変更するには、次の手順に従います。

- ステップ1. SDX Management Service GUIからSDXパスワードを変更します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ステップ2. SDXに関連付けられているNetScaler Consoleの管理者プロファイルを変更します。

注:

SDXアプライアンスが他のツールによっても管理されている場合は、それらのツールでも資格情報を変更する必要があります。

SDX Management Service GUIからSDXパスワードを変更する

1. SDXマネジメントサービスから、**System > User Administration > Users**に移動します。
2. パスワードを変更するユーザー名を選択し、**Edit**をクリックします。
3. **Change Password**を選択します。
4. 新しいパスワードを入力し、**OK**をクリックします。
5. SDXパスワードが変更されました

NetScaler Consoleの管理者プロファイルを変更する

SDXパスワードを変更したら、インスタンスの管理者プロファイルを変更する必要があります。次の手順に従います。

1. **Infrastructure > Instances Dashboard > NetScaler > SDX** に移動します。
2. すべての管理者プロファイルを表示するには、**Profiles** を選択します。
3. 管理者プロファイルを作成するには、**Add** を選択します。
4. 新しいNetScaler資格情報を入力し、**Create** をクリックします。

5. 新しく作成されたプロファイルは、**Admin Profiles** の下に表示されます。
6. **Network > Instances > NetScaler > SDX** に移動します。パスワードが変更されたインスタンスを選択し、**Edit** を選択します。
7. 新しく作成されたプロファイル名を選択し、**OK** をクリックします。

8. インスタンスを再度選択し、右クリックして **Rediscover** をクリックします。

パスワードが正常に変更されました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDXアプライアンスのパスワード変更に関する情報については、NetScaler MPXまたはVPXのrootパスワードを変更する方法を参照してください。

NetScaler® インスタンスのテクニカルサポートバンドルを生成する方法

NetScaler インスタンスに関する問題の分析と解決を支援するため、インスタンス上でテクニカルサポートバンドルを生成し、Citrix テクニカルサポートに送信できます。テクニカルサポートバンドルは、システム構成データと統計情報の圧縮された tar アーカイブです。テクニカルサポートバンドルは、バンドルを生成する NetScaler インスタンスから以下のデータを収集します。

- 構成ファイル。/flash/nsconfig ディレクトリ内のすべてのファイル。
- `newnslog` ファイル。現在実行中の `newnslog` および一部の以前のファイル。アーカイブファイルサイズを最小限に抑えるため、`newnslog` の収集は、500 MB、6 ファイル、または 7 日間のいずれか早い方に制限されます。古いデータが必要な場合は、手動での収集が必要になる場合があります。
- ログファイル。/var/log/messages、/var/log/ns.log、および /var/log と /var/nslog の下のその他のファイル。
- アプリケーションコアファイル。過去 1 週間以内に /var/core ディレクトリに作成されたファイル（存在する場合）。
- 一部の CLI show コマンドの出力。
- 一部の CLI stat コマンドの出力。
- BSD シェルコマンドの出力。

テクニカルサポートファイルを生成する際には、時間を指定することが必須です。テクニカルサポートファイルを生成する際には、時間参照を明示的に選択する必要があります。`custom` オプションを選択してカスタムの日付と時刻を指定するか、`Now` オプションを使用できます。時間を指定することで、正確な時間コンテキストが明示的に定義されます。

時間パラメータは、`newnslog` ファイルの検索に使用される、Common Log Format での参照時間を指定します。形式は `DD/MMM/YYYY:HH:MM:SS` です。

時間が指定されている場合、最大 4 つの `newnslog` ログファイルが収集されます。

- 指定された時間範囲に対応する `newnslog` ファイル
- 最初のファイルの直前に作成されたログファイル（利用可能な場合）
- 最初のファイルの直後に作成されたログファイル（利用可能な場合）
- 最新の`newnslog`ディレクトリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

スコープがクラスターに設定されている場合、2番目と3番目のログファイルはどのノードでも収集されません。

テクニカルサポートバンドルをCitrixテクニカルサポートサーバーに安全にアップロードすることもできます。NetScaler 14.1リリース8.xビルド以降、テクニカルサポートバンドルをアップロードする前に認証トークンを生成する必要があります。以前のビルドでは、Citrixのユーザー名とパスワードを使用してテクニカルサポートバンドルをアップロードできます。

認証トークンを生成するには：

1. ブラウザを起動し、次のURLを入力します - `<https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600>`。
2. 多要素認証を使用してログインします。

   注：

   多要素認証への登録方法については、多要素認証 (MFA) への登録方法を参照してください。

3. 画面に表示されている認証トークンをコピーするには、**Copy**をクリックします。トークンは3600秒（1時間）有効です。トークンの最大許容長は1023文字です。

認証トークンをコピーしたら、GUIを使用してファイルをアップロードします。

GUIを使用してテクニカルサポートバンドルをアップロードするには：

1. **Infrastructure > Instances > NetScaler**に移動します。
2. NetScalerインスタンスを選択します。
3. **Select Actions**から**Generate Technical Support File**を選択します。
4. 「**テクニカルサポートファイルの生成**」をクリックします。
5. 「**スコープ**」オプションを使用して、現在のノード、すべてのクラスターノード、または指定されたパーティションのデータを収集するかどうかを指定します。
6. 「**テクニカルサポートデータの時間オプションを選択**」から、次のオプションのいずれかを選択します。

   - 「**今すぐ**」 - 現在のシステム時刻を使用し、以前のリリースでの動作を維持します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**カスタム**」 - 指定された日付と時刻を使用します。

7. 「**コレクターアーカイブをアップロード**」を選択します。
8. 「**マイCitrixアカウント**」セクションで、「**Citrix認証トークン**」フィールドに認証トークンを入力します。
9. 「**テクニカルサポートの作成**」をクリックします。

「テクニカルサポートバンドルの生成」(/en-us/netscaler-console-service/media/technical-support-bundle.png)

イベント

Citrix Application Delivery Controller (NetScaler) インスタンスのIPアドレスがNetScaler Consoleに追加されると、NetScaler ConsoleはNITROコールを送信し、暗黙的に自身をインスタンスのトラップまたはイベントを受信するトラップ送信先として追加します。

イベントは、管理対象のNetScalerインスタンスで発生したイベントまたはエラーを表します。たとえば、システム障害や構成の変更があった場合、イベントが生成され、NetScaler Consoleサーバーに記録されます。NetScaler Consoleで受信したイベントは、イベント概要ページ（**インフラストラクチャ > イベント**）に表示され、すべてのアクティブなイベントはイベントメッセージページ（**インフラストラクチャ > イベント > イベントメッセージ**）に表示されます。

NetScaler Consoleは、インスタンスで生成されたイベントもチェックし、さまざまな重大度レベルのアラームを形成してメッセージとして表示します。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」なイベント重大度として分類され、即座に対応できます。

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。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さまざまなイベントを監視しやすくなります。

特定の条件を持つルールを構成し、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、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、イベントに対して特定の時間間隔で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、ユーザーメッセージ、および添付ファイルのアップロードでメールをカスタマイズすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イベントダッシュボードの使用

ネットワーク管理者として、Citrix Application Delivery Controller (NetScaler) インスタンスでの構成変更、ログイン状況、ハードウェア障害、しきい値違反、エンティティの状態変更などの詳細、および特定のインスタンスでのイベントとその重大度を表示できます。NetScaler Console 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の重大度詳細に関する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「トップ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/ NetScaler**）に移動して、以下の詳細を表示できます。

  - ハードウェア障害による上位10デバイス
  - 構成変更による上位10デバイス
  - 認証失敗による上位10デバイス

- [ ]
  - エンティティの状態変更による上位10デバイス

- [ ]
  - しきい値違反による上位10デバイス

- [ ]

このダッシュボードのレポートをエクスポートするには：

このページのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページでは、次のいずれかを実行できます。

1. **今すぐエクスポート**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。
2. **エクスポートのスケジュール**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- **毎週**の繰り返しを選択する場合は、レポートをスケジュールする曜日を選択していることを確認してください。
- **毎月**の繰り返しを選択する場合は、レポートをスケジュールするすべての日をコンマで区切って入力していることを確認してください。

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イベントをより簡単にフィルタリングできます。

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ー条件を満たすと、そのルールに関連付けられたアクションが実行されます。

以下の条件でフィルターを作成できます。

- 重大度
- シトリックス アプリケーションデリバリーコントローラー (ネットスケーラー) インスタンス
- カテゴリ
- 障害オブジェクト
- 構成コマンド
- メッセージ

イベントを作成した後、イベントにアクションを割り当てることができます。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。

たとえば、管理者として、NetScalerインスタンスで障害につながる可能性のある「CPU使用率が高い」イベントを監視したい場合があります。通知を受け取るには、次のいずれかのアクションを実行できます。

- インスタンスを監視するルールを作成し、そのようなイベントが発生したときに通知を受け取るようにルールにアクションを追加します。
- 特定の期間でインスタンスを監視するルールをスケジュールします。これにより、その期間内にそのようなイベントが発生したときに通知を受け取ることができます。

次の図は、イベントルールの仕組みのワークフローを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イベントの仕組み(/en-us/netscaler-console-service/media/createeventruleflow.png)

イベントルールを設定する

イベントルールを設定するには、**Infrastructure > Events > Rules**に移動し、**Add**をクリックします。**Create Rule**ページで、次のタスクを実行します。

1. 名前とインスタンスファミリを指定する(#step-1---specify-name-and-instance-family)
2. イベントの経過時間を設定する(#step-1---specify-name-and-instance-family)
3. ルールが検出するイベントの重大度を選択する(#step-3---choose-severity-of-event)
4. イベントのカテゴリを指定する(#step-4---specify-event-category)
5. ルールを適用するNetScaler®インスタンスを指定する(#step-5---specify-netscaler-instances)
6. 障害オブジェクトを選択する(#step-6---select-failure-objects)
7. 詳細フィルターを指定する(#step-7---specify-advanced-filters)
8. ルールがイベントを検出したときに実行するアクションを指定する(#step-8---add-event-rule-actions)

ステップ1 - 名前とインスタンスファミリを指定する

1. **名前**。イベントルールの名前を入力します。
2. **インスタンスファミリ**。**Instance Family**ドロップダウンリストからインスタンスファミリを選択します。

   Instance Familyでイベントルールをフィルタリングして、NetScaler Consoleがイベントを受信するNetScalerインスタンスを追跡できます。

   名前とインスタンスファミリーを指定します(/en-us/netscaler-console-service/media/create-rule-name-instance.png)

ステップ2 - イベント期間を設定する

1. **イベント期間**。NetScaler Console がイベントルールを更新するまでの時間間隔 (秒単位) を指定します。

   例えば、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メールを送信したいとします。イベント期間を60秒に設定できます。これで、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、メール通知が届きます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> **イベント期間**は必須フィールドです。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。

2. イベントを追跡するには、次のいずれかのオプションを選択します。

   - **イベント期間に達するまでイベントログをスキップする**。指定されたイベント期間より前に発生したイベントは、NetScaler Console サーバーデータベースにログ記録されません。イベント期間に達すると、イベントはデータベースにログ記録され、設定されたイベントアクションがトリガーされます。
   - **イベント期間に関係なくイベントを即座にログに記録する**。指定されたイベント期間に関係なく、すべてのイベントがNetScaler Console サーバーデータベースにログ記録されます。イベント期間に達すると、設定されたイベントアクションがトリガーされます。

   イベント期間を設定する(/en-us/netscaler-console-service/media/create-rule-event-age.png)

3. **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**。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には、このオプションを選択します。このオプションは、障害オブジェクト、構成コマンド、およびメッセージに適用されます。

ステップ3 - イベントの重大度を選択する

- **重大度**セクションで、イベントルールの重大度を選択します。

  次の重大度レベルを定義できます: 重大、メジャー、マイナー、警告、クリア、情報。

> **注:**
>
> 汎用イベントとAdvanced固有イベントの両方について、重大度を設定できます。NetScaler Consoleで管理されているNetScalerインスタンスのイベント重大度を変更するには、**Infrastructure > Events > Event Settings**に移動します。イベント重大度を設定したい**Category**を選択し、**Configure Severity**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。

イベント重大度を指定(/en-us/netscaler-console-service/media/createer2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステップ4 - イベントカテゴリを指定する

NetScalerインスタンスによって生成されるイベントのカテゴリを指定できます。すべてのカテゴリはNetScalerインスタンスで作成されます。これらのカテゴリは、イベントルールを定義するために使用できるNetScaler Consoleにマッピングされます。

- 考慮したいカテゴリを選択し、**Available**テーブルから**Configured**テーブルに移動します。

  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「cpuUtilization」を選択する必要があります。

  イベントカテゴリを指定(/en-us/netscaler-console-service/media/createer3.png)

ステップ5 - NetScalerインスタンスを指定する

Instancesセクションで、次の操作を行います。

1. **Select Instances**をクリックします。**Select Instances**ページで、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。
2. **Select**をクリックします。

   NetScalerインスタンスを選択(/en-us/netscaler-console-service/media/createer4.png)

ステップ6 - 障害オブジェクトを選択する

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。

1. **Select Failure Objects**をクリックします。
2. 「**Failure Objects**」ページで、リストから障害オブジェクトを選択します。「**Select**」をクリックします。
3. 障害オブジェクトを追加するには、「**Add Failure Objects**」に正規表現を入力します。指定された正規表現に応じて、障害オブジェクトが自動的にリストに追加されます。

   「

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、手順 1で「**Enable Advanced Filter with Regex Matching**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高度な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、障害オブジェクトはユーザー名またはパスワードであり、`nsroot`のようになります。

4. エンティティを追加するには、「**Select Entities**」からエンティティを選択します。

   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を含めることができます。

手順 7 - 高度なフィルターを指定する

高度なフィルターを使用して、イベントルールをさらにフィルター処理できます。次のいずれかのフィルターを選択します。

- 「**Configuration Commands**」 - 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処理します。

  コマンドの認証ステータスと実行ステータスでイベントルールをフィルター処理することもできます。たとえば、`NetscalerConfigChange event`の場合、`[.]*bind system global policy_name[.]*`と入力します。

- 「**Messages**」 - 完全なメッセージ記述を指定するか、正規表現を指定してイベントをフィルター処理します。

  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。

  高度なメッセージフィルター(/en-us/netscaler-console-service/media/advance-filters-messages.png)

重要:

アスタリスク (*) パターンマッチング以外の正規表現を使用して構成コマンドとメッセージをフィルタリングするには、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.

ステップ 8 - 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、ステップ 7 で設定した定義済みのフィルター条件をイベントが満たした場合に送信または実行されます。

1. **アクションの追加** をクリックします。
2. **イベントアクションの追加** ページで、次のイベントアクションを追加できます。

- メール送信アクション
- トラップ送信アクション
- コマンド実行アクション
- ジョブ実行アクション
- 抑制アクション
- Slack 通知の送信
- PagerDuty 通知の送信
- ServiceNow 通知の送信

メール送信アクション

メール送信アクションを選択すると、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。

1. **メール配信リスト**。メール配信リストを選択します。配信リストを追加するには、 をクリックします。

   a. **メール配信リストの作成**ページで、次の操作を行います。

      i. **名前**。配信リストの名前を追加します。

      ii. **メールサーバー**。メールサーバーを選択します。サーバーを追加したり、既存のサーバーを編集したりすることもできます。

      iii. **差出人**。送信者のメールアドレスを追加します。

      iv. **宛先**。受信者のメールアドレスを追加します。CCおよびBccリストに含めるメールアドレスを指定することもできます。

      v. **作成**をクリックします。

2. **件名**。影響を受けるエンティティの名前、つまり障害オブジェクトの名前など、メールの件名を追加します。この件名行は、これらのイベントが発生する仮想サーバーに関する情報を提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注記:

件名行を追加しない場合、デフォルトの件名行が表示されます。デフォルトの件名行は、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のみを提供します。イベントが発生した仮想サーバーの名前は利用できません。

3. **添付ファイル**。メールに添付ファイルをアップロードします。この添付ファイルは、受信イベントが設定されたルールと一致したときに送信されます。
4. **テスト**。メールサーバー、関連する配信リスト、およびその他の設定を構成した後、このボタンをクリックしてテストメールを送信します。このオプションを使用すると、構成された設定をテストできます。
5. **イベントがクリアされるまでメール通知を繰り返す**。このオプションを選択すると、重要なイベントのメール通知を見逃さないようにすることができます。このオプションは、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を送信します。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たとします。問題が解決するまで通知を受け取りたい場合は、こ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します。

6. **OK** をクリックします。

注:

設定 > **通知** > **メール** に移動して、メール配信リストを追加することもできます。**追加** をクリックしてリストを作成します。

トラップ送信アクション

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。イベントが定義されたフィルタ条件を満たすと、トラップメッセージは特定のトラップリスナーに送信されます。

1. **トラップ配信リスト**。トラップ配信リスト (またはトラップ宛先とトラッププロファイルの詳細) を選択します。トラップ配信リストを作成するには、**追加** をクリックします。
2. **トラップ配信リストの作成** ページで、次の操作を行います。

   a. **プロファイル名**。プロファイル名を入力します。

   b. **トラップ宛先**。トラップメッセージを受信するインスタンスの名前または IP アドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **SNMP トラップのポート番号**。ポート番号を入力します。

d. **トラップコミュニティ**。インスタンスが属するグループを入力します。

e. **作成** をクリックします。

3. **OK** をクリックします。

コマンド実行アクション

コマンド実行アクションイベントアクションを選択すると、特定のフィルター条件に一致するイベントに対してNetScaler Consoleで実行できるコマンドまたはスクリプトを作成できます。

コマンド実行アクションスクリプトに対して、以下のパラメータも設定できます。

パラメータ	説明
ソース	このパラメータは、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	このパラメータは、フィルターのカテゴリで定義されている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。
障害オブジェクト	障害オブジェクトは、イベントの処理方法に影響を与え、通知されたとおりに正確な問題を表示するようにします。これにより、単に生のイベントを報告するのではなく、問題を迅速に追跡し、障害の原因を特定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注記:

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**の場合に、実行コマンドアクションを設定したいとします。管理者として、別の仮想サーバーを追加することで、迅速な回避策を提供したいと考えるかもしれません。NetScaler Consoleでは、次のことができます。

- スクリプト (.sh) ファイルを作成します。

  以下はスクリプト (.sh) ファイルのサンプルです。

```
#!/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 ファイルをエージェント上の永続的な場所に保存します。例: `/var`。
- ルール条件が満たされたときに実行されるように、NetScaler Consoleで.shファイルの場所を指定します。

1. **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**。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**。スクリプトを実行する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

> **注記:**
>
> NetScaler Consoleサーバーのログファイルに、コマンドスクリプトを実行したときに生成された出力とエラー（もしあれば）を保存したい場合は、**出力の追加**と**エラーの追加**オプションを有効にできます。これらのオプションを有効にしない場合、NetScaler Consoleは、コマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

d. **作成**をクリックします。

2. ページで、 をクリックします。

> **注:**
>
> NetScaler Consoleサーバーのログファイルに、コマンドスクリプトの実行時に生成された出力とエラー（もしあれば）を保存したい場合は、 オプションと オプションを有効にできます。これらのオプションを有効にしない場合、NetScaler Consoleはコマンドスクリプトの実行中に生成されたすべての出力とエラーを破棄します。

ジョブアクションの実行

構成ジョブでプロファイルを作成すると、指定したフィルター条件に一致するイベントおよびアラームに対して、NetScalerおよびNetScaler SDXインスタンスの組み込みジョブまたはカスタムジョブとしてジョブが実行されます。

1. で、ジョブプロファイルを選択します。リストを追加するには、 をクリックします。
2. ページで、次の操作を行います。

a. 。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するジョブを含むプロファイルを作成します。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するアクションを指定します。

b. 。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、変数値を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. をクリックしてジョブを作成します。

3. をクリックします。

抑制アクション

- に、イベントが抑制または破棄される期間を分単位で入力します。イベントは最低1分間抑制できます。

  イベントを抑制(/en-us/netscaler-console-service/media/createer11.png)

  注:

  抑制時間を0分に設定することもでき、これは無限の時間を意味します。時間期間を指定しない場合、NetScaler Consoleは抑制時間をゼロとみなし、期限切れになることはありません。

Slack通知を送信する

Slackチャネルを設定すると、イベント通知が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. **Slackプロファイルリスト**で、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。
2. **Slackプロファイルの作成**ページで、次の操作を行います。
   a. **プロファイル名**。NetScaler Consoleで設定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**。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。すべてのイベント通知はこのURLに送信され、選択した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>`
   d. **作成**をクリックします。
3. **OK**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

設定 > **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**をクリックしてプロファイルを作成します。

PagerDuty通知を送信する

NetScaler ConsoleでPagerDutyプロファイルを追加して、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。

1. **PagerDutyプロファイルリスト**で、PagerDutyプロファイルを選択します。プロファイルを追加するには、**追加**をクリックします。
2. **PagerDutyプロファイルの作成**ページで:
   a. **プロファイル名**。任意のプロファイル名を入力します。
   b. **統合キー**。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。

NetScaler ConsoleにPagerDutyプロファイルを追加する前に、PagerDutyで必要な設定が完了していることを確認してください。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ためのオプションの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。

ユースケース:

次のシナリオを検討してください。

- PagerDutyプロファイルに通知を送信します。
- PagerDutyで通知を受け取るためのオプションとして、電話を設定します。
- NetScalerイベントの電話アラートを受け取ります。

PagerDutyの設定を作成します。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。電話で、次のことを決定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

ServiceNow通知を送信する

NetScaler Console GUIでServiceNowプロファイルを選択することで、NetScaler ConsoleイベントのServiceNowインシデントを自動生成できます。イベントルールを設定するには、NetScaler Consoleで**ServiceNow**プロファイルを選択する必要があります。

ServiceNowインシデントを自動生成するイベントルールを設定する前に、NetScaler ConsoleをServiceNowインスタンスと統合します。詳細については、「ServiceNow用ITSMアダプターの構成」を参照してください。

1. **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。
2. **OK**をクリックします。

イベントフィルターをスケジュールする

ルールにフィルターを作成した後、生成されたイベントがフィルター条件を満たすたびにNetScaler Consoleが通知を送信しないようにしたい場合は、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。

例えば、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 Console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 Consoleを使用してフィルターをスケジュールするには:

1. NetScaler Consoleで、**Infrastructure > Events > Rules** に移動します。
2. フィルターをスケジュールしたいルールを選択し、**View Schedule** をクリックします。
3. **Scheduled Rule** ページで、**Schedule** をクリックし、次のパラメーターを指定します。
    - **Enable Rule** – スケジュールされたイベントルールを有効にするには、このチェックボックスを選択します。
    - **Recurrence** - ルールをスケジュールする間隔。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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。

NetScalerインスタンスで発生するイベントの報告された重大度を変更する

すべてのデバイスで生成されたイベントのレポートを管理し、インスタンス上の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。また、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することもできます。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。

次の重大度レベルを定義できます: 致命的、メジャー、マイナー、警告、クリア。

イベントの重大度を変更するには:

1. **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。
2. 変更するNetScalerインスタンスタイプのタブをクリックします。次に、リストからカテゴリを選択し、**重大度の構成**をクリックします。
3. **イベントの重大度の構成**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。

イベントの概要を表示

NetScaler Consoleで受信したイベントとトラップを監視するためのイベント概要ページを表示できるようになりました。**インフラストラクチャ > イベント**に移動します。イベント概要ページには、以下の情報が表形式で表示されます。

- **NetScaler Consoleが受信したすべてのイベントの概要**。イベントはカテゴリ別に一覧表示され、異なる重大度が異なる列に表示されます: 重大、メジャー、マイナー、警告、クリア、情報。たとえば、Citrix Application Delivery Controller (NetScaler) インスタンスがダウンし、NetScaler Consoleへの情報の送信を停止した場合に、重大なイベントが発生します。イベント中に、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について説明する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、イベントの詳細にアクセスできます。

  イベントの概要(/en-us/netscaler-console-service/media/eventssummary.png)

© 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 Consoleに送信される各トラップには重大度が割り当てられていますが、ネットワーク管理者として、NetScaler Console GUIでその重大度を指定できます。

カテゴリタイプまたはトラップをクリックすると、**イベント**ページに移動し、カテゴリや重大度などのフィルターが事前に選択されています。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。

イベントの詳細(/en-us/netscaler-console-service/media/eventsinfo.png)

NetScaler Consoleでイベントを表示する日数を1日から40日の間で設定できます。たとえば、30日を選択した場合、NetScaler Consoleは30日間のイベントを表示し、30日後にイベントはクリアされます。このイベント設定を構成するには、**設定 > グローバル設定 > データ保持ポリシー**に移動します。詳細については、「データ保持ポリシー」を参照してください。

このダッシュボードのレポートをエクスポートするには:

このページのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページでは、次のいずれかを実行できます。

1. **今すぐエクスポート**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。
2. **エクスポートのスケジュール**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。

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ください。

イベントメッセージ

NetScaler® Consoleで受信したすべてのアクティブなイベントは、**Infrastructure > Events > Event Messages**ページに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Messagesページでは、インスタンスのリストとイベントの詳細（重大度、カテゴリ、イベント発生日時、障害オブジェクトなど）を表示できます。

イベントが発生した時間に基づいてイベントをフィルタリングできます。たとえば、過去30分、1時間、1日などです。また、好みに応じてカスタム時間を選択することもできます。

NetScaler ConsoleはカスタムSNMPトラップをサポートしており、**Event Messages**の下で**custom**としてタグ付けされます。**custom**タグは、それらをデフォルトのSNMPアラートと区別するのに役立ちます。

イベントメッセージ(/en-us/netscaler-console-service/media/event-messages.png)

イベントの重大度とSNMPトラップの詳細を表示する

NetScaler Consoleでイベントとその設定を作成すると、イベントサマリーページでイベントをすぐに表示できます。同様に、NetScaler Consoleサーバーに追加されたすべてのCitrix Application Delivery Controller (NetScaler) インスタンスの健全性、稼働時間、モデル、およびバージョンを、インフラストラクチャダッシュボードで詳細に表示および監視できます。

インフラストラクチャダッシュボードでは、関連性のない値をマスクできるようになり、重大度別のイベント、健全性、稼働時間、モデル、NetScalerインスタンスのバージョンなどの情報をより簡単に詳細に表示および監視できます。

例えば、**Critical** (重大) の重大度レベルのイベントはめったに発生しないかもしれません。しかし、これらの重大なイベントがネットワークで発生した場合、イベントがどこでいつ発生したかをさらに調査、トラブルシューティング、監視したいと思うかもしれません。Critical以外のすべての重大度レベルを選択すると、グラフには重大なイベントの発生のみが表示されます。また、グラフをクリックすると、**Severity based events** (重大度別イベント) 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、インスタンスがサービス停止中だった時間のみを表示できます。グラフをクリックすると、そのインスタンスのページに移動し、*out of service* (サービス停止中) フィルターがすでに適用されており、ホスト名、1秒あたりのHTTPリクエスト数、CPU使用率などの詳細を確認できます。インスタンスを選択して、インスタンスダッシュボードで詳細を確認することもできます。

NetScaler Consoleで重大度別に特定のイベントを選択するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Infrastructure > Instances** に移動します。

   または、,

   Infrastructure > Events > Reports に移動します。

3. ページの右上隅にあるドロップダウンリストから、重大度別にイベントを表示したい期間を選択します。

   イベント期間(/en-us/netscaler-console-service/media/masvc-events-report-severity-mask.png)

4. **Events by Severity** (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現します。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**Severity based events** (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関する以下の詳細が表示されます。

   - インスタンスソース
   - イベントのデータ
   - NetScalerインスタンスによって生成されたイベントのカテゴリ
   - 送信されたメッセージ通知

注:

ドーナツチャートの下には、チャートに表示されている重要度の一覧が表示されます。デフォルトでは、ドーナツチャートはすべての重要度タイプのすべてのイベントを表示するため、リスト内のすべての重要度タイプが強調表示されます。重要度タイプにカーソルを合わせると、選択した重要度をより簡単に表示および監視できます。

NetScaler ConsoleでNetScaler SNMPトラップの詳細を表示するには:

これで、管理対象のNetScalerインスタンスから受信した各SNMPトラップの詳細を、NetScaler Consoleの**イベント設定**ページで表示できるようになりました。**インフラストラクチャ > イベント > イベント設定**に移動します。インスタンスから受信した特定のトラップについて、以下の詳細を表形式で表示できます。

- **カテゴリ** - イベントが属するインスタンスのカテゴリを指定します。
- **重要度** - イベントの重要度は、色とその重要度タイプによって示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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**aggregateBWUseNormal**のイベントの場合、トラップの説明は「このトラップは、システムの集約帯域幅使用量が正常に戻ったときに送信されます。」と表示されます。

syslogメッセージの表示とエクスポート

NetScaler Consoleにログインすることなく、サーバーで受信したすべてのsyslogメッセージのエクスポートをスケジュールすることで、syslogメッセージを表示できます。Citrix Application Delivery Controller (NetScaler) インスタンスで生成されたsyslogメッセージをPDF、CSV、PNG、JPEG形式でエクスポートできます。また、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することもできます。

syslogメッセージの表示

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。メッセージを表示するには、インスタンスがsyslogメッセージをNetScaler Consoleサーバーにリダイレクトするように構成する必要があります。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Syslog Viewerで利用できます。このログ情報を組み合わせて、収集されたデータから分析レポートを作成できます。

syslogを構成して、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。

Syslog Viewerを表示するには、**Infrastructure > Events > Syslog Messages**に移動します。適切なフィルターを選択して、システムログメッセージを表示します。

syslogメッセージの検索

フィルターを使用してsyslogメッセージと監査ログメッセージを検索し、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。

NetScaler Consoleソフトウェアに存在するすべてのNetScalerインスタンスのsyslogメッセージを検索するには、NetScaler Console GUIから**Infrastructure > Events > Syslog Messages**に移動します。新しいフィルターカテゴリは、インスタンス、モジュール、イベント、重大度、メッセージです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleソフトウェアに存在するすべてのNetScaler Consoleシステム監査ログメッセージを検索するには、NetScaler Console GUIから**Settings > Audit Log Messages**に移動します。新しいフィルターカテゴリは、インスタンス、モジュール、イベント、重大度、メッセージです。

NetScaler Consoleに存在するすべてのアプリケーションの監査ログメッセージを検索するには、NetScaler Console GUIから**Infrastructure > Network Functions > Auditing**に移動します。

NetScaler Console上の特定のアプリケーションの監査ログメッセージを検索するには、NetScaler Console GUIから**Application > Dashboard**に移動し、監査ログメッセージを検索する仮想サーバーを選択します。次に、**Audit Log**タブをクリックします。

フィルターカテゴリを選択したら、検索語句と等しいか、または検索語句を含むかを指定します。

次に、検索語句を追加します。一部のカテゴリでは、事前入力された検索語句のリストが表示されます。デフォルトでは、検索期間は1日です。下矢印をクリックして、時間と日付の範囲を変更できます。**Syslog Summary**または**Audit Log 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

NetScaler Consoleを使用してsyslogメッセージレポートをエクスポートするには：

1. **Infrastructure > Events > Syslog Messages** に移動します。
2. 右側のペインで、Syslog Messagesページの右上隅にあるエクスポートボタンをクリックします。
3. **Export Now** で、必要な形式を選択し、**Export** をクリックします。

NetScaler Consoleを使用してsyslogメッセージレポートのエクスポートをスケジュールするには：

1. **Infrastructure > Events > Syslog Messages** に移動します。
2. **Syslog Messages** ページの右側のペインで、**Export** をクリックします。
3. **Schedule Report** タブで、次のパラメータを設定します。
   - **Description**: レポートをエクスポートする理由を説明するメッセージ。
   - **Format**: レポートをエクスポートする形式。
   - **Recurrence**: レポートをエクスポートする間隔。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Export Time**: レポートをエクスポートする時刻。現地時間帯の24時間形式で時刻を入力します。
- **メール配信リスト**: レポートをメールで受信する受信者のリストです。提供されたリストからメール配信リストを選択します。レポートが生成され、スケジュールされた時間条件を満たすと、メールがトリガーされます。メール配信リストを作成する場合は、**+** をクリックして、メールサーバーとメールプロファイルの詳細を指定します。

syslogメッセージの抑制

syslogサーバーとして構成されている場合、NetScaler Consoleは、構成済みのCitrix Application Delivery Controller (NetScaler) インスタンスからすべてのsyslogメッセージを受信します。表示したくないメッセージが多数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は関心がないかもしれません。関心のないsyslogメッセージの一部を破棄できるようになりました。いくつかのフィルターを設定することで、NetScaler Consoleに入ってくるsyslogメッセージの一部を抑制できます。NetScaler Consoleは、基準に一致するすべてのメッセージを破棄します。これらの破棄されたメッセージはNetScaler Console GUIには表示されず、顧客のNetScaler Consoleデータベースにも保存されません。

いくつかのフィルターを設定することで、NetScaler Consoleに入ってくるログに記録されたsyslogメッセージの一部を抑制できます。syslogメッセージの抑制に使用できる2つのフィルターは、重大度とファシリティです。特定のNetScalerインスタンスまたは複数のインスタンスから送信されるメッセージを抑制することもできます。NetScaler Consoleがメッセージを検索して抑制するためのテキストパターンを提供することもできます。NetScaler Consoleは、基準に一致するすべてのメッセージを破棄します。これらの破棄されたメッセージはNetScaler Console GUIには表示されず、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ためのいくつかのユースケースは次のとおりです。

- すべての情報レベルのメッセージを無視したい場合は、レベル6（情報）を抑制します。
- ファイアウォールのエラー状態のみを記録したい場合は、レベル3（エラー）以外のすべてのレベルを抑制します。

フィルターを作成してsyslogメッセージを抑制する

1. NetScaler Consoleで、**インフラストラクチャ > イベント > Syslogメッセージ** に移動します。
2. 歯車アイコンをクリックして、**抑制フィルター** ページを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

syslogメッセージを抑制する(/en-us/netscaler-console-service/media/suppress-filter-button.png)

3. **抑制フィルター** ページで、**追加** をクリックします。
4. **抑制フィルターの作成** で、次の情報を更新します。

   a. **名前** - フィルター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、ユーザーはアクセス権を持つすべてのインスタンスのフィルターのみを表示できるため、インスタンスごとに異なるフィルターを作成する必要があります。

   b. **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、受信す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。

   抑制フィルターを作成(/en-us/netscaler-console-service/media/create-suppress-filter.png)

   d. **ファシリティ** - メッセージを生成するソースに基づいてメッセージを抑制するファシリティを選択します。

   e. **メッセージパターン** - アスタリスク (*) で囲まれたテキストパターンを入力して、メッセージを抑制することもできます。メッセージはテキストパターン文字列で検索され、このパターンを含むメッセージは抑制されます。

フィルターの無効化

NetScaler Consoleでメッセージを表示できるようにするには、フィルターを無効にする必要があります。

1. **Infrastructure > Events > Syslog Messages**に移動します。
2. 歯車アイコンをクリックして、**抑制フィルター**ページを表示します。
3. **抑制フィルター**ページで、フィルターを選択し、**編集**をクリックします。
4. **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。

   抑制フィルター(/en-us/netscaler-console-service/media/disable-suppress-filter.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSLダッシュボード

NetScaler Consoleは、証明書管理のあらゆる側面を効率化します。単一のコンソールを通じて、適切な発行者、鍵強度、正しいアルゴリズムを確保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厳密に監視できます。NetScaler Console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、そしてNetScaler Consoleを使用してSSL証明書を追跡する方法を理解する必要があります。

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含まれており、サーバーとの安全なトランザクションを開始したいクライアントから参照できます。対応する秘密鍵はNetScalerアプライアンスに安全に保存されており、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。

SSL証明書と鍵は、以下のいずれかの方法で取得できます。

- 認証局 (CA) から
- NetScalerアプライアンスで新しいSSL証明書と鍵を生成する

NetScaler Consoleは、管理対象のすべてのNetScalerインスタンスにインストールされているSSL証明書を一元的に表示します。SSLダッシュボードでは、証明書の発行者、鍵強度、署名アルゴリズム、期限切れまたは未使用の証明書などを追跡するのに役立つグラフを表示できます。また、仮想サーバーで実行されているSSLプロトコルの分布や、それらで有効になっている鍵も確認できます。

証明書の有効期限が近づいている場合や、その証明書を使用しているNetScalerインスタンスに関する情報を含めて通知を設定することもできます。

NetScalerインスタンス証明書をCA証明書にリンクできます。ただし、同じCA証明書にリンクする証明書は、同じソースと同じ発行者であることを確認してください。1つ以上の証明書をCA証明書にリンクした後、それらのリンクを解除できます。

注記:

NetScaler ConsoleでVenafi Trust Protection Platformサーバーを使用して、SSL証明書のライフサイクル全体を自動管理することもできます。詳細については、「SSL証明書管理の自動化」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACMEプロトコルを使用した証明書の自動更新

NetScaler Consoleは、SSL/TLS証明書の更新を自動化するために設計されたオープンプロトコルであるACME（Automated Certificate Management Environment）をサポートしています。

以前は、ネットワーク管理者は証明書の更新に、手間のかかる多段階の手動プロセスを経る必要がありました。ACMEサポートは、証明書の自動更新のための堅牢なフレームワークを提供することで、これらの課題を軽減し、以下の操作を実行します。

- 信頼できる認証局（CA）から新しい証明書を要求する。
- 自動化された方法を使用してドメインの所有権を検証する（現在、NetScaler ConsoleはDNS-01チャレンジのみをサポートしています）。
- 有効期限が切れる前に証明書を自動的に更新する。

NetScaler® ConsoleでのACMEサポート

NetScaler Consoleは`acme.sh`クライアントを使用し、以下の認証局をサポートしています。

- レッツエンクリプト
- DigiCert Inc
- セクティゴ・リミテッド
- エントラスト・インク
- GlobalSign
- GoDaddy.com, Inc
- ZeroSSL
- グーグル トラスト サービス
- グーグル 公開 認証局
- BuyPass Go SSL
- アクタリス
- SSL.com
- ハシコープ ヴォールト
- スモールステップ
- ペブル
- HARICA
- EJBCA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® Console での証明書の自動更新の仕組みを以下の手順で説明します。

1. NetScaler Console が `acme.sh` クライアントを使用してドメインの証明書要求を開始すると、クライアントは選択された認証局 (例: Let's Encrypt または DigiCert) に接続します。
2. 認証局はドメイン所有権を証明するためのチャレンジを発行します。この場合、それは DNS-01 チャレンジです。
3. NetScaler Console は、事前に設定された資格情報を使用して、認証局から提供された値でドメインの DNS TXT レコードを自動的に更新します。
4. 認証局は TXT レコードを検証し、ドメイン所有権を確認します。
5. 正常な検証が完了すると、CAはSSL/TLS証明書をNetScaler Consoleに発行します。
6. NetScaler Consoleは、証明書をそれぞれのストア（証明書ストア/ゼロタッチストア）に保存します。
7. お客様が指定した更新期間に基づいて、NetScaler Consoleは証明書の有効期限が切れる前に、この更新プロセスを自動的に繰り返します。

ACMEサポートのハイレベルアーキテクチャ(/en-us/netscaler-console-service/media/acme-high-level-architecture.png)

NetScaler ConsoleのACMEサポートにより、以下の操作を実行できます。

- 証明書の有効期限が切れる前に自動的に更新する
- 更新時にあるCAから別のCAに切り替える
- CSRを生成またはアップロードし、新しい証明書を要求する

主な利点は次のとおりです。

- 証明書の発行または更新において手動介入なしの完全自動化されたライフサイクル。
- 組織のニーズに合わせたカスタマイズ可能な更新スケジュール（例：有効期限の7日前に更新するように設定）。
- 有効期限切れの証明書によるダウンタイムを排除します。
- 有効期限の追跡と更新を自動化することで、運用上のオーバーヘッドを削減します。
- 常に有効で、CAのベストプラクティスに準拠した証明書により、セキュリティ体制が向上します。

ACME統合のための構成手順

ACMEの統合は一度限りのプロセスであり、以下の手順が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ステップ1：認証局（CA）を構成します。
- ステップ2：更新する証明書を選択します。
- ステップ3：DNSプロバイダーを追加し、対応するドメインをマッピングします。

前提条件

- 認証局（CA）の有効なアカウントと、そのライセンスがあることを確認してください。
- DNSプロバイダーのアクセス資格情報があることを確認してください。

ステップ1：認証局（CA）を構成する

更新に使用される認証局（CA）を登録するには、以下の手順を実行します。

1. **Infrastructure > SSL Dashboard** に移動します。ACMEを初めて構成する場合、「SSL証明書の自動更新」というバナーが表示されます。**Get Started** をクリックします。

   ACMEの開始(/en-us/netscaler-console-service/media/acme-get-started.png)

   または

   Infrastructure > SSL Dashboard > Third-party Integration > CA Vendors に移動し、**Add** をクリックします。
2. 名前を入力し、CAベンダーを選択します。
3. メールアドレス、ACME Directory URLなどのその他の詳細情報を提供します。
4. NetScaler Console が証明書を自動的に更新する必要がある日数。
5. 「**保存して続行**」をクリックします。NetScaler Console は CA への接続を試行します。接続に失敗した場合は、提供された詳細を確認し、構成の詳細を修正してから再試行してください。

   ▢

ステップ2：更新する証明書を選択する

CA の詳細が追加されると、NetScaler Console はすべての証明書（証明書ストアとゼロタッチストアの両方から）を自動的にスキャンし、構成された CA によって発行された証明書を個別にリストします。リストされた証明書を確認します。

1. 自動的に更新したい証明書を選択します。たとえば、Let’s Encrypt を CA として構成し、Let’s Encrypt から 2 つの証明書、別のベンダーから 2 つの証明書がある場合、ダッシュボードには次のように表示されます。`Let’s Encrypt: 2 and Other CA: 2`。

   ▢

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 別の CA によって発行された証明書を追加するには「**追加**」をクリックするか、自動的に更新したくない証明書を削除するには「**削除**」をクリックします。別のベンダーの証明書を選択した場合、ベンダー変更を確認するプロンプトが表示されます。確認すると、これらの証明書は更新期間に達したときに、新しく構成された CA を介して更新されます。

   注:

   証明書ストアとゼロタッチ証明書ストアに重複する証明書がないことを確認してください。重複する証明書がある場合、更新プロセスは各ストアで2回実行されます。

3. 「**保存して続行**」をクリックします。

   注:

   証明書は更新後もそれぞれのストアに残ります。たとえば、証明書が証明書ストアに保存されている場合、その更新されたバージョンも証明書ストアに配置されます。証明書がゼロタッチストアに保存されている場合、その更新されたバージョンもゼロタッチストアに配置されます。

   証明書の展開動作はストアの種類によって異なります。

   - 証明書が証明書ストアに保存されている場合、それらは手動でNetScalerに展開する必要があります。
   - 証明書がZero-touchストアに保存されている場合、証明書は管理者の介入なしに自動的にNetScalerに展開されます。 更新された証明書のシームレスで完全に自動化された展開には、Zero-touch Certificate Managementを使用することをお勧めします。詳細については、「Zero-touch certificate management」を参照してください。

ステップ3：DNSプロバイダーを追加し、ドメインをマッピングする

1. **DNS provider & domain mapping**ページで**Add**をクリックします。
2. **Select DNS provider**ドロップダウンリストからDNSプロバイダーを選択します。`acme.sh`でサポートされているDNSプロバイダーがドロップダウンリストに表示されます。リストにDNSプロバイダーが表示されない場合、それはサポートされていないことを意味します。
3. Access key ID、Secret Access Keyなどのプロバイダーの詳細を入力し、**Save**をクリックして設定を保存します。
4. **Domain Mapping**の下にある**Add Domain**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 設定済みのDNSプロバイダーによって提供されるドメインを選択します。

重要：

各ドメインが正しいDNSプロバイダーにリンクされていることを確認してください。NetScaler Consoleはこれらのマッピングを使用して、DNS-01チャレンジを自動的に実行します。発行または更新中に、NetScaler ConsoleはマッピングされたDNSプロバイダーに必要なTXTレコードを作成します。検証が成功すると、CAは証明書を発行または更新します。証明書は、関連するすべてのドメインがDNSプロバイダーに正しくマッピングされている場合にのみ更新されます。

たとえば、組織がAmazon Route53をDNSプロバイダーとして使用している場合。まず、DNS Provider Detailsの下にAmazon Route53の資格情報（Access Key IDとSecret Key）を追加します。次に、Amazon Route53によって管理されるドメイン（例：example.com、app.example.com）をマッピングします。これらのドメインの証明書が発行または更新されると、NetScaler ConsoleはAmazon Route53に必要なTXTレコードを自動的に作成します。検証が成功すると、CAは証明書を発行または更新します。
以下のパブリックDNSプロバイダーがサポートされています。

- 1984.ホスティング
- ACME DNS
- アクメプロキシ サーバー API
- アクティブ24
- Akamai.com エッジDNS
- アリユン
- All-inkl Kasサーバー
- Alviy.com
- アマゾン ルート53
- Anexia.com CloudDNS
- ArtFiles.de
- ArvanCloud.ir
- autoDNS-InternetX
- アジュール DNS
- Azion.om

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Beget.com
- BookMyName.com
- Bunny.net
- クラウドフレア
- ClouDNS.net
- ConoHa
- Constellix.com
- コアネットワーク
- cPanelサーバーAPI
- Curanet.dk
- cyon.ch
- DDNSS.de
- deSEC.io
- デジタルオーシャン
- DirectAdmin
- DNSサービス
- DNSExit.com
- dns.la
- DNSMadeEasy
- ディーエヌシンブル
- dnsHome.de
- DNSPod.cn
- DNSPod.com
- ドメインオフェンシブ do.de
- DomeneShop.no
- DreamHost
- DuckDNS.org
- durabledns.com
- Dyn.com
- DynDnsFree.de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Dynu.com
- DynV6.com
- easyDNS.net
- エッジセンター DNS API
- EUserv.com
- エクソスケール
- Fornex.com
- FreeDNS
- FreeMyIP.com
- ガンディ ライブDNS
- Gcore.com
- GeoScaling.com
- GoDaddy.com
- グーグル クラウド DNS
- グーグル ドメイン
- Hetzner.com
- Hexonet.com
- hosting.de
- HuaweiCloud.com
- ハリケーンエレクトリック
- ハリケーンエレクトリック HE.net DDNS
- インフォブロックス
- Infomaniak.com
- INWX
- IONOS クラウド DNS
- IONOS.de
- InternetBS.net
- ISPコンフィグ 3.1
- jdcloud.com
- Joker.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- kapper.net
- King.host
- ノットDNS
- Leaseweb.com
- Lexicon DNS クライアント
- リマシティ.de
- リノード
- Linode.com-Old
- ルーピア
- LuaDNS
- MailinaBox
- MaraDNS
- mijn.host
- Misaka.io
- MyDNS.JP
- ミシックビースト.com
- Name.com
- ネームチャープ
- NameMaster.de
- ネームシロ
- Nanelo.com
- NederHost.nl
- Neodigit.net
- ネットカップ
- Netlify.com
- nic.ru
- ニャラ
- NLnetLabs NSD
- NS1.com
- ネクセス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- one.com
- Online.net
- omg.lol
- OpenProvider
- オープンスタック デザインエイト API
- オーピーエヌセンス
- オラクル クラウド インフラストラクチャ - OCI
- OVH.com
- プレスク XML
- PointHQ
- Porkbun.com
- PowerDNS
- RackCorp.com
- RackSpace.com
- rage4.com
- RcodeZero
- reg.ru
- ScaleWay.com
- シュルントテック
- セレクテル
- SelfHost.de
- ServerCow.de
- Simply.com
- テクニティウム DNS サーバー
- tele3.cz
- Tencent.com
- Timeweb.Cloud
- TransIP.nl
- UltraDNS
- ユナイテッドドメインズ リセリング

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- unoeuro.com
- variomedia.de
- Vercel.com
- veesp.com
- versio.nl AuroraDNS
- VSCALE
- vshosting.cz CloudDNS
- ヴァルチャー
- Websupport.sk
- West.cn
- World4You.com
- ヤンデックス 360 for Business DNS API。
- ヤンデックス クラウド DNS
- ジローレ
- Zone.eu
- ZoneEdit.com
- ゾノミ

これら3つのステップがすべて完了すると、NetScaler ConsoleはACME CAサーバーを設定します。選択された証明書は、マッピングされたドメインに対して更新されます。 NetScaler Consoleは定期的に証明書の有効性をチェックし、有効期限が切れる前に（設定された期間に基づいて）更新します。手動での介入は不要で、証明書は常に有効で最新の状態に保たれます。

発行と更新

証明書の発行から発生したすべての更新アクティビティと新しいリクエストを確認するには、**Infrastructure > SSL Dashboard > Issuance & Renewals** に移動します。

自動更新

Automatic renewals タブには、自動更新に登録されている証明書が一覧表示されます。設定された更新期間に達すると、NetScaler Consoleはそれらを自動的に更新します。

スケジュールされた更新期間の前に、オンデマンドで更新をトリガーすることもできます。オンデマンド更新の場合は、必要な証明書を選択し、**Renew now** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一部の証明書を自動的に更新したくない場合は、手動更新に移行できます。証明書を自動更新から手動更新に移行するには、必要な証明書を選択し、**Migrate to manual renewal** をクリックします。

手動更新

Manual renewals タブには、手動で更新する必要があるすべての証明書が一覧表示されます。これらの証明書は、オフラインで証明書を更新して新しい証明書を適切なストアにアップロードするか、**Renew now** オプションを使用して手動で更新する必要があります。

証明書を更新するには、証明書を選択して **Renew now** をクリックします。証明書が登録済みのCAによって発行され、そのドメインのDNSプロバイダーが設定されている場合、自動更新に移行することなく、ACMEを使用してオンデマンドで更新できます。

証明書を自動更新に移行することもできます。証明書を手動更新から自動更新に移行するには、必要な証明書を選択し、**Migrate to automatic renewal** をクリックします。

注記：

一度に更新または移行できる証明書は1つだけです。

ACMEサポートのハイレベルアーキテクチャ(/en-us/netscaler-console-service/media/acme-manual-renewals.png)

発行と更新のログ

発行と更新のログタブには、ACMEを使用した証明書要求（発行と更新を含む）のリストが表示されます。失敗したイベントについては、情報アイコンをクリックして詳細なエラー情報を表示できます。

ACMEサポートのハイレベルアーキテクチャ(/en-us/netscaler-console-service/media/acme-issuance-renewal-logs.png)

証明書の発行

NetScaler ConsoleにおけるACME統合は、ACMEプロトコルを使用して新しい証明書を直接要求することをサポートしています。NetScaler Console内でCSRを作成するか、既存のCSRをアップロードして新しい証明書を要求できます。

Infrastructure > SSL dashboard > Issuances & Renewalに移動し、**Issue Certificate**をクリックして、シナリオに基づいて以下のいずれかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **CSRがありません**: CSRをまだ持っていない場合、NetScaler ConsoleでCSRを生成し、新しい証明書を発行できます。
- **CSRがあります**: オフラインで生成されたCSRをすでに持っている場合、それをアップロードして証明書を発行できます。

CSRなしで証明書を発行する

CSRを生成して新しい証明書を発行するには、以下の手順を実行します。

1. **Infrastructure > SSL dashboard > Issuances & Renewal**に移動し、**Issue Certificate**をクリックして、**CSRがありません**を選択します。

   ACMEサポートの証明書発行(/en-us/netscaler-console-service/media/acme-issue-certificate.png)

2. **証明書キー**ページで、**キーがあります**を選択して既存のキーをアップロードするか、**キーがありません**を選択して新しいキーを生成します。

   ACME証明書キー(/en-us/netscaler-console-service/media/acme-certificate-key-without-csr.png)

3. 必要なCSR情報を入力します。

   ACME CSR情報(/en-us/netscaler-console-service/media/acme-csr-details.png)

4. ACMEリクエストのCA、DNSプロバイダー、および証明書展開モードを選択します。手動展開の場合は**Cert Store**を、NetScalerでの自動展開の場合は**Zero Touch Store**を選択します。
5. 将来的に証明書を自動更新したい場合は、**証明書を自動更新**を選択します。

   ACME CSR情報(/en-us/netscaler-console-service/media/acme-certificate-store-without-csr.png)

6. **保存**をクリックします。

CSRを使用して証明書を発行する

オフラインで生成されたCSRをすでに持っており、それをアップロードして証明書を発行したい場合は、以下の手順を実行します。

1. **Infrastructure > SSL dashboard > Issuances & Renewal**に移動し、**Issue Certificate**をクリックして**I have CSR**を選択します。

   ACMEサポート証明書の発行(/en-us/netscaler-console-service/media/acme-issue-certificate.png)

2. ローカルシステムからCSRファイルと関連するキーファイルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ACME CSR情報(/en-us/netscaler-console-service/media/acme-csr-file-selection.png)

3. ACMEリクエストのCA、DNSプロバイダー、および証明書展開モードを選択します。手動展開の場合は**Cert Store**を、NetScalerでの自動展開の場合は**Zero Touch Store**を選択します。
4. 将来的に証明書を自動更新したい場合は、**証明書を自動更新**を選択します。

   ACME CSR情報(/en-us/netscaler-console-service/media/acme-issue-certificate-with-csr.png)
5. 「**保存**」をクリックします。

サードパーティ統合

複数のCAベンダーとDNSプロバイダーを追加および管理できます。

「**サードパーティ統合**」ページから次のアクションを実行できます。

- CAベンダーの追加または編集
- 自動更新設定の変更
- 既存の構成済みCAからの証明書の追加または編集
- DNSプロバイダーの追加または編集
- ドメインマッピングの変更

CAベンダーの追加または編集

複数のCAベンダーを登録して、異なるベンダーによって発行された証明書を管理できます。また、既存のCAベンダーの詳細を編集することもできます。

1. **SSL dashboard > Third party integration > ACME > CA Vendors** に移動します。「**追加**」をクリックします。
2. CAベンダーを追加するには、CAベンダーの名前を指定し、CAを選択します。
3. 既存のCAベンダーの詳細を編集するには、CAベンダーを選択し、「**編集**」をクリックします。
4. 必要な詳細を追加または更新します。
5. **保存**をクリックします。

自動更新設定を変更する

自動更新設定を変更するには、次の手順を実行します。

1. **SSLダッシュボード > サードパーティ統合 > ACME > CAベンダー**に移動します。
2. CAベンダーを選択し、**編集**をクリックします。
3. **証明書認証局ベンダーの構成**で、**自動更新設定**セクションの要件に応じて日数を変更します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **保存して続行**をクリックします。
5. ワークフローを完了します。

既存の構成済みCAから証明書を追加または編集する

既存の構成済みCAから証明書を追加または編集するには、次の手順を実行します。

1. **SSLダッシュボード > サードパーティ統合 > ACME > CAベンダー**に移動します。
2. CAベンダーを選択し、**編集**をクリックします。
3. **ステップ2 証明書の選択**に移動し、必要な証明書を追加または削除します。
4. **保存して続行**をクリックします。
5. ワークフローを完了します。

注:

証明書が元のCAからマッピング解除されていない場合、新しいCAの選択リストには表示されません。

DNSプロバイダーの追加または編集

新しいDNSプロバイダーを追加するか、既存のDNSプロバイダーの既存のドメインマッピングを編集するには、次の手順を実行します。

1. **SSLダッシュボード > サードパーティ統合 > ACME > DNSプロバイダー**に移動します。
2. DNSプロバイダーを追加するには、**追加**をクリックします。DNSプロバイダーを選択し、**保存**をクリックします。
3. 既存のDNSプロバイダーを編集するには、DNSプロバイダーを選択し、**編集**をクリックします。
4. 必要な詳細を追加または更新します。
5. **保存**をクリックします。

ドメインマッピングの変更

既存のDNSプロバイダーのドメインマッピングを編集するには、次の手順を実行します。

1. **SSLダッシュボード > サードパーティ統合 > ACME > DNSプロバイダー**に移動します。
2. DNSプロバイダーを選択し、**編集**をクリックします。
3. **ドメインマッピング**に移動し、必要に応じてドメインを追加または削除します。
4. **保存**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

ドメインがマッピング解除されると、その証明書の更新は停止します。更新が継続されるように、常にドメインを有効なDNSプロバイダーに再マッピングしてください。

制限事項

- 証明書の更新は、`acme.sh`でサポートされているDNSプロバイダーに対してのみ行われます。

自動証明書更新に関する問題のトラブルシューティング

発生する可能性のある一般的なエラーメッセージとその根本原因をこのセクションに示します。

- **Certificate has invalid domain - ADCD**エラーは、ACME要件に従って証明書内のドメイン名が有効でない場合に報告されます。
- 要求されたドメイン名にドットがない場合（「example.com」ではなく「example」など）、**Invalid identifiers requested :: Cannot issue for "testdomain": Domain name needs at least one dot**が報告されます。
- ACMEクライアントがCAからノンスを取得できない場合（多くの場合、ネットワークまたはサーバーの問題が原因）、**Could not get nonce from the CA server. Please check the CA server configuration.**が報告されます。
- ACMEクライアントがCAサーバーとの通信を初期化できない場合（設定ミスが原因である可能性あり）、**Cannot initialize API for the CA server. Please check the CA server configuration.**が報告されます。
- ドメイン名の形式が無効であるか、ACMEプロトコルで許可されていない場合、**Invalid domain name provided. Please check the domain name and try again.**が報告されます。
- ドメインリストに変更がなく、証明書がすでに存在する場合に証明書要求が行われると、**Domains not changed. Certificate with same configuration already exists.**が報告されます。
- ACMEクライアントがドメイン検証に必要なDNS TXTレコードの追加に失敗した場合、**Error adding TXT record for domain validation. Please check the DNS configuration and try again.**が報告されます。
- 署名が一致しない場合（多くの場合、クライアントとサーバー間の時刻同期の問題が原因）、**Signature does not match. Please check the server time as it may not be in sync.**が報告されます。
- DNSベースのドメイン検証にDNSプロバイダーが指定されていない場合、**Certificate is missing a DNS provider name.**が報告されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**アクティブなDNSプロバイダーが設定されていないため、更新がスキップされました。**」は、証明書の更新が試行されたが、アクティブなDNSプロバイダーが設定されていない場合に報告されます。
- 「**連絡先の検証エラー :: メールアドレスを解析できません**」は、提供された連絡先メールアドレスが無効であるか、解析できない場合に報告されます。
- 「**注文の最終処理リクエストを処理できません。(無効なACMEディレクトリURLの場合)**」は、ACMEクライアントが注文を最終処理できない場合に報告されます。これは多くの場合、無効または到達不能なACMEディレクトリURLが原因です。
- 「**DNSプロバイダー - TestDNSが存在しないか、アクティブではありません。**」は、指定されたDNSプロバイダーが見つからないか、システムで非アクティブである場合に報告されます。
- 「**設定CA IDが空であるか、存在しません。**」は、CA設定IDが不足しているか、既存のどの設定とも一致しない場合に報告されます。

ゼロタッチ証明書管理

NetScaler Consoleでは、ビルド**14.1-43.x**以降を実行している管理対象のNetScalerインスタンスで、ゼロタッチ証明書管理を設定できます。ゼロタッチ証明書管理を使用すると、手動による介入を排除し、アプリケーション要求に対応するためのインメモリゼロタッチ証明書ストアを構築できます。**Infrastructure > SSL Dashboard > Zero-Touch Certificate Management**に移動して、NetScaler Consoleにすべての証明書とキーをアップロードし、管理対象のNetScalerインスタンスで有効にします。NetScalerは定期的に証明書リポジトリをポーリングし、必要に応じて必要な証明書を配信します。

ゼロタッチ証明書管理では、次のプロセスがNetScalerによって自動的に実行されます。

- 証明書の追加、バインド、およびリンク
- 証明書とキーを特定の順序で、またはまとめて提供する
- 要求に基づいて適切な証明書をインストールして使用する
- 定期的なポーリングサイクル中に期限切れの証明書を削除する

NetScalerインスタンスでのゼロタッチ証明書の仕組みの詳細については、「NetScaler zero touch certificate management」を参照してください。

管理者として、NetScaler Consoleで次のことを確認する必要があります。

- NetScalerインスタンスがビルド14.1-43.x以降を実行しており、NetScaler Consoleで管理されていること。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 証明書（任意の形式）とキーをアップロードします。次に、管理対象のNetScalerインスタンスでゼロタッチを有効にします。
- 有効なCA証明書がNetScaler Consoleに存在することを確認します。更新されたConsole CA証明書がある場合は、管理対象のNetScalerインスタンスでゼロタッチを有効にする前に、証明書をアップロードしてください。NetScaler ConsoleにCA証明書がない場合、次のエラーメッセージが表示されます。

証明書のアップロード

1. **インフラストラクチャ > SSLダッシュボード > ゼロタッチ証明書管理** に移動します。
2. 「**Get Started**」をクリックします。

3. ビルド14.1-43.x以降を実行しているNetScalerインスタンスが一覧表示されます。ゼロタッチを有効にするには「**Configure zero-touch**」をクリックするか、次のステップに進むには「**Skip**」をクリックします。
4. すべての証明書をアップロードするには（.pem、.cer、.crtなど、任意の形式で構いません）、「**Upload**」をクリックします。

「

注意事項:

」.

- 証明書またはキーファイルは8192バイト未満である必要があります。
- 複数の証明書またはキーファイルをアップロードする場合、サポートされる最大サイズは50000バイトです。
- 証明書またはキーファイルがパスワードで保護されている場合は、パスワードを指定してください。パスワードが指定されていない場合、証明書またはキーファイルはアップロードされません。

ゼロタッチ証明書管理を有効にする

証明書をアップロードした後、管理対象のNetScalerインスタンスでゼロタッチを有効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**Zero-Touch Certificate Management**」ページから、「**Configure zero-touch**」をクリックします。

2. 「**Add instances**」をクリックし、インスタンスを選択し、その後「**Enable**」をクリックします。

NetScaler Consoleは、デフォルトのポーリング間隔を使用して、NetScalerインスタンスからすべての証明書をポーリングします。「**Poll Now**」オプションを使用して、すぐにポーリングできます。

SSLダッシュボードでは、アクティブおよび非アクティブな証明書の詳細を示すゼロタッチ証明書の使用状況も表示できます。

SSLフィルターモードのサポート

NetScaler®インスタンスは、特定のSSL証明書と秘密キーのメタデータをフェッチします。この最小特権アプローチを実装することで、インスタンスが必要なアセットのみにアクセスできるようになり、1つのインスタンスの侵害によって証明書インフラストラクチャ全体が露出するのを防ぎます。この機能は、複数の管理者が異なる目的でNetScalerインスタンスのグループを管理する環境で特に役立ちます。

利点の一部を以下に示します。

- **セキュリティセグメンテーション** - 攻撃対象領域を最小限に抑え、組織のセキュリティポリシーに準拠するために、NetScalerごとのレベルでメタデータアクセスを制限します。
- **合理化された管理者エクスペリエンス** - 管理者にNetScalerインスタンスのグループに関連するアセットのみを表示することで、マルチテナントまたは部門展開の複雑さを軽減します。
- **最適化されたリソース利用** - 必要なSSL証明書と秘密キーのメタデータのみをフェッチすることで、システムメモリの肥大化を防ぎます。

フィルターモード構成は、特定の同期タイプを通じてNetScalerインスタンスとSSLファイルがどのように相互作用するかを定義します。これらの設定はNetScaler Consoleを通じて管理でき、各インスタンスが必要なメタデータのみをフェッチするようにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンポーネント	同期タイプ	説明
NetScalerインスタンス	カスタム同期	このモードのNetScalerインスタンスは、インスタンスに具体的にマッピングされた証明書とキーのメタデータのみをフェッチします。
NetScaler インスタンス	グローバル同期	このモードのNetScalerインスタンスは、アップロードされたすべての証明書と秘密鍵のメタデータをフェッチします。
SSLファイル	カスタムファイル	これらのファイルは、カスタム同期モードのNetScalerインスタンスに具体的にマッピングされます。
SSLファイル	グローバルファイル	これらのファイルのメタデータは、グローバル同期モードのすべてのNetScalerインスタンスによってフェッチされます。

フィルターモード設定の構成

フィルターモードを構成するには、インスタンスとファイルの同期タイプを定義します。これにより、機密性の高いメタデータの安全かつ最適化された配布が保証されます。

証明書ファイルとNetScalerインスタンスのセクションにあるアップロードボタンを使用して、証明書と秘密鍵を直接アップロードできるようになりました。

GUIを使用して構成するには：

1. **新しいファイルをアップロード（Day Zero）** - 証明書ファイルとNetScalerインスタンス > アップロードに移動して新しいアセットを追加します。次の同期タイプから1つを選択します。

    - **グローバル** - グローバル同期モードを使用し、アップロードを完了するには、これを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **カスタム** - カスタム同期モードを使用し、マッピングする特定のインスタンスを選択し、ファイルをアップロードするには、これを選択します。

2. **既存ファイルの移動 (Day N)** - 証明書とキーをグローバル同期モードからカスタム同期モードに移行するには、ターゲットのNetScalerインスタンスを選択し、「既存ファイルの追加」をクリックします。
3. **ドメインの選択** - インスタンスが選択されたら、移行をトリガーする関連ドメインを選択します。NetScaler Consoleは、対応する証明書と秘密鍵ファイルを自動的に検出し、カスタム同期モードに移行します。
4. **アセットの表示** - ランディングページに移動して、カスタム同期モードで各NetScalerインスタンスにマッピングされているすべての証明書と秘密鍵ファイルを表示します。
5. **同期モードの切り替え** - インスタンスをグローバル同期モードに戻すには、ランディングページで「グローバル同期に切り替え」をクリックします。

SSLダッシュボードを使用する

NetScaler ConsoleのSSL証明書ダッシュボードを使用すると、証明書発行者、キー強度、署名アルゴリズムを追跡するのに役立つグラフを表示できます。SSL証明書ダッシュボードには、以下の情報を示すグラフも表示されます。

- 証明書の有効期限が切れるまでの日数
- 使用済みおよび未使用の証明書の数
- 自己署名証明書とCA署名証明書の数
- 発行者の数
- 署名アルゴリズム
- SSLプロトコル
- 使用中の証明書の数による上位10インスタンス

SSL証明書を監視する

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機関によって承認される必要があるなど、特定のSSL証明書要件を定義している場合は、NetScaler ConsoleのSSLダッシュボードを使用して証明書を監視します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。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が表示されます。

NetScaler ConsoleでSSL証明書を監視するには、「**Infrastructure > SSL Dashboard**」に移動します。

- NetScaler Consoleでは、SSL証明書をポーリングし、インスタンスのすべてのSSL証明書をNetScaler Consoleに即座に追加できます。これを行うには、「**Infrastructure > SSL Dashboard**」に移動し、「**Poll Now**」をクリックします。「**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。

NetScaler Console SSLダッシュボードを使用して、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。これらの数字はハイパーリンクであり、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が表示されます。

- たとえば、上記の図で**自己署名 vs. CA署名**の下にある数字の30をユーザーがクリックすると、新しいウィンドウが表示され、NetScalerインスタンス上の30個のSSL証明書の詳細が表示されます。

- NetScaler Console SSLダッシュボードには、仮想サーバーで実行されているSSLプロトコルの分布も表示されます。管理者として、SSLポリシーを通じて監視したい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、TLS1.0、TLS1.1、TLS1.2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。

-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL証明書の監査ログを表示する

NetScaler Console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、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、NetScaler ConsoleでSSL証明書を使用して実行された操作が表示されます。監査ログ情報は、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 Consoleで実行された特定の操作の監査ログを表示するには、**Infrastructure > SSL Dashboard**に移動し、**Audit Logs**を選択します。

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

NetScaler Consoleでは、設定に基づいて、SSLダッシュボードのチャートに表示されるデフォルトの証明書を表示または非表示にできます。デフォルトでは、すべての証明書（デフォルトの証明書を含む）がSSLダッシュボードに表示されます。

SSLダッシュボードでデフォルトの証明書を表示または非表示にするには：

1. NetScaler Console GUIで**Infrastructure > SSL Dashboard**に移動します。
2. 「**SSLダッシュボード**」ページで、「**設定**」をクリックします。
3. 「**設定**」ページで、「**一般**」を選択します。
4. 「**証明書フィルター**」セクションで、「**デフォルト証明書の表示**」を無効にし、「**保存して終了**」を選択します。

   デフォルト証明書を表示(/en-us/netscaler-console-service/media/default-certificates-clear-ssl-dash.png)

SSL証明書をダウンロードする

SSL証明書はインスタンスごとに個別に管理する必要があります。NetScaler Consoleは、複数のインスタンスに展開されているすべての証明書を可視化します。

- 有効期限が切れる証明書を選択し、証明書の更新を自動化できます。
- 許可される証明書の種類と署名機関に関するポリシーを設定し、適用できます。
- 更新のためにSSL証明書をダウンロードし、後でアップロードすることもできます。

SSL証明書をダウンロードするには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Console GUIで、**インフラストラクチャ > SSLダッシュボード**に移動します。
2. 「**SSLダッシュボード**」ページで、いずれかのグラフにあるSSL証明書の合計数をクリックします。

証明書を選択(/en-us/netscaler-console-service/media/ssl-ceritificates-download-1.png)

1. 「**SSL証明書**」ページで、ダウンロードしたい証明書をクリックします。たとえば、次の1週間で有効期限が切れる証明書をダウンロードしたい場合などです。
2. 「**アクションの選択**」リストボックスから、「**ダウンロード**」を選択します。 証明書がシステムにダウンロードされます。

このダッシュボードのレポートをエクスポートするには：

このページのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページで、次のいずれかを実行できます。

1. **今すぐエクスポート**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。
2. **エクスポートのスケジュール**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。

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。

SSLダッシュボードでSSL証明書を削除するには

NetScaler 14.1-38.x以降では、選択したSSL証明書を削除する際に、関連するSSL証明書ファイルをNetScalerから削除するオプションが提供されます。SSL証明書を削除するには:

1. **インフラストラクチャ > SSLダッシュボード**に移動します。
2. SSL証明書の詳細が表示される**SSL証明書**セクションで、**未使用**ラベルのリンクをクリックします。未使用の証明書の一覧が表示されたページが表示されます。
3. 削除する未使用の証明書を1つ以上選択します。

   SSL監査証跡(/en-us/netscaler-console-service/media/unused-certificates.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **削除**をクリックします。
5. **確認**ダイアログボックスが表示され、NetScaler®から証明書ファイルを削除するための次のオプションが提供されます。

   - **削除しない**: NetScalerからの証明書ファイルの削除をスキップします。
   - **削除**: 期限切れおよび期限切れでない証明書の両方について、NetScalerから証明書ファイルを削除します。
   - **期限切れの場合に削除**: 期限切れの証明書のみ、NetScalerから証明書ファイルを削除します。

   注:

   - NetScalerバージョン14.1-38.xより前のバージョンでは、3つのオプションすべてで証明書ファイルの削除はスキップされます。
   - 設定とともに証明書ファイルを削除するオプションは、NetScaler 14.1-38.x以降にのみ適用されます。

6. 必要に応じて適切なオプションを選択してください。
7. 証明書を削除するには**はい**をクリックするか、変更を加えずにワークフローを終了するには**いいえ**をクリックします。

SSL証明書チェーンの表示

証明書の完全なリンクチェーンを、中間証明書からルートCA証明書まで含めて表示できます。

証明書チェーンを表示するには:

1. **インフラストラクチャ > SSLダッシュボード**に移動し、いずれかのタイルでSSL証明書をクリックします。
2. **SSL証明書**ページで、証明書を選択し、**詳細**をクリックします。証明書チェーンは**リンク**の下に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL証明書の有効期限切れ通知を設定する

セキュリティ管理者として、証明書の有効期限が近づいたときに通知を設定し、どのNetScalerインスタンスがそれらの証明書を使用しているかに関する情報を含めることができます。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。

たとえば、証明書の有効期限が切れる30日前に、メール配信リストにメール通知が送信されるように設定できます。

NetScaler Consoleから通知を設定するには：

1. NetScaler Console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**をクリックします。
4. **Notification Settings**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。メニューから通知の種類と配信リストを選択します。通知の種類は次のとおりです。

   - **Email** – 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、メールがトリガーされます。
   - **Slack** - Slackプロファイルを指定します。証明書の有効期限が近づくと、通知が送信されます。
   - **PagerDuty** - PagerDutyプロファイルを指定します。PagerDutyポータルで設定された通知設定に基づいて、証明書の有効期限が近づくと通知が送信されます。
   - **ServiceNow** - 証明書の有効期限が近づくと、デフォルトのServiceNowプロファイルに通知が送信されます。

   重要

   Citrix Cloud ITSM AdapterがServiceNow用に構成され、NetScaler Consoleと統合されていることを確認してください。詳細については、「NetScaler ConsoleとServiceNowインスタンスを統合する」を参照してください。

6. **保存して終了** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インストール済みの証明書を更新する

証明機関 (CA) から更新された証明書を受け取った後、個々のNetScalerインスタンスにログオンして証明書を更新する必要はありません。NetScaler Consoleで、証明書ストアの証明書を使用して既存の証明書を更新できます。

NetScaler ConsoleからSSL証明書を更新するには：

1. NetScaler Consoleで、**Infrastructure > SSL Dashboard** に移動します。
2. いずれかのグラフをクリックして、SSL証明書のリストを表示します。
3. **SSL 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、**Certificate** を選択して **Certificate Store** ページを表示します。

   SSL証明書を更新する(/en-us/netscaler-console-service/media/update-ssl-certificate.jpg)
5. **Certificate Store** ページで、追加する証明書ファイルを選択します。**Select** をクリックします。

   証明書ストアから更新する(/en-us/netscaler-console-service/media/update-ssl-cert-store.jpg)
6. 新しい証明書のドメイン名が古い証明書と一致せず、サーバーに新しいドメインをホストさせたい場合は、**No Domain Check** を選択します。

   ドメインチェックなしを選択する(/en-us/netscaler-console-service/media/update-ssl-cert-domain-check.jpg)

   OK をクリックします。この証明書がバインドされているすべてのSSL仮想サーバーが自動的に更新されます。

   既存のSSL証明書を証明書ストアの証明書チェーンで更新すると、既存の証明書はリンクされた証明書で更新されます。

   証明書チェーンを更新する(/en-us/netscaler-console-service/media/update-ssl-cert-chain.jpg)

   証明書を選択し、**詳細**をクリックして証明書チェーンを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスにSSL証明書をインストールする

NetScalerインスタンスにSSL証明書をインストールする前に、証明書が信頼できるCAによって発行されていることを確認してください。また、証明書キーの鍵長が2,048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：

NetScaler Console GUIから、選択したNetScalerインスタンスから証明書をインポートし、他のターゲットNetScalerインスタンスに適用することもできます。

1. **Infrastructure > SSL Dashboard**に移動します。
2. SSLダッシュボードの右上隅で、**Install**をクリックします。
3. **NetScalerインスタンスにSSL証明書をインストール**ページで、次のパラメータを指定します。

   a. 証明書ソース

      インスタンスからインポートオプションを選択します。

      - 証明書をインポートする**インスタンス**を選択します。
      - インスタンス上のすべてのSSL証明書ファイルの一覧から**証明書**を選択します。

   b. 証明書の詳細

      - **証明書名**。証明書キーの名前を指定します。
      - **パスワード**。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。

4. 証明書をインストールするNetScalerインスタンスを選択するには、**インスタンスの選択**をクリックします。
5. 「OK」をクリックします。

NetScaler Console から SSL 証明書をインストールするには:

1. **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. ダッシュボードの右上隅にある **証明書のインストール** をクリックします。
3. **NetScaler インスタンスに SSL 証明書をインストール** ページで、次のパラメータを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **証明書ファイル** - **ローカル** (ローカルマシン) または **アプライアンス** (証明書ファイルが NetScaler 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 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、**設定の保存** 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。

証明書署名要求 (CSR) を作成する

証明書署名要求 (CSR) は、証明書が使用されるサーバーで生成される暗号化されたテキストのブロックです。これには、組織名、共通名 (ドメイン名)、地域、国など、証明書に含まれる情報が含まれています。

NetScaler Console を使用して CSR を作成するには:

1. NetScaler Console で、 **>** 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 証明書の一覧を表示し、CSR を作成する証明書を選択して、 ドロップダウンリストから を選択します。
3. ページで、CSR の名前を指定します。
4. 次のいずれかを実行します。

- **キーをアップロードする** - オプションを選択します。キーファイルをアップロードするには、 (ローカルマシン) または (キーファイルは NetScaler Console 仮想インスタンスに存在する必要があります) のいずれかを選択します。
- **キーを作成する** - オプションを選択し、次のパラメータを指定します。

オプション	説明
暗号化アルゴリズム	キーの種類。例: RSA。
キーファイル名	RSA キーが保存されているファイルの名前。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オプション	説明
キーサイズ	ビット単位のキーサイズ。
公開指数値	提供されている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。このアルゴリズムを選択した場合、PEMパスフレーズを指定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。

新しいキーが作成されます。**Infrastructure > SSL Dashboard** に移動し、リストから **View Files on NetScaler Console** を選択し、**SSL Keys** タブを選択してキーを表示します。

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、コモンネーム、組織名、都道府県、国などの詳細が含まれています。

   サブジェクト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を使用すると、単一の証明書で複数のドメインを保護できます。

   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>
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例えば、`10.0.0.1` はIPアドレスで、`www.example.com` はドメイン名です。

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ています。CAは、CSRを提出した電子メールアドレスに有効な証明書を返します。

SSL証明書をリンクおよびリンク解除する

複数の証明書をリンクすることで、証明書バンドルを作成します。ある証明書を別の証明書にリンクするには、最初の証明書の発行者が2番目の証明書のドメインと一致している必要があります。たとえば、証明書Aを証明書Bにリンクする場合、証明書Aの「発行者」は証明書Bの「ドメイン」と一致している必要があります。

NetScaler Consoleを使用して、あるSSL証明書を別の証明書にリンクするには：

1. NetScaler Consoleで、**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. リンクしたい証明書を選択し、**アクションの選択**ドロップダウンリストから**リンク**を選択します。
4. 一致する証明書のリストから、リンクしたい証明書を選択し、**OK**をクリックします。

注

一致する証明書が見つからない場合、次のメッセージが表示されます：リンクする証明書が見つかりません。

NetScaler Consoleを使用してSSL証明書のリンクを解除するには：

1. NetScaler Consoleで、**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. リンクされている証明書のいずれかを選択し、**アクションの選択**ドロップダウンリストから**リンク解除**を選択します。
4. **OK**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **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 Consoleで、エンタープライズポリシーを構成し、すべての信頼できるCA、セキュアな署名アルゴリズムを追加し、証明書キーに推奨されるキー強度を選択できます。NetScalerインスタンスにインストールされている証明書のいずれかがエンタープライズポリシーに追加されていない場合、SSL証明書ダッシュボードには、それらの証明書の発行元が「推奨されません (Not Recommended)」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 (Not Recommended)」と表示されます。

NetScaler Consoleでエンタープライズポリシーを構成するには：

1. NetScaler Consoleで、 **>** の順に移動し、 をクリックします。
2. ページで、 アイコンをクリックして、すべての信頼できるCA、セキュアな署名アルゴリズムを追加し、証明書とキーに推奨されるキー強度を選択します。サポートされているキー強度は、512、1024、2048、3072、および4096ビットです。
   - **推奨されるキー強度** - アルゴリズムのセキュリティとキーのビット数を表します。
   - **推奨される署名アルゴリズム** - アプリケーション用に発行された署名済みトークンを表します。
   - **推奨される信頼できるCA** - デジタル証明書を発行する信頼できるエンティティを表します。**+** アイコンをクリックして、さらにエンティティを追加します。
   - **推奨されるSSLプロトコル** - TLS/SSLバージョンを表します。
3. または 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、 オプションで選択された**署名アルゴリズム**のみが表示され、その他は**推奨されません (Not Recommended)** と表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスからSSL証明書をポーリングする

NetScaler Consoleは、NITROコールとSecure Copy (SCP) プロトコルを使用して、24時間ごとに1回、SSL証明書を自動的にポーリングします。NetScalerインスタンスで新しく追加された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. **Infrastructure > SSL Dashboard** に移動します。
2. **SSL Dashboard** ページの右上隅にある **Poll Now** をクリックします。
3. **Poll Now** ページがポップアップ表示され、ネットワーク内のすべてのNetScalerインスタンスをポーリングするか、選択したインスタンスをポーリングする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。

4. 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。

NetScaler Console証明書ストアを使用してSSL証明書を管理する

NetScaler Console証明書ストアは、SSL証明書を一箇所に保存および管理するのに役立ちます。保存された証明書は、後でNetScalerの設定を構成するために利用できます。

証明書ストアでは、SSL証明書を追加、更新、削除できます。また、証明書ストアを使用して、NetScalerインスタンスから証明書をインポートし、他のターゲットNetScalerインスタンスに適用することもできます。

証明書ストアにSSL証明書を追加する

1. **Infrastructure > SSL Dashboard > Certificate Store**に移動します。**追加**をクリックします。
2. **証明書の追加**ページで、次の詳細を入力します。

    - **証明書キー名** - 証明書の名前を入力します。名前には、ASCII英数字、アンダースコア、ハイフン文字のみを使用し、30文字未満である必要があります。証明書作成後に名前を変更することはできません。
    - **証明書ファイル** - ローカルドライブを参照し、証明書ファイルをアップロードします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **キーファイル** - ローカルコンピューターからキーファイルをアップロードします。
- **パスワード** - PEM形式で暗号化された秘密キーがある場合は、秘密キーの暗号化に使用されたパスフレーズを入力します。
- **証明書チェーンを追加** - 証明書を証明書チェーンに追加するには、このオプションを選択します。
- **証明書チェーン** - ローカルドライブを参照し、証明書ファイルをアップロードします。
- **作成**をクリックします。

証明書ストアでSSL証明書を更新する

1. **Infrastructure > SSL Dashboard > Certificate Store**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。
2. 「**証明書の更新**」ページで、次の詳細を入力します。

   - **証明書キー名** - 更新用に選択した証明書の名前が表示されます。
   - **証明書ファイル** - 証明書ファイルを更新するには、証明書ファイルをアップロードします。
   - **キーファイル** - キーファイルを更新するには、ローカルコンピューターからキーファイルをアップロードします。
   - **パスワード** - PEM形式で暗号化された秘密鍵をお持ちの場合は、秘密鍵の暗号化に使用されたパスフレーズを入力します。
   - **証明書チェーンの追加** - 証明書チェーンに証明書を追加するには、このオプションを選択します。
   - **証明書チェーン** - ローカルドライブを参照して証明書ファイルをアップロードします。
   - **OK**をクリックします。

証明書ストアからSSL証明書を削除する

1. **Infrastructure > SSL Dashboard > Certificate Store**に移動します。**Delete**をクリックします。
2. プロンプトが表示されたら、**Yes**をクリックして証明書を削除します。

NetScaler®インスタンスにSSL証明書をインストールする

1. **Infrastructure > SSL Dashboard > Certificate Store**に移動します。NetScalerインスタンスにインストールする証明書を選択します。
2. 「**NetScalerインスタンスにSSL証明書をインストール**」ページで、次の詳細を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **証明書ソース**

- **証明書** - 選択した証明書の名前を表示します。

b. **証明書の詳細**

- **証明書名** - 証明書の名前を表示します。
- **構成の保存** - NetScaler構成を保存するには、このオプションを選択します。証明書のインストール後にNetScaler構成が保存されます。

3. 「**インスタンスの選択**」をクリックして、証明書をインストールするNetScalerインスタンスを選択します。

「**OK**」をクリックします。

NetScalerインスタンスから証明書をインポートする

1. **Infrastructure > SSL Dashboard > Certificate Store**に移動します。「**NetScaler証明書のインポート**」をクリックします。
2. 「**NetScaler証明書のインポート**」ページで、次のいずれかのタブを選択できます。

   - **NetScaler証明書のインポート** - 「**ポーリングの開始**」をクリックして、すべてのNetScalerインスタンス上のすべてのSSL証明書をポーリングします。
   - **インスタンスの選択** - NetScalerインスタンスを選択し、「**NetScaler証明書のインポート**」をクリックして、選択したNetScalerインスタンスのみのSSL証明書をポーリングします。

   ポーリング後、SSL証明書とキーファイルがダウンロードされ、証明書ストアに追加されます。

   注:

   ストアに同一の証明書名が存在する場合、証明書のインポート操作は失敗します。ただし、インポート操作は残りの証明書のポーリングを続行し、利用可能な場合はNetScaler証明書をストアに追加します。

中間アップロードなしでサーバー証明書を更新する

中間証明書を再アップロードする反復的な作業なしに、証明書を更新できます。この機能強化により、手作業が軽減され、構成エラーのリスクが最小限に抑えられます。

簡単な更新:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleは、デフォルトで更新中に既存の証明書チェーンを保持します。これにより、新しいサーバーレベルの証明書のみをアップロードした場合でも、チェーンが損なわれず有効な状態に保たれます。

主な改善点:

- **複雑さの軽減**: 標準的なサーバー証明書の更新時に、必須の中間証明書のアップロードが不要になります。
- **安全性の確保**: 自動チェーン保持により、SSLハンドシェイクエラーの一般的な原因である「チェーンの破損」が防止されます。

中間証明書をアップロードせずにサーバー証明書を更新するには

1. **インフラストラクチャ > SSLダッシュボード > 証明書ストア** に移動します。
2. 更新する証明書を選択し、**Update** をクリックします。
3. **既存の証明書チェーンを上書き** - 更新で中間チェーンの変更が必要な場合は、このオプションを選択します。
    - **バンドルを使用**: 既存のチェーンを新しくアップロードされたバンドルに置き換えます。
    - **バンドルなし**: 現在の証明書チェーンを完全に削除します。
4. **証明書チェーンを追加** - プライマリサーバー証明書ファイルに中間証明書が含まれていない場合は、このオプションを選択して手動でアップロードし、追加します。

例

最終的な証明書構造は、既存の証明書のチェーンステータスと、更新中に選択するオプションによって異なります。

シナリオ A: 既存の証明書にチェーンがない場合

更新アクション	結果
新しくアップロードされた証明書にチェーンが含まれていない	サーバー証明書が更新されます。中間チェーンは追加されません。
新しくアップロードされた証明書にチェーンが含まれている	サーバー証明書が更新され、新しい中間チェーンがアタッチされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シナリオ B: 既存の証明書にチェーンがある場合

更新アクション	結果
新しくアップロードされた証明書にチェーンが含まれている (既存の証明書チェーンを上書きが有効になっている)	サーバー証明書が更新され、既存の中間チェーンが新しいチェーンに置き換えられます。
新しくアップロードされた証明書にチェーンが含まれていない (既存の証明書チェーンを上書きが有効になっている)	サーバー証明書が更新され、既存の中間チェーンは明示的に削除されます。

構成ジョブ

NetScaler Consoleの構成管理プロセスは、ネットワーク内の複数のNetScalerインスタンスにわたる構成変更、システムアップグレード、およびその他のメンテナンスアクティビティの適切なレプリケーションを保証します。

NetScaler Consoleでは、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 Console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アプライアンスからファイルをコピーできます。たとえば、HAフェイルオーバーやHAアップグレードをスケジュールできます。

NetScaler Consoleでは、次の4つのオプションのいずれかを使用して構成ジョブを作成できます。これらのいずれかを使用して、構成ジョブを実行するためのコマンドと指示の再利用可能なソースを作成します。

1. 構成テンプレート
2. インスタンス
3. ファイル
4. 記録と再生

構成テンプレート

ジョブの作成中に構成テンプレートを作成し、一連の構成コマンドをテンプレートとして保存できます。これらのテンプレートを「ジョブの作成」ページに保存すると、「テンプレートの作成」

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ページに自動的に表示されます。詳細については、「NetScaler Consoleでマスター構成テンプレートを使用する方法」を参照してください。

注

デフォルトの構成テンプレートでは、**名前の変更**オプションは無効になっています。ただし、カスタム構成テンプレートの名前は変更できます。

次のいずれかのテンプレートを使用できます。

構成エディター: 構成エディターを使用してCLIコマンドを入力し、構成をテンプレートとして保存して、ジョブの構成に使用できます。

組み込みテンプレート: 設定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。ジョブは、1つ以上の管理対象インスタンスで実行できる設定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サーバーを設定するジョブをスケジュールできます。ジョブをすぐに実行するか、後で実行するようにスケジュールすることもできます。

詳細については、「設定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」を参照してください。

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 Consoleの組み込みタスクを使用します。また、実行中の設定または保存された設定を抽出し、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。このアップグレードにより、あるインスタンスの設定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設定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、設定コマンドの再利用可能な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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 Consoleにコピーされます。詳細については、「記録と再生を使用して設定ジョブを作成する方法」を参照してください。

このダッシュボードのレポートをエクスポートする

このページのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページでは、次のいずれかを実行できます。

1. 「**今すぐエクスポート**」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するには。
2. 「**エクスポートのスケジュール**」タブを選択します。レポートを毎日、毎週、または毎月スケジュールし、メールまたはSlackメッセージでレポートを送信するには。

注

- 「**毎週**」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いることを確認してください。

関連資料

- 構成ジョブでSCP (put) コマンドを使用する方法
- 構成ジョブで変数を使用する方法
- 修正コマンドから構成ジョブを作成する方法

構成ジョブの作成

ジョブとは、1つまたは複数の管理対象インスタンスで作成および実行できる構成コマンドのセットです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ジョブを作成して、インスタンス間で構成変更を行うことができます。ネットワーク上で複数のインスタンスに構成を複製したり、 NetScaler Console GUIを使用して構成タスクを記録および再生し、それをCLIコマンドに変換したりできます。

NetScaler Consoleの構成ジョブ機能を使用すると、構成ジョブの作成、電子メール通知の送信、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。

NetScaler Consoleで構成ジョブを作成するには：

1. **インフラストラクチャ > 構成 > 構成ジョブ**に移動します。
2. **ジョブの作成**をクリックします。
3. **ジョブの作成**ページで、**構成の選択**タブの下にあるジョブ名を指定し、リストから**インスタンスタイプ**を選択します。
4. **構成ソース**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、保存済みの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、構成エディターに異なるタイプの複数のテンプレートを追加することもできます。
    - **構成ソース**リストから異なるテンプレートを選択し、それらのテンプレートを構成エディターにドラッグします。テンプレートタイプは、**構成テンプレート**、**組み込みテンプレート**、**マスター構成**、**記録と再生**、**インスタンス**、**ファイル**です。

    注

    Deploy Master Configuration Jobテンプレートを初めて追加し、その後異なるタイプ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マスター構成タイプになります。

    構成エディターでコマンドを並べ替えたり、順序を変更したりすることもできます。コマンド行をドラッグアンドドロップすることで、ある行から別の行にコマンドを移動できます。また、テキストボックスのコマンド行番号を変更するだけで、ある行から任意のターゲット行にコマンド行を移動または並べ替えることもできます。構成ジョブの編集中にコマンド行を並べ替えたり、順序を変更したりすることもできます。

    変数を定義して、これらのパラメータに異なる値を割り当てたり、複数のインスタンスでジョブを実行したりできます。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

れた単一のビューで確認できます。「**変数をプレビュー**」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のビューでプレビューできます。

構成エディターのすべてのコマンドに対して、ロールバックコマンドをカスタマイズできます。カスタマイズしたコマンドを指定するには、カスタムロールバックオプションを有効にします。

重要

カスタムロールバックを有効にするには、「**ジョブの作成**」ウィザードを完了します。そして、「**実行**」タブで、「**コマンド失敗時**」リストから「**成功したコマンドをロールバック**」オプションを選択します。

5. 「**インスタンスの選択**」タブで、構成監査を実行するインスタンスを選択します。

   a. NetScalerの高可用性ペアでは、プライマリノードまたはセカンダリノード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。

   b. 「**インスタンスの追加**」をクリックし、リストからインスタンスを選択します。「**OK**」をクリックします。

   c. 「**次へ**」をクリックします。

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 Consoleサーバーにアップロードします。

   b. すべてのインスタンスに対して定義した変数の共通値を入力します。

   c. 「**次へ**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 「**ジョブプレビュー**」タブで、各インスタンスで実行されるコマンドを評価および検証します。このタブには、「**構成の選択**」タブで指定されている場合、ロールバックコマンドも表示されます。
8. 「**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します。

   また、コマンドが失敗した場合にNetScaler Consoleが実行する必要がある、次のいずれかのアクションを「**コマンド失敗時**」リストから選択します。

   - 「**エラーを無視して続行**」: NetScaler Consoleは失敗したコマンドを無視し、選択したインスタンスの残りのコマンドを実行します。

     「

     注

     」

     このアクションでは、進行中の構成ジョブを中止することはできません。

   - 「**それ以上の実行を停止**」: 実行中にいずれかのコマンドが失敗した場合、NetScaler Consoleは残りのコマンドを停止します。
   - 「**成功したコマンドをロールバック**」: 実行中にいずれかのコマンドが失敗した場合、NetScaler Consoleは正常に実行されたコマンドを復元します。

     カスタムロールバックが有効になっている場合、NetScaler Consoleは失敗したコマンドに対して対応するロールバックコマンドを実行します。
9. 「**完了**」をクリックします。

「**ジョブのメールおよびSlack通知を送信するには:**」:

ジョブが実行またはスケジュールされるたびに、メールとSlack通知が送信されるようになりました。通知には、ジョブの成功または失敗などの詳細と、関連する詳細が含まれます。

1. 「**インフラストラクチャ > 構成 > 構成ジョブ**」に移動します。
2. メールおよびSlack通知を有効にするジョブを選択し、「**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。

   - 「**Email**」チェックボックスを選択し、実行レポートを送信するメール配信リストを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メール配信リストを追加する場合は、「**Add**」をクリックし、メールサーバーの詳細を指定します。

- 「**Slack**」チェックボックスを選択し、実行レポートを送信するSlackチャンネルを選択します。

  Slackプロファイルを追加する場合は、「**Add**」をクリックし、必要なSlackチャンネルの「**Profile Name**」、「**Channel Name**」、「**Token**」を指定します。

Slackプロファイルの作成(/en-us/netscaler-console-service/media/configjobemail.png)

4. 「**Finish**」をクリックします。

実行サマリーの詳細を表示するには：

1. **インフラストラクチャ > 構成 > 構成ジョブ** に移動します。
2. 実行サマリーを表示するジョブを選択し、「**Details**」をクリックします。
3. 「**Execution Summary**」をクリックして、以下を表示します。

   - 実行されたジョブ上の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

実行サマリーの表示(/en-us/netscaler-console-service/media/instanceuser.png)

記録と再生を使用して構成ジョブを作成する

NetScaler GUI を使用して NetScaler インスタンスを構成することに慣れている場合、構成タスクを作成し、複数の NetScaler インスタンスで実行するための正確な CLI コマンドを思い出すのが難しい場合があります。

NetScaler Console を使用すると、NetScaler インスタンスの GUI を使用して実行された構成タスクを記録し、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 > 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

   構成ジョブを記録する(/en-us/netscaler-console-service/media/createjob_record1.png)

4. **NetScaler GUI** が開きます。構成タスクに含める機能と設定を構成します。その後、NetScaler GUI ウィンドウを閉じ、**Configuration Editor** で **Stop** をクリックします。コマンドは左ペインにリンクとして表示されます。コマンドを右ペインにドラッグし、**Next** をクリックします。

   その後、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再配置することもできます。

5. 構成ジョブの作成中または編集中に定義したすべての変数を、統合された単一のビューで確認できます。

6. すべての変数を統合された単一のビューで表示するには、次のいずれかを実行します。

   - 構成ジョブの作成中に、**Infrastructure > Configuration Jobs** に移動し、**Create Job** を選択します。**Create Job** ページで、構成ジョブの作成中に追加したすべての変数を確認できます。
   - 構成ジョブの編集中に、**Infrastructure > Configuration > 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。

7. その後、**Preview Variables** タブをクリックして、構成ジョブの作成中または編集中に定義した変数を、統合された単一のビューでプレビューできます。

8. 新しいポップアップウィンドウが表示され、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。

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。

10. コマンドで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.

- **変数値の入力ファイルをアップロード**: **入力キーファイルのダウンロード**をクリックして入力ファイルをダウンロードします。入力ファイルに、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。
- **すべてのインスタンスに共通の変数値**: 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構成ジョブを表示するには、**ネットワーク** > **構成ジョブ**に移動し、**ジョブの作成**をクリックします。**ジョブの作成**ページで、**変数値を指定**タブで、アップロードされたファイルを表示するために**すべてのインスタンスに共通の変数値**オプションを選択します。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、**変数値を指定**タブで、アップロードされたファイルを表示するために**すべてのインスタンスに共通の変数値**オプションを選択します。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**タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。

11. **ジョブプレビュー**タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
12. **実行**タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合にNetScaler Consoleが実行すべき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することを許可するかどうか、および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を選択できます。

13. **ジョブ**ページでは、すべてのインスタンスでの構成タスク実行の進捗状況を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ジョブを使用して、1つのインスタンスから複数のインスタンスへ構成を複製する

展開のために、NetScalerインスタンスで負荷分散とAppFlowの両方を構成している場合があります。しかし、今度はAppFlow構成のみを他のNetScalerインスタンスに複製したいと考えています。

NetScaler Consoleの構成ジョブ機能を使用して、NetScalerインスタンスからAppFlow構成を抽出し、複数のインスタンスに複製できます。

1つのインスタンスから他のNetScalerインスタンスへ構成を取得して複製するには：

1. **Infrastructure > Configuration > 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**として**Instance**を選択し、構成を複製したいソースインスタンスを選択します。抽出したい構成の種類を選択します。「Configuration by time duration」を選択した場合は、この構成を実行した期間を設定し、**Extract**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、下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。

   ジョブを指定する(/en-us/netscaler-console-service/media/replicatejob1.png)
4. コマンドを右ペインの**Commands**フィールドにドラッグします。

   ジョブにコマンドを追加する(/en-us/netscaler-console-service/media/replicatejob2.png)

   FEOに関連するコマンドのみを残し、負荷分散に関連するコマンド、またはその他の構成に関連するコマンドを手動で削除してから、**Next**をクリックします。
5. **Add Instances**をクリックし、FEO構成を適用したいインスタンスを追加します。**OK**をクリックし、次に**Next**をクリックします。

   コマンドに変数を指定している場合は、「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、NetScaler Consoleにファイルをアップロードします。

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。

「**Execute**」タブで、「**Finish**」をクリックして、選択したNetScalerインスタンスでジョブを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ジョブで変数を使用する

構成ジョブとは、1つ以上の管理対象インスタンスで実行できる一連の構成コマンドです。複数のインスタンスで同じ構成を実行する場合、構成で使用されるパラメーターに異なる値を使用したい場合があります。これらのパラメーターに異なる値を割り当てたり、複数のインスタンスでジョブを実行したりできる変数を定義できます。

たとえば、ロードバランシング仮想サーバーを追加し、2つのサービスを追加し、そのサービスを仮想サーバーにバインドする基本的なロードバランシング構成を考えてみましょう。ここで、2つのインスタンスで同じ構成を持ちたいが、仮想サーバーとサービスの名前およびIPアドレスには異なる値を使用したいとします。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 Consoleで変数を定義して構成ジョブを作成するには:

1. **インフラストラクチャ > 設定 > 設定ジョブ** に移動します。
2. **Create Job** をクリックします。
3. **Create Job** ページで、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、**Convert to Variable** をクリックします。

5. 変数の値がドル記号で囲まれていることを確認したら、その変数をクリックして、名前、表示名、タイプなどの変数の詳細をさらに指定します。変数のデフォルト値をさらに指定したい場合は、**Advanced** オプションをクリックすることもできます。**Save** をクリックし、次に **Next** をクリックします。
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 > 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** タブをクリックすると、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。

   変数の詳細を確認(/en-us/netscaler-console-service/media/record-and-play-preview-1.png)
10. その後、設定エディターでコマンドを適切に並べ替えたり、順序を変更したりできます。コマンド行をドラッグアンドドロップすることで、コマンドをある行から別の行に移動できます。また、テキストボックス内のコマンド行番号を変更するだけで、コマンド行をある行から任意のターゲット行に移動または再配置することもできます。
11. 設定ジョブを実行するインスタンスを選択します。
12. **変数値の指定**タブで、**変数値の入力ファイルをアップロード**オプションを選択し、**入力キーファイルをダウンロード**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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を指定して編集し、**アップロード**をクリックして入力キーファイルをNetScaler Consoleにアップロードできます。**次へ**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を指定して編集できます。

    注

    入力キーファイルでは、変数は次の3つのレベルで定義されます。

    - グローバルレベル
    - インスタンスグループレベル
    - インスタンスレベル

    グローバル変数は、すべてのインスタンスに適用される変数値です。インスタンスグループレベルの変数値は、グループで定義されているすべてのインスタンスに適用されます。インスタンスレベルの変数値は、特定のインスタンスにのみ適用されます。

    NetScaler Consoleは、インスタンスレベルの値を最優先します。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 Consoleはグループレベルで提供された値を使用します。グループレベルで値が提供されていない場合、NetScaler Consoleはグローバルレベルで提供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 Consoleはインスタンスレベルの値をデフォルト値として使用します。

14. **アップロード**をクリックして、入力キーファイルをNetScaler Consoleにアップロードします。**次へ**をクリックします。

    入力キーをアップロード(/en-us/netscaler-console-service/media/basic-lb-configuration-excel.jpg)

    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、テキストエディタを使用して必要な変更を加え、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で共通の変数値を指定することもでき、**Upload**をクリックして入力キーファイルをNetScaler Consoleにアップロードできます。

© 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された構成ジョブを表示するには、**Network** > **Configuration Jobs**に移動し、**Create Job**をクリックします。**Create Job**ページで、**Specify Variable Values**タブの**Common Variable Values for all Instances**オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してアップロードします（同じファイル名を維持します）。

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、**Network** > **Configuration Jobs**に移動し、ジョブ名を選択して**Edit**をクリックします。**Configure Job**ページで、**Specify Variable Values**タブの**Common Variable Values for all Instances**オプションを選択して、アップロードされたファイルを表示します。入力ファイルを編集するには、入力ファイルをダウンロードし、編集してアップロードします（同じファイル名を維持します）。

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. **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するかを選択できます。コマンドが失敗した場合にNetScaler Consoleが取るべきアクション、およびジョブの成功または失敗に関するメール通知を他の詳細とともに送信するかどうかも選択できます。

ジョブを設定して実行した後、**Infrastructure > Configuration > Configuration Jobs**に移動し、設定したジョブを選択することで、ジョブの詳細を確認できます。**Details**をクリックし、次に**Variable Details**をクリックして、ジョブに追加された変数の一覧を表示します。

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とき、または後で実行するようにジョブをスケジュールしたときに、NetScaler Consoleによって保持されます。

修正コマンドから構成ジョブを作成する

NetScaler Consoleの監査テンプレート機能を使用して、管理対象のNetScalerインスタンス全体の構成変更を監視し、構成エラーをトラブルシューティングできます。

監査テンプレートを使用し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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. インスタンス構成を監査するために、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の差異を確認するために、監査テンプレートを実行するNetScalerインスタンスを選択します。
3. 差分/修正コマンドを理解し、「ジョブの作成」機能を利用して、インスタンスの構成を目的の状態にします。

複数の管理者が5つのNetScalerインスタンスを管理しているシナリオを考えてみましょう。これらの管理者はすべて、必要な変更があるたびに既存のインスタンス構成を更新します。スーパー管理者は、他の管理者によって行われる変更に関係なく、特定の重要な構成セットが変更されないままであることを確認したいと考えています。このユースケースでは、スーパー管理者はNetScalerインスタンスに存在すると予想される構成のテンプレートを作成し、それをインスタンスに対して実行します。NetScaler Consoleは、監査テンプレート構成と実行中の構成を比較し、不一致を**構成監査**ダッシュボードに報告します。

一部のインスタンスの構成に変更があることに気づいた場合、NetScaler Consoleの修正コマンド機能を使用して、特定のNetScalerインスタンス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 Consoleで修正コマンドから構成ジョブを作成するには：

1. **インフラストラクチャ > 構成 > 構成監査**に移動します。
2. **構成監査**ページで、2つのドーナツチャートのいずれかをクリックして、**監査レポート**ページにアクセスします。
3. 構成コマンドを修正したいインスタンスの**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、および修正構成間の差異が一覧表示されます。

   構成差分を表示(/en-us/netscaler-console-service/media/auditreports.png)
4. **ジョブの作成**をクリックして**ジョブの作成**ページに移動します。このページには修正コマンドが事前に入力されています。構成ジョブの作成方法については、「NetScaler Consoleで構成ジョブを作成する方法」を参照してください。

   構成ジョブを作成する(/en-us/netscaler-console-service/media/correctivecommands2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1つの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

NetScalerインスタンスの構成を他のインスタンスに複製できるようになりました。NetScaler Consoleでジョブを構成する際、インスタンスを構成ソースとして選択し、選択したインスタンスの実行中または保存済みの構成を選択します。

たとえば、**実行中の構成**を選択して**抽出**をクリックすると、NetScaler Consoleは選択したNetScalerインスタンスに実行中の構成を検索するリクエストを送信し、それをテンプレートとして表示します。テンプレートを右側のペインの**コマンド**フィールドにドラッグできます。コマンド、パラメータ、およびインスタンスを変更できます。

NetScaler Consoleで、あるインスタンスの実行中および保存済みの構成コマンドを別のインスタンスに複製するには：

1. **インフラストラクチャ > 構成 > 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、その構成を他のインスタンスに複製したいソースインスタンスを選択します。
4. 次の3つのオプションが表示されます。
   - 実行中の構成
   - 保存済みの構成
   - 期間による構成
5. **実行中の構成**を選択し、**抽出**をクリックします。そのインスタンスで実行された実行中の構成コマンドの数が表示されます。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. コマンドに変数を指定している場合は、「**変数値を指定**」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 Consoleにアップロードします。
10. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
11. 「**実行**」タブでは、ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。コマンドが失敗した場合にNetScaler Consoleが実行すべきアクション、およびジョブの成功または失敗に関するメール通知をその他の詳細とともに送信するかどうかも選択できます。

実行済み構成ジョブを再利用する

構成ジョブを使用すると、1つ以上の管理対象インスタンスで実行できる一連の構成コマンドを作成できます。また、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、同じ一連の保存済み構成ジョブを実行することもできます。この機能は、同じ一連のコマンドを別のインスタンスで実行する必要がある場合や、ジョブがエラーに遭遇してそれ以上の実行を停止する場合に役立ちます。

NetScaler Consoleは、完了したジョブを再度実行する機能を提供します。この機能を使用すると、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。

完了したジョブを編集するには:

1. NetScaler Consoleのホームページから、**インフラストラクチャ > 構成 > 構成ジョブ**の順に移動します。
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。

   完了したジョブを実行する

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

ジョブを選択し、**再度実行**をクリックして、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。このオプションは、同じインスタンスで同じ一連のコマンドを実行する必要がある場合に役立ちます。サーバー側で一時的なエラーが発生し、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SCP (put) コマンドを使用する

NetScaler Consoleの**構成ジョブ**機能を使用して、構成ジョブを作成し、メール通知を送信し、作成されたジョブの実行ログを確認できます。ジョブとは、単一の管理対象インスタンスまたは複数の管理対象インスタンスで作成および実行できる一連の構成コマンドです。たとえば、デバイスのアップグレードに構成ジョブを使用できます。

NetScaler Consoleの構成ジョブは、インスタンスを構成するためにSecure Shell (SSH) コマンドを使用し、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。構成ジョブで「put」コマンドを使用して、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 Consoleにアップロードまたは転送し、その後NetScalerインスタンス上のディレクトリに転送できます。

注

ファイルはNetScaler Console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 Console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であり、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ジョブの作成中に、ローカルおよびリモートファイル名のパラメーター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ー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. NetScaler Consoleで、**インフラストラクチャ > 設定 > 設定ジョブ**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**ペインで「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。
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、 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す）を確認し、変数をクリックします。
6. 名前、表示名、タイプなど、変数の詳細を指定します。
7. ドロップダウンリストから を選択します。 をクリックします。

   変数を「ファイル」タイプとして宣言すると、NetScaler Consoleにファイルをアップロードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 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. タブで、 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、 をクリックしてNetScaler Consoleにファイルをアップロードし、 をクリックします。

10. タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
11. 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できます。コマンドが失敗した場合にNetScaler Consoleが実行するアクションを選択することもできます。また、ジョブの成功または失敗に関する通知やその他の詳細を受け取るためのメール通知を作成することもできます。 をクリックします。
12. 「**Infrastructure > Configuration > Configuration Jobs**」に移動し、設定したジョブを選択することで、ジョブの詳細を確認できます。「**Details**」をクリックし、次に「**Variable Details**」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。

構成テンプレートを使用する

構成テンプレートは、NetScaler Consoleに保存し、構成ジョブまたは構成監査の作成時に適用できる、再利用可能な構成コマンドのセットです。テンプレートを使用すると、構成を標準化し、反復作業を減らし、複数の管理対象NetScalerインスタンスにわたって一貫した設定を展開できます。

ジョブの作成時に、一連の構成コマンドをテンプレートとして保存することで、構成テンプレートを作成できます。また、組み込みテンプレート、マスター構成テンプレート、監査テンプレートを使用し、それらを構成ジョブモジュールと構成監査モジュール間で共有することもできます。

以下のトピックでは、NetScaler Consoleで構成テンプレートを操作する方法について説明します。

- マスター構成テンプレートを使用する(/ja-jp/netscaler-console-service/networks/configuration-jobs/use-master-configuration-template.html)
- 組み込みテンプレートを使用して作成されたジョブをスケジュールする(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-schedule-jobs-created-using-built-in-templates.html)
- NetScalerからPrometheusへのメトリックのエクスポートを構成するジョブをスケジュールする(/ja-jp/netscaler-console-service/networks/configuration-jobs/built-in-template-prometheus-export.html)

© 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(/ja-jp/netscaler-console-service/networks/configuration-jobs/use-configuration-templates-to-create-audit-templates.html)
- 組み込みテンプレートを使用して構成されたジョブを再スケジュールする(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-reschedule-jobs.html)
- 構成ジョブで構成監査テンプレートを再利用する(/ja-jp/netscaler-console-service/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(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-import-and-export-configuration-templates.html)

マスター構成テンプレートを使用する

マスター構成テンプレートを使用すると、複数のNetScalerインスタンスで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、構成の変更を行い、ライセンス、証明書、その他のファイルをNetScalerインスタンスに保存したい場合があります。新しい構成をマスター構成テンプレート（.confファイル）として保存できます。

NetScalerインスタンスからマスター構成テンプレートを保存するには、次のいずれかの操作を実行します。

- コマンドプロンプトで、「**save ns config**」と入力します。構成は、インスタンスのFLASHメモリ内の/nsconfig/ns.confファイルに保存されます。
- NetScalerインスタンスのGUIから、**Diagnostics** > **View Configuration** に移動します。保存する構成の種類を選択します。たとえば、NetScalerインスタンスの保存済み構成を保存する場合は、**Saved configuration** を選択します。「**Save text to a file**」リンクをクリックして、「ns.conf」ファイルをローカルマシンに保存します。

ジョブの作成時に「DeployMasterConfiguration」構成テンプレートを使用してマスター構成テンプレートを展開する場合、コマンドを追加したり、既存のコマンドを変更したり、入力ファイルに異なる変数値を指定したりすることで、特定のNetScalerインスタンスごとにさらにカスタマイズできます。

たとえば、管理者として、ns.confファイルに加えて証明書キーをNetScalerインスタンスにアップロードし、それらにもマスター構成を展開したい場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要

DeployMasterConfigurationテンプレートを使用して、NetScaler CPXインスタンス、クラスターで構成されたNetScalerインスタンス、またはパーティション化されたNetScalerインスタンスで構成ジョブを実行することはできません。

NetScaler Consoleでマスター構成テンプレートを使用して構成ジョブを作成するには：

1. NetScaler Consoleで、**Infrastructure > Configuration > 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** タブで、**Job Name** を指定し、ドロップダウンリストから **Instance Type** を選択します。
3. **Configuration Source** ドロップダウンリストから **Master Configuration** を選択します。DeployMasterConfigurationテンプレートのコマンドを右ペインにドラッグします。右ペインでコマンドを追加、変更、または削除することもできます。**Next** をクリックします。

   注

   テンプレートに入力ファイルを追加するには、**put**コマンドを追加できます。この例では、設定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. 構成ジョブの作成または編集時に定義したすべての変数を、統合された単一ビューで確認できます。
5. すべての変数を統合された単一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、**Infrastructure > Configuration > 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. 次に、**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ビューでプレビューできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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ら、**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。

   - **構成テンプレートファイル (.conf)** - NetScalerインスタンスから抽出した.confファイルをアップロードします。
   - **入力ファイル (.xml/csv) をアップロード** - コマンドで定義した変数の値を含む入力ファイルをアップロードします。

   使用のためにサンプルXMLファイルがここに提供されています。XMLファイルに、使用しているNetScalerインスタンスに対応する詳細が含まれていることを確認してください。

```
<?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.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence over the
instance group. The instance group specific parameters value will take
precedence over global parameters in the execution.



-  name. This attribute represents the name of the instance group.



-  device. This tag contains all the instance specific parameters and
value.



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>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<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>
```

使用のためにサンプルCSVファイルがここに提供されています。

```
#job-s_variable_input_key_file ,,,,
,,,,
#Global,NSIP,HostName,LBSERVER,SNMPTrapDest
Global Values,,,,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
#InstanceGroup,NSIP,HostName,LBSERVER,SNMPTrapDest

example_doc,,,,

#Instance(s),NSIP,HostName,LBSERVER,SNMPTrapDest

10.xx.xx.xx,,,,
```

同じファイルがMicrosoft Excelに表示されます。

Excel上のCSVの例(/en-us/netscaler-console-service/media/example-csv-template.png)

10. **次へ**をクリックします。

    ファイルを選択(/en-us/netscaler-console-service/media/master-config-create-newpng.png)

    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、**変数値の指定**タブで、アップロードされたファイルを表示するために**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、**ネットワーク** > **構成ジョブ**に移動し、ジョブ名を選択して**編集**をクリックします。**ジョブの構成**ページで、**変数値の指定**タブで、アップロードされたファイルを表示するために**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）。

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し、**次へ**をクリックできます。

    コマンドを検証(/en-us/netscaler-console-service/media/dmc4.png)

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 Consoleが取るべきアクションも選択できます。

    承認されたユーザーが管理対象インスタンスでジョブを実行することを許可することも選択でき、ジョブの成功または失敗に関するメール通知を、その他の詳細とともに送信するかどうかも選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

承認されたユーザーを許可(/en-us/netscaler-console-service/media/dmc5.png)

ジョブを実行した後、**インフラストラクチャ > 構成 > 構成ジョブ**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**実行概要**をクリックしてジョブの詳細を確認します。インスタンスをクリックして**コマンドログ**を表示し、ジョブで実行されたコマンドを確認します。

ジョブで実行されたコマンドを表示(/en-us/netscaler-console-service/media/dmc6.png)

組み込みテンプレートを使用して作成されたジョブをスケジュールする

組み込みテンプレートオプションを使用してジョブをスケジュールできます。ジョブとは、1つ以上の管理対象インスタンスで実行できる構成コマンドのセットです。たとえば、組み込みテンプレートオプションを使用して、Syslogサーバーを構成するジョブをスケジュールできます。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かを選択することもできます。

NetScaler Consoleで組み込みテンプレートを使用してジョブをスケジュールするには：

1. NetScaler Consoleで、**インフラストラクチャ > 構成 > 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** ページの **構成の選択** タブで、**ジョブ名** を指定し、ドロップダウンリストから **インスタンスタイプ** を選択します。
3. **構成ソース** ドロップダウンリストから **組み込みテンプレート** を選択します。*NSConfigureSyslogServer* コマンドを右ペインにドラッグし、**次へ** をクリックします。

   組み込みテンプレートを使用する(/en-us/netscaler-console-service/media/createjobinbuilttemp1.png)
4. **インスタンスの選択** タブで、**インスタンスの追加** をクリックし、ジョブを実行するインスタンスを選択して、**OK** をクリックします。
5. **次へ** をクリックします。**変数値の指定** タブで、インスタンスの変数を指定するために、次のいずれかのオプションを選択します。

   - **入力ファイルからの変数値** - 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。
   - **すべてのインスタンスの共通変数値** – SyslogサーバーのIPアドレスとポートを指定します。
6. **ジョブプレビュー** タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
7. **次へ** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. **実行** タブで、次の条件を設定します。

   - **コマンドの失敗時** - コマンドが失敗した場合、エラーを無視してジョブの実行を続行するか、ジョブのそれ以上の実行を停止するかを選択できます。ドロップダウンリストから実行するアクションを選択します。
   - 「**実行モード**」 - ジョブを今すぐ実行するか、後で実行するようにスケジュールできます。ジョブを後でスケジュールする場合は、そのジョブの実行頻度設定を指定する必要があります。ドロップダウンリストから、ジョブに適用するスケジュールを選択します。

9. 「**実行設定**」で必要な方法を選択することにより、一連のインスタンスでジョブを順次または並行して実行することもできます。いずれかのインスタンスでジョブの実行が失敗した場合、残りのインスタンスでは続行されません。

   承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることも選択できます。また、ジョブの成功または失敗に関するメール通知を、その他の詳細とともに送信するかどうかを選択できます。

10. 「**完了**」をクリックします。

NetScalerからPrometheusへのメトリクスエクスポートを設定するジョブをスケジュールする

`NSConfigurePrometheusAnalyticsProfile`テンプレートを使用して、デフォルトスキーマまたは変更されたパラメーターを持つカスタムスキーマのいずれかを使用し、すべての管理対象インスタンスでジョブを実行できます。

前提条件

管理対象のNetScalerが**13.1 build 39-27以降**であることを確認してください。

ジョブをスケジュールするには：

1. NetScaler Consoleで、**Infrastructure > Configuration > Configuration Jobs**に移動し、**Create Job**をクリックします。
2. **Create Job**ページで、ジョブの名前を指定し、**Instance Type**リストから**NetScaler®**を選択します。
3. **Configuration Source**リストから**Inbuilt Template**を選択します。*NSConfigurePrometheusAnalyticsProfile*コマンドを右ペインにドラッグし、**Next**をクリックします。**+**をクリックしてテンプレートを追加することもできます。

   Prometheusテンプレートの画像(/en-us/netscaler-console-service/media/inbuilt-template-prometheus.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. デフォルトスキーマで続行する場合は：

   a. ステップ3 (`put $Schema_file /var/metrics.conf/$schema_filename$`) を削除します。マウスカーソルをステップ3に置き、次のようにします：

      - Windowsでは、Control + Aを押してからDeleteを押します。
      - Macでは、Command + Aを押してからDeleteを押します。

   b. 削除後、**Next**をクリックします。

   c. **Select Instances**タブで、**Add Instances**をクリックし、ジョブを実行したいインスタンスを選択して、**Next**をクリックします。

   d. 「**変数値の指定**」タブで、「**すべてのインスタンスに共通の変数値**」を選択します。

      - **Analytics TimeSeries プロファイル名** - アナリティクスプロファイル名を指定します。詳細については、`https://docs.netscaler.com/ja-jp/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`を参照してください。
      - **NetScaler にアップロードするスキーマファイル名** - このファイル名をデフォルトファイルである`schema.json`として保持します。

        ▢

   e. ステップ6から先に進みます。

5. カスタムスキーマカウンターで続行する場合は、次の手順を実行します。

   a. 「**構成ソース**」リストから「**組み込みテンプレート**」を選択します。`NSConfigurePrometheusAnalyticsProfile`コマンドを右ペインにドラッグし、「**次へ**」をクリックします。「+」をクリックしてテンプレートを追加することもできます。

   b. 「**インスタンスの選択**」タブで、「**インスタンスの追加**」をクリックし、ジョブを実行するインスタンスを選択して、「**次へ**」をクリックします。

   c. 「**変数値の指定**」タブで、「**すべてのインスタンスに共通の変数値**」を選択します。

      - **NetScaler カウンタースキーマファイル (.json)** - パラメータで変更したスキーマファイルを選択します。NetScaler では、サポートされているすべてのカウンターを含む参照ファイル`reference_schema.json`がパス`/var/metrics_conf/`の下にあります。

        ▢

        FTPクライアントを使用してファイルをローカルにコピーし、必要なパラメータを編集して保存し、アップロードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScaler にアップロードするスキーマファイル名** - NetScaler にアップロードするスキーマファイル名を指定します。
- **Analytics TimeSeries プロファイル名** - アナリティクスプロファイル名を指定します。詳細については、`https://docs.netscaler.com/ja-jp/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector` を参照してください。

6. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。
7. 「**次へ**」をクリックします。
8. 「**実行**」タブで、次の条件を設定します。

   - 「**コマンド失敗時**」 - コマンドが失敗した場合、エラーを無視してジョブの実行を続行するか、ジョブのそれ以上の実行を停止するかを選択できます。ドロップダウンリストから実行するアクションを選択します。
   - 「**実行モード**」 - ジョブを今すぐ実行するか、後で実行するようにスケジュールするかを選択できます。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により、インスタンスのセットでジョブを順次または並行して実行することもできます。いずれかのインスタンスでジョブの実行が失敗した場合、残りのインスタンスでは続行されません。

   承認されたユーザーが管理対象インスタンスでジョブを実行できるようにすることも選択でき、ジョブの成功または失敗に関する通知を、その他の詳細とともに送信するかどうかを選択できます。

10. 「**完了**」をクリックします。

    組み込みテンプレートを使用したジョブのスケジュール(/en-us/netscaler-console-service/media/dmc5.png)

構成テンプレートを使用して監査テンプレートを作成する

以前に構成テンプレートとして保存された構成コマンドを使用して、特定のNetScalerインスタンスに適用できる監査テンプレートを作成できるようになりました。監査テンプレートの作成中に、以前に保存した構成テンプレートを**コマンド**フィールドにドラッグし、要件に合わせてテンプレートを編集できます。その後、監査テンプレートを特定のNetScalerインスタンスに適用でき

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ます。NetScaler Consoleはこれらのインスタンスを監査テンプレートと比較し、不一致を報告します。このプロセスは、エラーを特定し、タイムリーに修正するのに役立ちます。

ジョブの作成中に構成テンプレートを作成し、一連の構成コマンドをテンプレートとして保存できます。これらのテンプレートを**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、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、それら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**
```

NetScaler Console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 > 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、前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。

   テンプレートを保存(/en-us/netscaler-console-service/media/audittemplates1.png)

NetScaler Consoleで構成テンプレートを使用して監査テンプレートを作成するには：

1. **インフラストラクチャ > 構成 > 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。
2. **テンプレートの作成**ページで、テンプレートの名前を指定し、説明を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **構成ソース**リストから**構成テンプレート**を選択し、テンプレートを右ペインのコマンドフィールドにドラッグします。構成を編集して、別の名前でテンプレートを保存することもできます。**次へ**をクリックします。
4. **インスタンスの選択**タブで、**インスタンスの追加**をクリックし、構成を実行するインスタンスを追加します。**OK**をクリックします。
5. **完了**をクリックします。

   監査テンプレートを作成(/en-us/netscaler-console-service/media/auditttemplates2.png)

   監査テンプレートは監査テンプレートリストに表示され、指定されたインスタンスの構成に対して12時間ごとに実行されます。

組み込みテンプレートを使用して構成されたジョブを再スケジュールする

NetScaler Console の組み込みテンプレートを使用してスケジュールしたジョブを再スケジュールできます。たとえば、コマンドが失敗した場合に NetScaler Console が実行する必要があるアクションを変更できます。以前にエラーを無視して続行することを選択していた場合、コマンドが失敗した場合にすべての成功したコマンドをロールバックするように変更できます。

NetScaler Console の組み込みテンプレートを使用して構成されたジョブを再スケジュールするには：

1. NetScaler Console で、 **> >** の順に移動します。
2. 編集するジョブを選択し、インスタンスを追加または削除し、変数値を指定してから、実行アクションと設定を変更します。
3. をクリックしてジョブを再スケジュールします。

> **注**
>
> ジョブを選択してもう一度 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、ジョブを作成するとき、および構成監査を実行するときに、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**モジュール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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

監査テンプレートは、構成ジョブとしてテンプレートを実行できるように、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**モジュールの両方で表示されるようになりました。

以前は、同じ構成に対して構成ジョブテンプレートと構成監査テンプレートを個別に作成し、異なるファイルとして保存する必要がありました。これにより、テンプレートの作成と保守に労力の重複が生じていました。

NetScaler Consoleでは、このテンプレートをシステムに保存できるため、監査テンプレートが**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検討してください。その構成では、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、それら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それを再利用するには、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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**インフラストラクチャ > 構成 > 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。
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、前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。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。

   設定テンプレートを保存(/en-us/netscaler-console-service/media/nmas-configaudit-template-reuse--1.png)

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。

   インスタンスの選択(/en-us/netscaler-console-service/media/nmas-configaudit-template-reuse-2.png)

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 > 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は、構成テンプレートとしてリストされます。

構成ジョブで監査テンプレートを再利用するには:

1. ジョブの名前を入力し、インスタンスタイプを選択して、テンプレートをコマンドペインにドラッグします。

   構成ジョブの作成中に、ローカルおよびリモートのファイル名パラメータを変数に変換できます。これにより、ジョブを実行するたびに、同じNetScalerインスタンスのセットに対してこれらのパラメータに異なるファイルを割り当てることができます。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「**インスタンスの選択**」タブで、これらのコマンドを実行するインスタンスを選択します。
4. コマンドに変数を指定している場合は、「**変数値を指定**」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。

   - 入力ファイルからの変数値 - 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。
   - すべてのインスタンスの共通変数値 – syslogサーバーのIPアドレスとポートを指定します。

5. 「**ジョブプレビュー**」タブで、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証し、「**次へ**」をクリックします。
6. 「**実行**」タブで、「**完了**」をクリックして構成ジョブを実行します。

   この負荷分散サーバーに別のサービスを追加し、そのサービスをサーバーにバインドしたい場合は、コマンドページでコマンドを編集して保存できます。
7. 「**監査テンプレート**」に移動し、「**追加**」をクリックします。
8. 「LBVariablesTemplate」テンプレートをコマンドペインにドラッグします。テンプレートが新しいコマンドで更新されていることがわかります。

   監査テンプレートは監査テンプレートリストに表示され、指定されたインスタンスの構成に対して12時間ごとに実行されます。これで、テンプレートを作成し、構成ジョブと構成監査モジュール間で再利用できます。

構成テンプレートのインポートとエクスポート

任意のNetScaler Consoleアプライアンスから構成テンプレートをエクスポートし、将来いつでも同じまたは別のNetScaler Consoleアプライアンスにファイルをインポートできます。構成テンプレートデータ（構成コマンド、変数定義、パラメータなど）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、ローカルフォルダに保存できます。同じまたは別のNetScaler Consoleアプライアンスからエクスポートした、または手動で作成した構成テンプレートの **.json** ファイルをNetScaler Consoleアプライアンスにインポートできます。

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 > 設定 > 構成テンプレート** に移動します。
2. **Add** をクリックして構成テンプレートを作成します。

   構成テンプレートをエクスポートする (/en-us/netscaler-console-service/media/import-export.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Create Configuration Template** ページで、構成テンプレート名を指定し、インスタンスタイプを選択します。**Configuration Editor** で、ドロップダウンメニューから構成ソースとして Configuration Template を選択します。既存の構成テンプレートを構成エディタにドラッグできます。**OK** をクリックします。

   構成テンプレートを選択する (/en-us/netscaler-console-service/media/import-export-1.png)

4. **Infrastructure > Configuration > Configuration Templates** に移動して、構成テンプレートのリストに作成されたテンプレートを表示します。

   作成されたテンプレートを表示する (/en-us/netscaler-console-service/media/import-export-2.png)

5. 新しく作成した構成テンプレートを選択し、**Export** ボタンをクリックします。

   構成テンプレートをエクスポートする (/en-us/netscaler-console-service/media/import-export-3.png)

   対応する構成テンプレートが **.json** 形式でローカルシステムにダウンロードされます。

構成テンプレートをインポートするには:

1. 「**Infrastructure > Configuration > Configuration Templates**」に移動し、「**Import**」ボタンをクリックします。設定テンプレートの.**json**ファイルがあるパスを選択し、.**json**ファイルをアップロードします。既にエクスポート済みの.**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。

   設定テンプレートのインポート(/en-us/netscaler-console-service/media/import-export-4.png)

2. **Configuration Editor**の**File**オプションを使用して、設定テンプレートをインポートすることもできます。**Configuration Editor**のドロップダウンメニューから**File**を選択し、ローカルシステムから**Choose File** (.**json**ファイル) を選択して、設定テンプレートの.**json**ファイルをアップロードします。

   インポートする設定テンプレートファイルを選択(/en-us/netscaler-console-service/media/import-export-5.png)

   注

   設定テンプレートは、ファイルが.**json**形式で保存されている場合にのみインポートできます。ローカルシステムから.**json**ファイル以外の設定テンプレートをインポートすると、エラーが表示され、ファイルのインポートは失敗します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
- 監査レポートの表示
- インスタンス全体の構成変更の監査
- ネットワーク構成に関する構成アドバイスの取得
- NetScaler Consoleインスタンスの構成監査をポーリングする方法
- ConfigChange SNMPトラップの構成監査差分を生成する

監査テンプレートの作成

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場合があります。また、管理対象のNetScalerインスタンス全体で構成の変更を監視し、構成エラーをトラブルシューティングし、突然のシステムシャットダウン後に保存されていない構成を回復したい場合もあります。特定のインスタンスで監査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 Consoleはこれらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合は報告します。構成の不一致があるたびに、NetScaler Console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 Consoleがテンプレートを実行する頻度を設定する。テンプレートは毎日、週の特定の曜日、または月の特定の日付に実行できます。

また、NetScaler Consoleによって生成された差分レポートを、設定可能な指定されたメールアドレスに送信するオプションもあります。このオプションにより、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 Consoleにログインする必要がありません。

注 デフォルトの構成テンプレートでは、**名前の変更**オプションは無効になっています。ただし、カスタム構成テンプレートの名前は変更できます。

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 > 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、コマンドを構成テンプレートとして保存します。左側の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「ipaddress1」のIPアドレスを選択し、**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. 入力ファイルをダウンロードして、コマンドで定義した変数の値を入力し、そのファイルをNetScaler Consoleサーバーにアップロードします。

   b. すべてのインスタンスに対して定義した変数に共通の値を入力します。
8. **次へ**をクリックします。

   ☐
   ](/en-us/netscaler-console-service/media/nmas-config-audit-template-5.png)
9. **テンプレートプレビュー**タブでは、各インスタンスまたはインスタンスグループで実行されるコマンドを評価および検証できます。**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 Consoleでグローバルに設定された時刻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 Consoleでグローバルポーリング間隔を設定するには、**Infrastructure > Configuration > Configuration Audit > Audit Templates**に移動し、**Global Polling Interval**をクリックします。**Poll Interval**フィールドに、NetScaler Consoleがインスタンスをグローバルにポーリングする間隔（分）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設定します。
- **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。

NetScaler インスタンスの構成監査をポーリングする

NetScaler Console は、NetScaler インスタンスで発生する構成変更を検出するために、10 時間ごとに構成監査を自動的にポーリングします。手動で構成監査をポーリングして、最近の変更を検出することもできますが、すべての NetScaler インスタンスの構成をポーリングすると、ネットワークに大きな負荷がかかります。

NetScaler インスタンスの構成監査全体をポーリングする代わりに、選択した1つまたは複数のインスタンスの構成監査のみを手動でポーリングできます。

NetScaler インスタンスの構成監査をポーリングするには:

1. NetScaler Console で、**インフラストラクチャ > 構成 > 構成監査** に移動します。
2. **Configuration Audit** ページの右上隅にある **Poll Now** をクリックします。
3. **Poll Now** ページがポップアップ表示され、ネットワーク内のすべての NetScaler インスタンスをポーリングするか、選択したインスタンスをポーリングする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。

© 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、**Start Polling** をクリックします。

監査レポートを表示

NetScaler Consoleでは、構成監査セクションで構成監査差分レポートを表示およびダウンロードできます。構成監査セクションでは、すべてのインスタンスおよびインスタンスごとの概要レポートをエクスポートできるほか、各インスタンスとテンプレートのペアについて詳細な差分レポートをエクスポートできます。

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。**NetScaler Config Drift**チャートは、**構成監査**ダッシュボードで、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を表示します。**NetScaler Config Drift**チャートをクリックすると、その後の**監査レポート**ページに、「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 Consoleによって表示される差分レポートをダウンロードできます。

NetScaler Consoleには、差分レポートをメール添付ファイルとして自動的に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用意されています。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。

構成監査レポートのエクスポート

1. NetScaler Consoleで、**インフラストラクチャ > 構成 > 構成監査**の順に移動します。
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。
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**Saved Vs Running Diff**にのみ差分があり、一部のインスタンスでは**Template vs Running Diff**にのみ差分があることがわかります。一部のインスタンスでは、**Saved Vs Running Diff**と**Template vs Running Diff**の両方に差分が存在します。

保存済みと実行中の差分:

インスタンスに保存されている構成と、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、**Saved Vs Running Diff**の下にあるインスタンスの**Diff Exists**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。また、「**修正コマンドのエクスポート**」をクリックして、コマンドを.txtファイルにエクスポートすることもできます。その後、関連するNetScalerインスタンスで設定ジョブからコマンドを実行し、そのインスタンスの設定を修正できます。

テンプレートと実行中の設定の差分:

「**テンプレートと実行中の設定の差分**」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設定の差分**」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設定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設定の差分**」の下にあるインスタンスのいずれかで「**差分あり**」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インスタンスがテンプレートが求めているものとは異なる設定になっていることがわかります。

もう一度「**差分あり**」をクリックします。次の画像は、テンプレートが求めている設定と、そのようなコマンドが設定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設定を示しています。修正設定、または設定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設定、および実行中の設定とテンプレートのドリフト設定を使用して、両方向から設定を比較することもできます。

- 監査テンプレートの設定と、インスタンス上の実行中の設定を比較します。
- インスタンス上の実行中の設定と、監査テンプレートを比較します。

デフォルトでは、「テンプレートと実行中の設定のドリフト」設定が選択されています。ドリフト設定を変更するには、NetScaler Console GUIから「**設定監査**」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。また、「**修正コマンドのエクスポート**」をクリックして、コマンドを.txtファイルにエクスポートすることもできます。その後、CLIでコマンドを実行し、そのインスタンスの設定を修正できます。

次の画像は、システムにダウンロードされた.csv差分ファイルの例を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

.csv差分ファイルの例(/en-us/netscaler-console-service/media/nmas-view-config-audit-reports-7.png)

ファイルステータス監査レポートの表示

NetScalerファイルステータス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、NetScaler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、適切に対処できます。

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 Consoleで、**インフラストラクチャ > 構成 > 構成監査**の順に移動します。
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、差分ステータスのインスタンスが一覧表示されます。

   NetScalerファイルステータスの監査レポート(/en-us/netscaler-console-service/media/config-audit-reports-file-status.png)

   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、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。

     `nsconfig`フォルダーに差分が存在します(/en-us/netscaler-console-service/media/config-audit-file-status-diff.png)
   - **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以降変更されていないことを示します。
   - **NA** - このステータスは、ファイルステータスの監視が適用されないことを示します。このステータスは、NetScaler Consoleがインスタンスをポーリングしない場合に表示されます。たとえば、インスタンスが新しく追加された場合や、インスタンスの状態が非アクティブな場合、インスタンスのポーリングは行われません。

このダッシュボードのレポートをエクスポートする

このページのレポートをエクスポートするには、このページの右上にある**Export**アイコンをクリックします。**Export**ページで、次のいずれかを実行できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**今すぐエクスポート**」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するには。
2. 「**エクスポートのスケジュール**」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するには。

注

- 「**毎週**」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いることを確認してください。

設定監査からファイルを除外する

変更が監視されないように、特定のファイルをConfig Auditから除外できます。システム生成ファイルや頻繁に更新されるファイル（例えば、毎日変更されるファイル）に対して除外を使用すると、ノイズを減らし、監査結果における誤検知を回避できます。

Config Auditファイル差分から除外するファイル名（または相対パス）の例：

- 有効なファイル名（または相対パス）
  - `ns.conf`, `ssl/ns.cert`
- 無効なファイル名（または相対パス）
  - `/ns.txt`, `\nsconfig\ns.conf`（除外するファイル名は相対パスである必要があります）
  - `ñs.conf`（除外するファイル名にはASCII文字のみを含める必要があります）
  - `C:/nsconfig/ns.conf`（除外するファイル名にドライブレターパスを使用しないでください）
  - `ssl/../../ns.conf`（除外するファイル名に親ディレクトリトラバーサル `..` を含めないでください）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- `/nsconfig/license/`配下のすべてのファイルは、デフォルトで構成監査から除外されます。NetScaler Consoleは、トークン更新サイクル中に8時間ごとにこのディレクトリにLASファイルを書き込みます。これらのファイルは完全にNetScaler Consoleによって管理されており、顧客のNetScaler構成の一部ではないため、誤検知の**Diff Exists**アラートをトリガーします。この誤検知を防ぐため、`license/`ディレクトリはデフォルトの除外対象として設定されました。必要に応じて、この除外を削除できます。
- ファイルの差分比較は、`/nsconfig`ディレクトリ配下のファイルにのみ適用されます。
- 構成監査からファイルを除外する場合、ユーザーは`/nsconfig`配下の相対パスを指定する必要があります。たとえば、`/nsconfig`配下に`ssl`フォルダーがある場合、除外は次のように指定できます: `ssl/abc.pem`
- `/nsconfig`以外のファイルの差分は、構成監査の差分の一部とは見なされません。

構成監査からファイルを除外するには、次の手順を実行します。

1. **インフラストラクチャ > 設定 > 設定監査** に移動します。
2. **設定**を選択します。
3. **NetScaler構成ファイル設定**で、監査から除外するファイルパスを追加します。
4. **保存**をクリックします。

ConfigChange SNMPトラップの構成監査差分を生成する

ネットワーク内のNetScalerインスタンスで構成変更があるたびに、構成ファイルが更新されます。インスタンスはConfigChange SNMPトラップをNetScaler Consoleに送信します。インスタンスがConfigChange SNMPトラップを送信したときに、NetScaler Consoleがそのインスタンスで構成監査を実行するように有効にすることができます。

監査テンプレート構成と実行中の構成の間に差異がある場合、「監査レポート」ページに「Diff Exists」ステータスメッセージが表示されます。「Diff Exits」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 Consoleで修正コマンドから構成ジョブを作成する方法」を参照してください。

ConfigChange SNMPトラップを受信したときに構成監査テンプレートを実行するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleでは、NetScaler Consoleで構成監査テンプレートを実行するオプションを有効にできます。

1. NetScaler Consoleで、**インフラストラクチャ > 構成 > 構成監査** に移動します。
2. 「**構成監査**」ページで「**設定**」をクリックします。
3. 「**構成変更監査設定**」セクションで編集アイコンをクリックします。
4. 「**netScalerConfigChangeイベントを受信し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 Consoleは、今後netScalerConfigChange SNMPトラップを受信するすべてのインスタンスに対して構成監査を実行します。

5. 「**監査テンプレートを実行するまでの遅延時間（分）**」フィールドに分数を入力します。NetScaler Consoleは、そのインスタンスからConfigChange SNMPトラップを受信した後、この遅延時間の後にNetScalerインスタンスで構成監査テンプレートを実行します。

インスタンス全体の構成変更を監査する

ネットワークの最適なパフォーマンスのために、特定の構成が特定のインスタンスで実行されていることを確認したいとします。また、管理対象のNetScalerインスタンス全体の構成変更を監視し、構成エラーをトラブルシューティングし、突然のシステムシャットダウン後に保存されていない構成を回復したい場合もあります。特定のインスタンスで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 Consoleは、これらのインスタンスを監査テンプレートと比較し、構成に不一致がある場合に報告します。この比較により、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必要があ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 Console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 Consoleによって生成された差分レポートを、設定可能な指定されたメールアドレスに送信することもできます。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、手動でレポートを確認するためにNetScaler Console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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 「**Infrastructure > Configuration > Configuration Audit > Audit Templates**」に移動し、「**Add**」をクリックします。
2. 「**Create Template**」ページで、「**Audit Commands**」タブに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、次の図に示すように「**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。

   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 Consoleサーバーにアップロードします。

   b. すべてのインスタンスに対して定義した変数に共通の値を入力します。
8. **次へ**をクリックします。

   変数値を指定します(/en-us/netscaler-console-service/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する**。このオプションを選択すると、NetScaler Consoleでグローバルに設定された時間にインスタンスでテンプレートが実行されます。
    - **テンプレートのスケジュールをカスタマイズする**。このオプションを使用して、テンプレートを実行する時間と頻度を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **メールでレポートを送信する**。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。

    テンプレートをスケジュールします(/en-us/netscaler-console-service/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` フォルダーに追加、削除、または変更されたファイル

構成の変更を表示(/en-us/netscaler-console-service/media/config-audit-dashboard.png)

NetScaler Consoleでは、構成監査を手動でポーリングすることもでき、インスタンスのすべての構成監査をNetScaler Consoleに即座に追加します。これを行うには、**Infrastructure > Configuration > Configuration Audit** に移動し、**Poll Now** をクリックします。ポップアップページ **Poll Now** には、ネットワーク内のすべてのNetScalerインスタンスをポーリングするか、選択したインスタンスをポーリングするかのオプションが表示されます。

インスタンスで監査を強制することもできます。これを行うには、次のいずれかのグラフをクリックします。

- **NetScaler構成保存ステータス**
- **NetScaler構成ドリフト**

監査レポートページでインスタンスを選択し、**アクション**リストで**今すぐポーリング**を選択します。

今すぐポーリング(/en-us/netscaler-console-service/media/configuration-audit-poll-now.png)

NetScaler構成ファイルステータスグラフには、`nsconfig` フォルダーにあるNetScalerファイルの状態が表示されます。NetScaler Consoleは、`nsconfig` フォルダー内のファイルの変更を記録および比較し、その違いを表示します。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成監査通知を設定する

1. **Infrastructure > Configuration > Configuration Audit** に移動してください。
2. **構成監査**ページで、**設定**をクリックします。
3. **設定**ページで：
   a. 通知設定を有効にするには、**「netScalerConfigChange」イベントの受信時に監査を実行**チェックボックスをオンにします。
   b. 監査の遅延時間を設定します。
4. **構成監査ポーリング**で、**ポーリング間隔**を設定します。

   NetScaler Console は、指定されたポーリング間隔で構成監査イベントをポーリングします。
5. **構成ファイル差分通知**で、通知を受信するプラットフォームを選択します。
   - **メール** - メール配布リストを選択します。「追加」をクリックして、通知を受信するメール配布リストを追加します。
   - **Slack** - リストから Slack チャネルを選択します。「追加」をクリックして、通知を受信するチャネルを追加します。

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達成できるように、NetScalerインスタンスを最適な構成でセットアップします。ただし、一部の構成が標準構成ではない可能性があり、それがアプリケーションのパフォーマンスに影響を与えることがあります。

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 ConsoleはNetScalerインスタンスの構成を分析し、推奨事項を提供します。NetScaler Consoleから推奨される構成を適用できます。

NetScalerインスタンスを分析するには：

1. **インフラストラクチャ > 設定 > 設定監査 > 設定アドバイス** に移動します。
2. 次のいずれかを実行します。
   - **Upload Configuration File** をクリックし、ネットワークインスタンスの構成ファイルをアップロードします。
   - **Select Device** をクリックし、分析するNetScalerインスタンスを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleはインスタンスの構成を分析し、次の図に示すように構成推奨事項のリストを提供します。構成アドバイスの横にあるチェックボックスをクリックして、修正コマンドを表示します。

構成を更新する場合は、修正コマンドの変数に値を指定し、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。

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、次に、**Select Actions** ドロップダウンリストから **Show Events** をクリックします。

Events ページで、構成変更の詳細を表示できます。

© 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。April 15, 2026以降、LASはNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  注: ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026以降、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負

© 1997–2026 Citrix Systems, Inc. All rights reserved.

うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合には適用されません。
NetScaler Consoleを使用して、以下のメンテナンスジョブを作成できます。その後、特定の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 インスタンスをアップグレード
- オートスケールグループ内のNetScalerインスタンスをアップグレード
- NetScalerインスタンスのHAペアを構成
- インスタンスのHAペアをクラスターに変換

注:

アップグレードのために任意の数のNetScalerインスタンスを選択できますが、NetScaler Consoleサービスは、最大100の同時アップグレードスレッドをサポートしています。これは、同時にアップグレードできるインスタンスが100個のみであることを意味します。この制限は動的であり、他のテナントからの同時アップグレードアクティビティに基づいて変動する可能性があります。

アップグレード前の検証

NetScaler Consoleは次のチェックを実行します。

- **`/var`のディスク容量の空き状況**: `/var`パーティションに、イメージの抽出およびインストール操作を安全に実行するために十分な空き容量があることを確認します。
- **/flashのディスク容量の空き状況**: `/flash`パーティションに、インストール中の重要なシステム操作をサポートするために必要な最小限の空きディスク容量があることを確認します。
- **NSPEPI構成チェック**: NetScaler構成ファイルにサポートされていないポリシーまたは無効なポリシーがないかを検証し、インストールまたはアップグレード後の構成エラーを防ぎます。
- **高可用性（HA）構成チェック**: HAの状態と役割の一貫性を検証し、健全でサポートされているHAセットアップを確保します。
- **SSH接続チェック**: リモートインストールおよび管理操作に必要なSSHのアクセシビリティ、信頼性の検証、およびターゲットデバイスへの接続を確認します。
- **ダウングレード用の一致するns.conf**: ダウングレードシナリオのために、適切な互換性のある`ns.conf file`が利用可能であることを確認し、構成の非互換性を防ぎます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

すべての事前チェック結果は次のように統一的に分類されます。

- **クリティカル（ブロック中）**：アップグレードはブロックされています。続行する前に、報告されたすべての問題を解決する必要があります。
- **警告**：管理者の承認があれば、アップグレードを続行できます。
- **アドバイザリ**：管理者の承認があれば、アップグレードを続行できます。

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. NetScaler Consoleで、**Infrastructure > Upgrade Jobs**に移動します。**Create Job**をクリックします。

   メンテナンスジョブの作成(/en-us/netscaler-console-service/media/upgrade-1.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-console-service/media/upgrade-2.png)

3. **Select Instance**で、**Job Name**に任意の名前を入力します。
4. **Add Instances**をクリックして、アップグレードするNetScaler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. **Next**をクリックしてイメージを選択します。**Software Image**リストから次のいずれかのオプションを選択します。
   - **Local** - ローカルマシンからインスタンスアップグレードファイルを選択します。
   - **Appliance** - NetScaler Consoleのファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler Console GUIには、サーバー側にすでにアップロードされているインスタンスファイルが表示されます。
     - **選択したイメージがすでに利用可能な場合、NetScalerへのイメージのアップロードをスキップする** - イメージがすでにNetScalerインスタンスに存在する場合に、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に、NetScalerインスタンスにアップロードされたイメージをクリアするには、このオプションを選択します。

注:

- 選択したインスタンスがすでにターゲットビルドにある場合、警告が表示されます。この警告は、アップグレードジョブ中に誤ったインスタンスが選択されるのを防ぐのに役立ちます。インスタンスを再アップグレードする意図がある場合は、警告を無視してアップグレードを続行してください。

- 選択したインスタンスに既存のアップグレードジョブがすでにスケジュールされている場合、NetScaler Consoleは警告メッセージを表示します。この警告メッセージは、同じNetScalerインスタンスで誤って重複するアップグレードジョブがスケジュールされるのを防ぐのに役立ちます。

6. **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。詳細については、「アップグレード前検証」を参照してください。

重要

クラスターIPアドレスを指定した場合、NetScaler Consoleは指定されたインスタンスに対してのみアップグレード前検証を実行し、他のクラスターノードに対しては実行しません。

7. オプションで、**カスタムスクリプト**で、インスタンスのアップグレード前後に実行するスクリプトを指定します。コマンドを実行するには、次のいずれかの方法を使用します。

   - **ファイルからコマンドをインポート** - ローカルコンピューターからコマンド入力ファイルを選択します。
   - **コマンドを入力** - GUIに直接コマンドを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタムスクリプトを使用して、インスタンスのアップグレード前後の変更を確認できます。例：

- アップグレード前後のインスタンスバージョン。
- アップグレード前後のインターフェース、高可用性ノード、仮想サーバー、およびサービスのステータス。
- 仮想サーバーとサービスの統計。
- 動的ルート。

8. **次へ**をクリックします。**タスクのスケジュール**で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード** - アップグレードジョブはすぐに実行されます。
   - **後でスケジュール** - このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

     NetScaler HAペアを2段階でアップグレードする場合は、**HA内のノードに対して2段階アップグレードを実行**を選択します。

     HAペア内の別のインスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

9. **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NetScalerインスタンスをバックアップします。** - 選択したNetScalerインスタンスのバックアップを作成します。
      - **アップグレードを開始する前にNetScaler構成を保存** - アップグレード前にインスタンスで構成されている構成ジョブを保存します。
      - **NetScaler HAペアでのネットワーク停止を回避するためにISSUを有効にする** - インサービスソフトウェアアップグレード (ISSU) を有効にすると、ネットワークのダウンタイムを引き起こすことなく、NetScaler高可用性 (HA) ペアをアップグレードできます。ISSUは、アップグレード中に既存の接続が維持されるように、アクティブなセッションをノード間でシームレスに移行します。アップグレードワークフローでISSUを有効にした後、システムは顧客によって定義された遅延時間の後にISSU移行の完了をトリガーすることもできます。NetScaler Consoleが完全なISSU移行の完了をトリガー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

することで、接続が持続している場合でもアップグレードが完了します。NetScaler Consoleが移行を完了するまでの待機時間を設定するには、ISSU移行タイムアウトを分単位で指定します。

- **Console Advisory 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、Console Advisory Connectは自動的に有効になります。詳細については、「NetScaler Consoleサービス接続を使用した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。

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. NetScaler Consoleで、**インフラストラクチャ > アップグレードジョブ** に移動します。**ジョブの作成** をクリックします。
2. **NetScaler SDXのアップグレード** を選択し、**続行** をクリックします。
3. **NetScaler SDXのアップグレード** ページの**インスタンスの選択**タブで、次の操作を行います。
   a. **タスク名** を追加します。
   b. **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** (ビルドファイルがNetScaler Console仮想アプライアンスに存在する必要があります) のいずれかを選択します。

      アップロードプロセスが開始されます。
   c. アップグレードプロセスを実行するNetScaler SDXインスタンスを追加します。
   d. **次へ** をクリックします。
4. 「**Schedule Task**」タブで、「**Execution Mode**」リストから「**Now**」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、「**Finish**」をクリックします。
5. NetScaler SDXインスタンスを後でアップグレードするには、「**Execution Mode**」リストから「**Later**」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、「**Finish**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、メールとSlackの通知を有効にすることもできます。通知を有効にするには、「**Receive Execution Report Through Email**」チェックボックスと「**Receive Execution Report through slack**」チェックボックスをクリックします。

   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。

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. NetScaler Consoleで、**Infrastructure > Upgrade Jobs**に移動します。**Create Job**をクリックします。
2. 「**Create Maintenance Jobs**」で、「**Upgrade NetScaler BLX**」を選択し、「**Proceed**」をクリックします。
3. 「**Select Instance**」で、「**Job Name**」に任意の名前を入力します。
4. 「**Add Instances**」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. 「**Next**」をクリックしてイメージを選択します。「**Software Image**」リストから次のいずれかのオプションを選択します。

   - **ローカル** - ローカルマシンからインスタンスアップグレードファイルを選択します。
   - **アプライアンス** - NetScaler Consoleファイルブラウザからインスタンスアップグレードファイルを選択します。NetScaler Console GUIには、`/var/mps/mps_images`にあるインスタンスファイルが表示されます。

     - **選択したイメージがすでに利用可能な場合は、NetScalerへのイメージアップロードをスキップする** - イメージがNetScalerインスタンスにすでに存在する場合は、このオプションを選択します。
     - **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップ** - インスタンスのアップグレード後、NetScalerインスタンス内のアップロードされたイメージをクリアするには、このオプションを選択します。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレード前検証タブに失敗したインスタンスが表示されます。失敗したインスタンスを削除し、**次へ**をクリックします。

> **重要**
>
> クラスターIPアドレスを指定した場合、NetScaler Consoleは指定されたインスタンスに対してのみアップグレード前検証を実行し、他のクラスターノードに対しては実行しません。

7. オプションで、**カスタムスクリプト**で、インスタンスのアップグレード前後に実行するスクリプトを指定します。コマンドを実行するには、次のいずれかの方法を使用します。

   - **ファイルからコマンドをインポート** - ローカルコンピューターからコマンド入力ファイルを選択します。
   - **コマンドを入力** - GUIに直接コマンドを入力します。

   カスタムスクリプトを使用して、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はすぐに実行されます。
   - **後でスケジュール** - このアップグレードジョブを後で実行するには、このオプションを選択します。インスタンスをアップグレードする**実行日**と**開始時刻**を指定します。

     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したい場合に、**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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** - イメージをすぐにアップロードするには、このオプションを選択します。ただし、アップグレードジョブはスケジュールされた時刻に実行されます。
- **実行時にアップロード** - アップグレードジョブの実行時にイメージをアップロードするには、このオプションを選択します。
- **アップグレードを開始する前にNetScalerインスタンスをバックアップ** - 選択したNetScalerインスタンスのバックアップを作成します。
- **アップグレード開始前にNetScaler構成を保存** - アップグレード前にインスタンスで構成されている構成ジョブを保存します。
- **NetScaler HAペアでのネットワーク停止を回避するためにISSUを有効にする** - インサービスソフトウェアアップグレード (ISSU) を有効にすると、ネットワークのダウンタイムを発生させることなく、NetScaler高可用性 (HA) ペアをアップグレードできます。ISSUは、アクティブなセッションをノード間でシームレスに移行することで、アップグレード中に既存の接続が維持されるようにします。アップグレードワークフローでISSUを有効にした後、システムは顧客によって定義された遅延時間の後にISSU移行の完了をトリガーすることもできます。NetScaler Consoleが完全なISSU移行の完了をトリガーすることで、接続が持続する場合でもアップグレードが完了することが保証されます。NetScaler Consoleが移行を完了するまでの待機時間を設定するには、ISSU移行タイムアウトを分単位で指定します。

- **Console Advisory 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、Console Advisory Connectは自動的に有効になります。詳細については、Console Advisory 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** - 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** - 実行レポートをSlackで送信します。Slackプロファイルを追加するには、「Slackプロファイルの作成」を参照してください。

10. **ジョブの作成**をクリックします。

Autoscale™ グループのアップグレードをスケジュールする

Autoscale グループに属するクラウドサービス内のすべてのインスタンスをアップグレードするには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Console で、**Infrastructure > Upgrade Jobs** に移動します。**Create Job** をクリックします。
2. **Upgrade Autoscale Group** を選択し、**Proceed** をクリックします。
3. **Upgrade Settings** タブで、次の操作を行います。
   a. アップグレードする **Autoscale Group** を選択します。
   b. **Image** で、NetScaler のバージョンを選択します。このイメージは、Autoscale グループ内の NetScaler インスタンスの既存のバージョンです。
   c. **NetScaler Image** で、アップグレードする NetScaler バージョンファイルを参照します。

      Graceful Upgrade をオンにすると、アップグレードタスクは指定されたドレイン接続期間が終了するまで待機します。
   d. **Next** をクリックします。
4. **Schedule Task** タブで、次の操作を行います。
   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実行日と開始時刻を選択します。

   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。通知を有効にするには、**Receive Execution Report Through Email**チェックボックスと**Receive Execution Report through slack**チェックボックスをクリックします。
5. **完了**をクリックします。

NetScalerインスタンスのHAペア構成をスケジュールする

1. NetScaler Consoleで、**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。
3. **NetScaler HA Pair**ページの**Instance Selection**タブで、次のようにします。
   a. **タスク名**を追加します。
   b. プライマリIPアドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. セカンダリIPアドレスを入力します。

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（Independent Network Configuration）モードをオンにする**を有効にするためにクリックします。

4. **Schedule Task**タブで、次のいずれかのオプションを選択します。

- **今すぐアップグレード**: NetScalerインスタンスをすぐにアップグレードするには、このオプションを選択します。**完了**をクリックします。
- **後でスケジュール**: NetScaler HAペアを後でアップグレードするには、このオプションを選択します。

5. **後でスケジュール**オプションを選択した場合は、NetScalerインスタンスをアップグレードする**実行日**と**開始時刻**を選択します。

a. 「**NetScaler HAノードのアップグレードを2段階で実行**」を選択します。このオプションを選択すると、両方のノードが正常にアップグレードされるまで、HA SyncとHA Propagationは無効になります。

b. セカンダリノードのアップグレードをスケジュールするには、次のいずれかのオプションを選択します。このオプションを使用すると、ステージ2のアップグレードはステージ1が正常に完了した後にのみ実行されます。

- 「**設定された遅延の後**」：最初のノードのアップグレードが完了してから2番目のノードのアップグレードが開始されるまでの遅延時間（時間単位）を指定します。
- 「**特定の時刻に**」：セカンダリノードのアップグレードの日付と時刻を選択します。

6. 「**セカンダリノードのアップグレードが開始されるまでHAフェイルオーバーを遅延**」を選択します。「**次へ**」をクリックします。

NetScalerインスタンスのHAペア構成をスケジュールする(/en-us/netscaler-console-service/media/flexible-ha-upgrade.png)

7. NetScaler HAペア作成の実行レポートを受信するために、メールとSlack通知を有効にすることもできます。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. NetScaler Consoleで、**Infrastructure > Upgrade Jobs**に移動します。「**Create Job**」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、「**Proceed**」をクリックします。
3. 「**NetScaler HAをクラスターに移行**」ページで、「**インスタンス選択**」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。
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。
6. NetScaler SDXインスタンスのアップグレード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。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チャネルの設定に関する詳細については、NetScalerインスタンスのアップグレードのスケジュールの「**ステップ8**」を参照してください。

ジョブを使用してNetScalerインスタンスをアップグレードする

NetScaler Consoleでは、1つまたは複数のNetScalerインスタンスをアップグレードできます。インスタンスをアップグレードする前に、ライセンスフレームワークとライセンスの種類を把握しておく必要があります。

注: クラシックポリシーを持つインスタンスをアップグレードする場合は、NSPEPIツールを使用して、インスタンスをアップグレードする前にクラシックポリシーをアドバンストポリシーに変換することをお勧めします。これは、NSPEPIツールでサポートされている機能に適用されます。詳細については、「クラシックポリシーを使用した構成のアップグレードに関する考慮事項」を参照してください。

前提条件

NetScaler Consoleは、アップグレードするインスタンスに対して次の事前検証チェックを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **ディスク容量の確認** - インスタンスのアップグレードに十分なディスク容量を確保するために、ディスクスペースをクリーンアップします。ディスクの問題がある場合は解決します。
2. **ディスクハードウェアの問題の確認** - ハードウェアの問題がある場合は解決します。
3. **カスタマイズの確認** - カスタマイズをバックアップし、インスタンスから削除します。インスタンスのアップグレード後に、バックアップしたカスタマイズを再適用できます。
4. **ポリシーの問題** - NetScalerは、`13.1`バージョン以降、クラシックポリシーをサポートしていません。このバージョンにインスタンスをアップグレードする前に、クラシックポリシーをアドバンストポリシーに移行してください。

   詳細については、「クラシックポリシーとアドバンストポリシー」を参照してください。
5. **STAYPRIMARYおよびSTAYSECONDARYノードの確認** - NetScaler HAの場合、STAYPRIMARYおよびSTAYSECONDARY状態のノードではアップグレードがブロックされます。これらのノードは事前検証チェックで特定され、**アップグレードがブロックされたインスタンス**の下にリストされます。

カスタマイズされたNetScaler構成のアップグレードに関する考慮事項

アップグレードの変更とカスタマイズの両方が、アップグレードされたNetScalerアプライアンスに適用されることが重要です。したがって、/etcディレクトリにカスタマイズされた構成ファイルがある場合は、NetScalerアプライアンスのアップグレードを続行する前に、「カスタマイズされた構成ファイルのアップグレードに関する考慮事項」を参照してください。実行する必要がある主な手順は次のとおりです。

1. NetScalerでのアップグレード前の手順
   - アップグレード前にカスタマイズされたファイルをバックアップする
   - アップグレード前にカスタマイズされたファイルのシンボリックリンクを削除する
2. ADMを使用してNetScalerをアップグレードします。アップグレードするには、ページ冒頭の指示に従ってください。
3. NetScalerでのアップグレード後の手順
   - アップグレード後にカスタマイズを復元する(https://docs.citrix.com/ja-jp/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-considerations-customized-files.html#apply-customizations-to-upgraded-file-and-add-persistency-after-upgrade)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレード前とアップグレード後の両方の手順は、各NetScalerインスタンスで実行する必要があります。ただし、手順2では、ADMを使用してNetScalerをアップグレードするために、脆弱なNetScalerインスタンスをすべて選択して同時にアップグレードできます。

NetScaler高可用性ペア

NetScaler高可用性ペアをアップグレードする際は、次の点に注意してください。

- セカンダリノードが最初にアップグレードされます。
- 両方のノードが正常にアップグレードされるまで、ノードの同期と伝播は無効になります。
- 高可用性ペアのアップグレードが正常に完了すると、実行履歴にエラーメッセージが表示されます。このメッセージは、高可用性ペア内のノードが異なるビルドまたはバージョンである場合に表示されます。これは、プライマリノードとセカンダリノード間の同期が無効になっていることを示します。

NetScaler高可用性ペアは、次の2つの段階でアップグレードできます。

1. アップグレードジョブを作成し、いずれかのノードで直ちに実行するか、後でスケジュールします。
2. 残りのノードで実行するアップグレードジョブを後でスケジュールします。このジョブは、最初のノードのアップグレード後にスケジュールするようにしてください。

NetScalerクラスター

NetScalerクラスターをアップグレードする際、アップグレード前の検証段階では、NetScaler Consoleは指定されたインスタンスのみを検証します。そのため、クラスターノードで以下の問題を確認し、解決してください。

- カスタマイズ
- ディスク使用量
- ハードウェアの問題

NetScalerアップグレードジョブの作成

NetScalerアップグレードジョブを作成するには、次の手順を実行します。

1. **Infrastructure > Upgrade Jobs** に移動します。

   メンテナンスジョブの作成(/en-us/netscaler-console-service/media/upgrade-1.png)
2. **Create Maintenance Jobs** で、**Upgrade NetScaler (Standalone/High-Availability/Cluster)** を選択し、**Proceed** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレードメンテナンスジョブの選択(/en-us/netscaler-console-service/media/upgrade-2.png)

注:

オートスケールグループをアップグレードするには、「オートスケールグループのアップグレード」を参照してください。

3. **Select Instances** タブで、,
   a. **Job Name** に任意の名前を指定します。
   b. アップグレードするNetScalerインスタンスを追加するには、**Add Instances** をクリックします。
      - NetScaler高可用性ペアをアップグレードするには、高可用性ペアのIPアドレス（「S」と「P」の添え字で示されます）を選択します。
      - クラスターをアップグレードするには、クラスターIPアドレス（「C」の添え字で示されます）を選択します。

      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-console-service/media/upgrade-add-instances.png)
   c. **OK**をクリックします。
4. **イメージの選択**タブで、イメージライブラリ、ローカル、またはアプライアンスからNetScalerイメージを選択します。
   - **イメージライブラリから選択**: リストからNetScalerイメージを選択します。このオプションには、NetScalerダウンロードWebサイトで利用可能なすべてのNetScalerイメージが表示されます。

     NetScalerイメージ(/en-us/netscaler-console-service/media/adc-images.png)

     NetScalerソフトウェアイメージには、星のアイコンが付いた推奨ビルドと、ブックマークアイコンが付いた最もダウンロードされたビルドが表示されます。
   - **ローカルまたはアプライアンスから選択**: ローカルコンピューターまたはNetScalerアプライアンスからイメージをアップロードできます。NetScalerアプライアンスを選択すると、NetScaler Console GUIに`/var/mps/ns_images`にあるインスタンスファイルが表示されます。NetScaler Console GUIからイメージを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **選択したイメージがすでに利用可能な場合は、NetScalerへのイメージのアップロードをスキップする** - このオプションは、選択したイメージがNetScalerで利用可能かどうかを確認します。アップグレードジョブは新しいイメージのアップロードをスキップし、NetScalerで利用可能なイメージを使用します。
- **アップグレード成功時にNetScalerからソフトウェアイメージをクリーンアップする** - このオプションは、インスタンスのアップグレード後、NetScalerインスタンスにアップロードされたイメージをクリアします。

次へをクリックして、選択したインスタンスのアップグレード前検証を開始します。

注:

- ダウンロードされたNetScalerイメージはエージェントに保存され、`/var/mps/adcimages`にあります。これらのキャッシュされたイメージは複数のNetScalerアップグレードに使用できるため、アップグレードのたびにイメージをダウンロードする必要がなくなります。
- NetScaler Consoleは、イメージの最終変更時間に基づいて、キャッシュされたNetScalerイメージを3日ごとにクリアします。一度にエージェントにキャッシュされるのは、最新の2つのイメージファイルのみです。

5. 「**アップグレード前検証**」タブには、以下のセクションが表示されます。

- **アップグレード準備完了インスタンス**。これらのインスタンスのアップグレードを続行できます。
- **アップグレードがブロックされたインスタンス**。これらのNetScalerインスタンスは、アップグレード前検証エラーのため、アップグレードがブロックされています。

  エラーを確認し、修正してから、**アップグレード準備完了に移動**をクリックしてアップグレードできます。インスタンスでディスク容量不足に直面した場合は、ディスク容量を確認してクリーンアップできます。「NetScalerディスク容量のクリーンアップ」を参照してください(#clean-up-the-adc-disk-space)。

- **ポリシーチェック**: NetScaler Consoleがサポートされていないクラシックポリシーを検出した場合、アップグレードジョブを作成するために、そのようなポリシーを削除できます。

© 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 Consoleは、指定されたインスタンスに対してのみアップグレード前検証を実行し、他のクラスターノードに対しては実行しません。

アップグレード中にプライマリノードとセカンダリノード間の不一致を表示するには、高可用性ノードを選択し、**詳細**をクリックします。

- **HAのプライマリノードで見つかった構成の不一致** - NetScaler®高可用性ペアのセカンダリノードで見つかったが、プライマリノードにはないすべての構成を表示します。
- **HAのセカンダリノードで見つかった構成の不一致** - NetScaler高可用性ペアのプライマリノードで見つかったが、セカンダリノードにはないすべての構成を表示します。

注:

構成の不一致セクションに表示される可能性のある以下の不一致は無視できます。

- IPアドレスなどのデバイス固有の設定。
- 暗号化されたパスワードまたは証明書。これらは、パスワードが同じであってもノード間で異なる場合があります。

不一致を確認し、関連性がない場合は無視することを選択できます。

6. **検証スクリプト**で、インスタンスのアップグレード前後に実行するスクリプトを指定します。次のいずれかを実行できます。

   - **デフォルト検証スクリプト** - このオプションを選択すると、事前定義された検証スクリプトが実行されます。これらのスクリプトは、アップグレードジョブの前後両方で実行され、検証スクリプトの差分レポートが生成されます。

     注:

     これらの事前定義されたコマンドセットを変更または編集することはできません。

   - **カスタム検証スクリプト** - このオプションを選択すると、独自の検証スクリプトが実行されます。スクリプトをアップグレード前またはアップグレード後に実行するかどうかを指

© 1997–2026 Citrix Systems, Inc. All rights reserved.

定できます。差分レポートは、アップグレードの前後で同じスクリプトが選択されている場合にのみ生成されます。

各構成のコマンドセットを知るには、**詳細表示**をクリックします。 詳細については、「カスタムスクリプトの使用」を参照してください。

7. **タスクのスケジュール**で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード**: アップグレードジョブはすぐに実行されます。
   - **後でスケジュール**: この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。

   NetScalerの高可用性ペアを2段階でアップグレードする場合は、**高可用性ノードの2段階アップグレードを実行**を選択します。

   高可用性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。

   詳細については、「NetScaler高可用性ペア」(#adc-high-availability-pair)を参照してください。

8. **ジョブの作成**で、次の詳細を指定します。

   アップグレードジョブをスケジュールする場合、インスタンスにイメージをアップロードするタイミングを指定できます。

   - **今すぐアップロード**: このオプションを選択すると、イメージがすぐにアップロードされます。ただし、アップグレードジョブはスケジュールされた時刻に実行されます。
   - **実行時にアップロード**: このオプションを選択すると、アップグレードジョブの実行時にイメージがアップロードされます。

   高可用性ペアの場合、イメージをアップロードするノードを指定できます。

   - **プライマリノードとセカンダリノードの両方にアップロード**: ビルドイメージファイルをプライマリノードとセカンダリノードの両方にアップロードします。
   - **セカンダリノードのみにアップロード**: ビルドイメージファイルをセカンダリノードのみにアップロードします。セカンダリノードがアップグレードされると、フェイルオーバーが発生し、以前プライマリノードだった新しいセカンダリノードにビルドイメージファイルがアップロードされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性ペアで利用可能なスケジューリングシナリオの詳細については、「NetScaler高可用性ペアのアップグレードジョブのスケジュール」(#scheduling-upgrade-jobs-for-an-adc-high-availability-pair)を参照してください。

その他のアップグレードオプションの詳細については、「NetScalerアップグレードオプション」(#adc-upgrade-options)を参照してください。

9. **ジョブの作成**をクリックします。

アップグレードジョブは、**インフラストラクチャ > アップグレードジョブ**に表示されます。既存のジョブを編集する場合、必要なフィールドがすでに記入されていれば、任意のタブに切り替えることができます。たとえば、**構成の選択**タブにいる場合、**ジョブプレビュー**タブに切り替えることができます。

スケジュールされたアップグレードジョブの一時停止または再開

スケジュールされたアップグレードジョブを一時停止することもできます。

この機能を使用するには、**Infrastructure > Upgrade Jobs** に移動し、既存のスケジュールされたアップグレードジョブを選択して、**Stop** をクリックしてジョブを一時停止します。スケジュールされたアップグレードジョブを再開するには、**Resume** をクリックします。

スケジュールされたジョブを停止または再開する(/en-us/netscaler-console-service/media/upgrade-job-pause-resume.png)

注:

アップグレードジョブを再開することを決定した後、スケジュールされた時間が過ぎていた場合は、アップグレードジョブを再度作成する必要があります。

失敗したアップグレードジョブを再試行する

1. **Infrastructure > Upgrade Jobs** で、失敗したアップグレードジョブを選択し、**Retry** をクリックします。または、**Select Action > Retry Upgrade Job** に移動して、失敗したジョブを再試行することもできます。

   失敗したジョブを再試行する(/en-us/netscaler-console-service/media/retry-failed-job-main-page.png)

2. **Select Instance** で、次の詳細を指定します。

   - **ジョブ名** - アップグレードの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- リストからアップグレードするNetScalerインスタンスを選択します。インスタンスを削除するには、**Remove** をクリックします。

Next をクリックして検証プロセスを開始します。

失敗したジョブを再試行する(/en-us/netscaler-console-service/media/retry-job-select-instance.png)

3. **Pre-upgrade validation** タブには、次のセクションが表示されます。

   - **アップグレード準備完了インスタンス**。これらのインスタンスのアップグレードを続行できます。
   - **アップグレードがブロックされているインスタンス**。これらのNetScalerインスタンスは、アップグレード前の検証エラーのため、アップグレードがブロックされています。

     エラーを確認して修正し、「**アップグレード準備完了に移動**」をクリックしてアップグレードできます。インスタンスでディスク容量不足が発生した場合は、ディスク容量を確認してクリーンアップできます。「NetScalerディスク容量のクリーンアップ」(#clean-up-the-adc-disk-space)を参照してください。
   - **ポリシーチェック**: NetScaler Consoleがサポートされていないクラシックポリシーを検出した場合、そのようなポリシーを削除してアップグレードジョブを作成できます。

   ☐ 「**次へ**」をクリックします。

4. 「**タスクのスケジュール**」で、次のいずれかのオプションを選択します。

   - **今すぐアップグレード**: アップグレードジョブはすぐに実行されます。
   - **後でスケジュール**: この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したいときに、「**実行日**」と「**開始時刻**」を指定します。

   ☐ 「**再試行**」をクリックします。

NetScalerディスク容量のクリーンアップ

NetScalerインスタンスのアップグレード中にディスク容量不足の問題が発生した場合は、NetScaler Console GUIからディスク容量をクリーンアップします。

1. 「**アップグレード前の検証**」タブの「**アップグレードがブロックされているインスタンス**」セクションには、ディスク容量不足のためアップグレードに失敗したインスタンスが表示されます。ディスク容量の問題があるインスタンスを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 「**ディスク容量の確認**」をクリックします。

   「**ディスク容量の詳細**」ペインが表示されます。このペインには、インスタンス、使用済みメモリ、および利用可能なメモリが表示されます。

3. **ディスク領域の詳細**ペインで、クリーンアップが必要なインスタンスを選択し、次のいずれかを実行します。

   a. **ディスククリーンアップ** - 必要なフォルダーまたはディレクトリに移動し、それらを削除してディスク領域を解放します。

   b. **クイッククリーンアップ** - 複数のフォルダーを削除して、ディスク領域をすばやくクリアします。表示される**確認**ペインで、削除するフォルダーを選択し、**はい**をクリックします。

   c. ディスク領域をクリアした後、インスタンスをアップグレードするのに十分なディスク領域が利用可能になったかどうかを確認できます。**アップグレードがブロックされているインスタンス**セクションで、**再検証**をクリックします。

   次の例では、ディスク領域が利用可能です。インスタンスをアップグレードするには、**アップグレード準備完了に移動**をクリックするか、次のステップに進むには**次へ**をクリックします。

カスタムスクリプトを使用する

NetScalerアップグレードジョブを作成する際に、カスタムスクリプトを指定できます。カスタムスクリプトは、NetScalerインスタンスのアップグレード前後の変更を確認するために使用されます。例:

- アップグレード前後のインスタンスバージョン。
- アップグレード前後のインターフェース、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。

次の段階で実行するカスタムスクリプトを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アップグレード前**: 指定されたスクリプトはインスタンスのアップグレード前に実行されます。
- **アップグレード後フェイルオーバー前 (HAに適用)**: このステージは高可用性展開にのみ適用されます。指定されたスクリプトはノードのアップグレード後に実行されますが、フェイルオーバー前です。
- **アップグレード後 (スタンドアロンに適用) / アップグレード後フェイルオーバー後 (HAに適用)**: 指定されたスクリプトはスタンドアロン展開でインスタンスのアップグレード後に実行されます。高可用性展開では、スクリプトはノードのアップグレードとそのフェイルオーバー後に実行されます。

注:

- 必要なステージでスクリプトまたはコマンドの実行を有効にしてください。そうしないと、指定されたスクリプトは実行されません。
- 差分レポートは、アップグレード前とアップグレード後のステージで同じスクリプトを指定した場合にのみ生成されます。したがって、アップグレード後のステージで**アップグレード前と同じスクリプトを使用**を選択するようにしてください。参照: NetScalerアップグレードジョブの統合差分レポートをダウンロードする。

スクリプトファイルをインポートするか、NetScaler Console GUIに直接コマンドを入力できます。

- **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。

アップグレード後のステージでは、アップグレード前のステージで指定したスクリプトと同じものを使用できます。

NetScalerアップグレードオプション

NetScalerアップグレードジョブを作成する際に、**ジョブの作成**タブで以下のオプションを選択できます。

- **アップグレードを開始する前にNetScalerインスタンスをバックアップする。**: 選択したNetScalerインスタンスのバックアップを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アップグレード後も高可用性ノードのプライマリおよびセカンダリステータスを維持する**: 各ノードのアップグレード後にアップグレードジョブがフェイルオーバーを開始するようにしたい場合は、このオプションを選択します。これにより、アップグレードジョブはノードのプライマリおよびセカンダリステータスを維持します。
- **アップグレード開始前にNetScaler構成を保存** - NetScalerインスタンスをアップグレードする前に、実行中のNetScaler構成を保存します。
- **NetScaler HAペアでのネットワーク停止を回避するためにISSUを有効にする** - ISSUは、NetScaler高可用性ペアでのゼロダウンタイムアップグレードを保証します。このオプションは、アップグレード中に既存の接続を維持する移行機能を提供します。そのため、ダウンタイムなしでNetScaler高可用性ペアをアップグレードできます。ISSU移行タイムアウトを分単位で指定します。
- **メールで実行レポートを受信する** - 実行レポートをメールで送信します。メール配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。

NetScaler高可用性ペアのアップグレードジョブのスケジュール設定

次の表に、**タスクのスケジュール**ページでのさまざまなスケジュール設定シナリオと、**ジョブの作成**ページで利用可能な対応するアップグレードオプションを示します。

アップグレードジョブを実行するタイミングはいつですか？	ソフトウェアイメージをNETSCALERにアップロードするタイミングはいつですか？	ビルドイメージをHAノードにアップロードする方法は？
今すぐアップグレード	該当なし	**プライマリノードとセカンダリノードの両方にアップロード** (デフォルトオプション)
	セカンダリノードのみにアップロード	
後でスケジュール	**実行時にアップロード**（デフォルトオプション）	**プライマリノードとセカンダリノードの両方にアップロード**（デフォルトオプション）
	セカンダリノードのみにアップロード	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレードジョブを実行するタイミングはいつですか？	ソフトウェアイメージをNETSCALERにアップロードするタイミングはいつですか？	ビルドイメージをHAノードにアップロードする方法は？
	今すぐアップロード	該当なし
後でスケジュール（HAのノードに対して2段階アップグレードを実行が選択されている場合）	**実行時にアップロード**（デフォルトオプション）	**セカンダリノードのみにアップロード**（デフォルトかつ唯一のオプション）
	今すぐアップロード	該当なし

NetScalerアップグレードジョブの統合差分レポートをダウンロードする

NetScaler Consoleでは、NetScalerアップグレードジョブの差分レポートをダウンロードできます。そのためには、アップグレードジョブにカスタムスクリプトが必要です。差分レポートには、アップグレード前スクリプトとアップグレード後スクリプトの出力間の違いが含まれています。このレポートを使用すると、アップグレード後にNetScalerインスタンスでどのような変更が発生したかを判断できます。

注:

差分レポートは、アップグレード前とアップグレード後の段階で同じスクリプトを指定した場合にのみ生成されます。

アップグレードジョブの差分レポートをダウンロードするには、次の手順を実行します。

1. **インフラストラクチャ > 構成ジョブ > メンテナンスジョブ** に移動します。
2. 差分レポートをダウンロードするアップグレードジョブを選択します。
3. 「**Diff Reports**」をクリックします。
4. 「**Diff Reports**」で、選択したアップグレードジョブの統合差分レポートをダウンロードします。

   このページでは、以下のいずれかの差分レポートタイプをダウンロードできます。

   - **アップグレード前とアップグレード後（フェイルオーバー前）の差分レポート**
   - **アップグレード前とアップグレード後の差分レポート**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerアップグレードジョブの差分レポートをダウンロード(/en-us/netscaler-console-service/media/diff-reports-page.png)

ネットワーク機能

ネットワーク機能機能を使用すると、管理対象のCitrix Application Delivery Controller (NetScaler) インスタンスに構成されているエンティティの状態を監視できます。ロードバランシング仮想サーバーの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。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台
- サーバー接続数が最も多い仮想サーバー上位5台
- スループットが最大 (MB/秒) の仮想サーバー上位5台
- スループットが最小 (MB/秒) の仮想サーバー下位5台
- 仮想サーバーが最も多いインスタンス上位5台
- 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方式
- ロードバランシングの永続性

ロードバランシングエンティティのレポートを生成する

NetScaler Consoleでは、Citrix Application Delivery Controller (NetScaler) インスタンスエンティティのレポートをすべてのレベルで表示できます。**NetScaler Console > 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、統合または要約されたレポートをダウンロードして表示できます。

このレポートでは、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

統合レポートはCSV形式です。各列のエントリは次のとおりです。

- **NetScaler IPアドレス**: NetScalerインスタンスのIPアドレスがレポートに表示されます。
- **NetScalerホスト名**: ホスト名がレポートに表示されます。
- **パーティション**: 管理パーティションのIPアドレスが表示されます。
- **仮想サーバー**: \<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **サービス**: \<name_of_the_service\>#service-IP_address:port_number
- **サービスグループ**: \<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

注

- ホスト名が利用できない場合は、対応するIPアドレスが表示されます。
- 空白の列は、それぞれのエンティティがそのNetScalerインスタンス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 Consoleでは、レポートを即座にダウンロードできます。また、レポートを1日1回、週に1回、または月に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。

統合ロードバランシングレポートを生成する

1. NetScaler Consoleで、**Infrastructure > Network Functions** に移動します。
2. **Generate Report** をクリックします。
3. 開いた **Generate Report** ページで、レポートを表示するための2つのオプションがあります。
   a. **Export Now** タブで、**Load Balancing** を選択し、**OK** をクリックします。

      統合レポートがシステムにダウンロードされます。
   b. **Schedule Report** を選択して、定期的にレポートを生成およびエクスポートするスケジュールを作成します。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. **Enable Schedule** を選択します。

ii. **繰り返し** - リストから **毎日**、**毎週**、または **毎月** を選択します。

> **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。

レポートをスケジュールする (/en-us/netscaler-console-service/media/load-balancing-scheduled-report.png)

> **注**
>
> **月次**の繰り返しを選択した場合は、1から31までの値で月の日数を入力してください。

iii. **エクスポート時刻** - 時:分 の24時間形式で時刻を入力します。

iv. **メール** - チェックボックスをオンにしてリストからプロファイルを選択するか、「**追加**」をクリックしてメールプロファイルを作成します。

v. **Slack** - Slackチェックボックスをオンにしてリストボックスからプロファイルを選択するか、「**追加**」をクリックしてSlackプロファイルを作成します。

vi. 「**スケジュール**」をクリックしてプロセスを完了します。

個別のロードバランシング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ロードバランシングサービスの一覧を表示したいシナリオを考えてみましょう。

1. NetScaler Consoleで、**インフラストラクチャ > ネットワーク機能 > ロードバランシング > 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。

   レポートのエクスポート(/en-us/netscaler-console-service/media/services-export.png)

   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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

レポートはダウンロードするか、メールの添付ファイルとしてエクスポートすることしかできません。NetScaler Console GUIでレポートを表示することはできません。

ネットワーク機能レポートのエクスポートまたはエクスポートのスケジュール設定

NetScaler Console では、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 などの選択し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、ネットワーク内に存在するインスタンス、パーティション、および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、およびサービス) 間のマッピングの概要を把握できます。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さまざまな間隔でエクスポートするようにスケジュールできます。メール通知の設定方法については、「イベントルールの作成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

- GSLB仮想サーバーの場合、ネットワーク機能レポートはGSLB仮想サーバーと関連サービスのみを表示します。
- コンテンツスイッチングおよびキャッシュリダイレクション仮想サーバーの場合、レポートには、関連するLBサーバーへのバインディングのみが表示されます。
- SSL仮想サーバーは、NetScaler ConsoleでSSL仮想サーバーの個別のリストが管理されていないため、このレポートには表示されません。
- 新しいレポートが生成されると、古いレポートはアカウントから自動的に削除されます。

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、右側のペインにあるページの右上隅の**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. **Schedule Report**を選択して、定期的にレポートを生成およびエクスポートするスケジュールを作成します。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** - 24時間形式で時:分を入力します。

      iii. **メール** - チェックボックスを選択し、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、**追加**をクリックしてメールプロファイルを作成します。

      iv. **Slack** - チェックボックスを選択し、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、**追加**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 Console でネットワークレポートを監視することで、リソースの使用状況を最適化できます。複数の場所に多くのアプリケーションが展開されている分散展開環境があるかもしれません。アプリケーションの最適なパフォーマンスを確保するために、トラフィックの負荷分散、コンテンツスイッチ、または圧縮を行うために、複数の Citrix Application Delivery Controller (NetScaler) インスタンスも展開しています。ネットワークパフォーマンスはアプリケーションパフォーマンスに影響を与える可能性があります。アプリケーションのパフォーマンスを維持し続けるには、ネットワークパフォーマンスを定期的に監視し、すべてのリソースが最適に使用されていることを確認する必要があります。

NetScaler Console を使用すると、グローバルレベルのインスタンスや、仮想サーバーやネットワークインターフェースなどのエンティティのレポートを生成できます。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 Console では、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ます。

ネットワークレポートダッシュボード

次の画像は、ダッシュボードのさまざまな機能を示しています。

ネットワークレポートダッシュボードの概要 (/en-us/netscaler-console-service/media/network-rprt-dashboard1.png)

- 左側のパネルには、NetScaler Console で作成されたすべてのカスタムダッシュボードが表示されます。いずれかをクリックすると、そのダッシュボードを構成するさまざまなレポートを

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表示できます。たとえば、TCP および SSL ダッシュボードには、TCP および SSL プロトコルに関連するさまざまなレポートが含まれています。

- 各ダッシュボードは、複数のウィジェットでカスタマイズして、さまざまなレポートを表示できます。ウィジェットはダッシュボード上のレポートを表し、それは関連する複数のレポートの集合です。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。NetScaler Consoleで生成されるレポートの期間をカスタマイズするには、タイムラインスライダーオプションを使用できます。
- 「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。レポートを送信したいメール配信リストを設定することもできます。
- ダッシュボード上部の「インスタンス」セクションには、レポートが生成されるすべてのインスタンスのIPアドレスが一覧表示されます。
- 「X」をクリックしてインスタンスを削除するか、レポートにインスタンスを追加できます。ただし、現在NetScaler Consoleでは10個のインスタンスのレポートを表示できます。
- ダッシュボード全体を.pdf、.jpeg、.png、または.csv形式でシステムにエクスポートすることもできます。ダッシュボードに加えた変更はすべて保存する必要があります。変更を保存するには、をクリックします。

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 Consoleで、**インフラストラクチャ > ネットワークレポート**に移動します。

   ダッシュボードを作成(/en-us/netscaler-console-service/media/nw-dash.png)
2. 既存のダッシュボードを表示するには、**をクリックします。ネットワークレポートのダッシュボード**ページが開き、すべてのダッシュボードとレポートウィジェットを表示できます。
3. ダッシュボードを作成するには、****をクリックします。

   ****ページが開きます。

   ダッシュボードの種類を選択(/en-us/netscaler-console-service/media/nw-dash-create.png)
4. ****タブで、次の詳細を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **名前**。ダッシュボードの名前を入力します。
b. **インスタンスファミリー**。インスタンスのタイプ（NetScalerまたはNetScaler SDX）を選択します。

a. **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、ロードバランシング仮想サーバーを選択します。
b. **説明**。ダッシュボードのわかりやすい説明を入力します。

5. 「**次へ**」をクリックします。
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。

   レポートの選択(/en-us/netscaler-console-service/media/nw-dash-rprt.png)
7. 「**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。
8. 監視するエンティティを選択します。

   エンティティの選択(/en-us/netscaler-console-service/media/nw-dash-entities.png)
9. 「**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。

集計を適用してネットワークレポートデータを表示する

ネットワークパフォーマンスデータに集計を適用し、ダッシュボードでアプリケーションパフォーマンスを表示できます。要件に基づいて結果をエクスポートすることもできます。データに適用されたこれらの集計を使用して、すべてのリソースが最適に使用されているかどうかを分析および確認できます。 **>** に移動し、 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、 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。 をクリックし、 を選択します。

追加できる集計は次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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
- 最初
- 最後

ダッシュボードには最大4つの集計オプションを追加できます。集計オプションを追加すると、NetScaler Console は選択し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。

ネットワークレポートのエクスポート

ウィジェットレポートは.pdf、.png、.jpeg、または.csv形式でエクスポートできますが、ダッシュボード全体は.pdf、.jpeg、または.png形式でのみエクスポートできます。

注

読み取り専用権限がある場合、NetScaler Console でレポートをエクスポートすることはできません。NetScaler Console でファイルを作成し、エクスポートするには編集権限が必要です。

ダッシュボードレポートをエクスポートするには:

1. **Infrastructure > Network Reporting** に移動します
2. 作成したすべてのダッシュボードを表示するには、**View Dashboards** をクリックします。
3. 左側の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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 「**今すぐエクスポート**」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. 「**エクスポートのスケジュール**」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。

   ネットワークレポート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ている場合、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ます。
- 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ます。

ネットワークレポートをスケジュールする際に、「**件名**」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。

たとえば、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

「

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、レポートに見出しを追加することはできません。

「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. ページの右上隅にあるエクスポートボタンをクリックします。
6. **「Export Now」**タブで、必要な形式を選択し、**「Export」**をクリックします。

   レポートのエクスポート(/en-us/netscaler-console-service/media/nw-dash-widget-export.png)

NetScaler Consoleでのネットワークレポートのしきい値の管理方法

NetScalerインスタンスの状態を監視するには、カウンターにしきい値を設定し、しきい値を超過したときに通知を受け取ることができます。NetScaler Consoleでは、しきい値を構成し、表示、編集、削除できます。

たとえば、コンテンツスイッチング仮想サーバーのConnectionsカウンターが指定された値に達したときに、電子メール通知を受け取ることができます。特定のインスタンスタイプにしきい値を定義できます。また、選択したインスタンスから特定のカウンターメトリックに対して生成するレポートを選択することもできます。

カウンターの値がしきい値を超過または下回った場合（ルールで指定されている場合）、パフォーマンス関連の問題を示すために、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される値に戻ると、イベントはクリアされます。これらのイベントは、**Infrastructure > Events > Reports**に移動して表示できます。**「Reports」**ページで、**「Events by Severity」**ドーナツをクリックして、重大度別にイベントを表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

しきい値が侵害されたときに電子メールまたはSMSメッセージを送信するなど、しきい値にアクションを関連付けることもできます。

しきい値を作成するには：

1. NetScaler Consoleで、**Infrastructure > Network Reporting > Thresholds**に移動します。「**Thresholds**」の下にある「**Add**」をクリックします。
2. 「**Create Threshold**」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インスタンス。
   - 「**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。「**Configure Rule**」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か、しきい値以下かを確認するための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%に達した場合に、重大なイベント重大度でイベントを生成したいとします。この場合、しきい値として80と入力します。「重大なイベント」は、**インフラストラクチャ > イベント** > **レポート**に移動して表示できます。**レポート**ページで、**重大度別イベント**ドーナツをクリックすると、重大度別にイベントを表示できます。
   - **クリア値**。値をクリアするタイミングを示す値を入力します。たとえば、監視対象の値が50%に達したときに、現在のクライアント接続のしきい値をクリアしたいとします。この場合、クリア値として50と入力します。
   - **イベントの重大度**。しきい値に設定するセキュリティレベルを選択します。
4. しきい値を設定するインスタンスとエンティティを選択できます。**インスタンス**セクションで、次のいずれかのオプションを選択します。
   - **すべてのインスタンス**。すべてのインスタンスにしきい値が設定されます。
   - **特定のインスタンス**。特定のインスタンスにしきい値が設定されます。右矢印を使用して、**利用可能**リストから**構成済み**リストにインスタンスを移動します。しきい値は、**構成済み**リストのインスタンスに設定されます。
   - **特定のエンティティ**。特定のエンティティにしきい値が設定されます。

     エンティティを選択するには、**追加**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レポート名フィールドで選択し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。

- [ ] しきい値を設定するエンティティを選択します。**選択**をクリックします。選択したエンティティが**インスタンス**セクションに表示されます。

5. しきい値に達したときにメッセージを表示するように選択できます。**イベントメッセージ**セクションで、メッセージボックスにメッセージを入力します。NetScaler Consoleは、監視対象の値としきい値をこのメッセージに追加します。
6. **通知設定**セクションで、**しきい値を有効にする**を選択して、アラームを生成するしきい値を有効にします。オプションで、**電子メールで通知**を選択すると、しきい値に達したときに、電子メール、Slack、ServiceNow、PagerDutyなどのさまざまなチャネルを通じて通知を受け取ることができます。
7. 「**作成**」をクリックします。

ネットワークレポートのパフォーマンスポーリング間隔を設定する

デフォルトでは、5分ごとにNITRO呼び出しがネットワークレポートのパフォーマンスデータを収集します。NetScaler Consoleは、カウンター情報などのインスタンス統計を取得し、1分ごと、1時間ごと、1日ごと、または1週間ごとに集計します。この集計データは、事前定義されたレポートで表示できます。

パフォーマンスポーリング間隔を設定するには、**Infrastructure > Network Reporting** に移動し、**Configure Polling Interval** 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。

ポーリング間隔の設定(/en-us/netscaler-console-service/media/networkreportingpolling.png)

ネットワークレポートのパージ設定

NetScaler Consoleでネットワークレポートデータのパージ間隔を設定できます。この間隔は、NetScaler Consoleサーバーのデータベースに保存されるネットワークレポートデータの量を制限します。デフォルトでは、ネットワークレポートの履歴データは24時間ごと（01:00）にパージされます。

注

指定できる値は、90日を超えることはできず、1日未満にすることはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プロビジョニング

このセクションでは、以下のトピックについて説明します。

- AWSでのアプリベースのプロビジョニング(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/app-based-provisioning-in-aws.html)
- Azureでのアプリベースのプロビジョニング(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/app-based-provisioning-in-azure.html)
- NetScaler VPXインスタンスのプロビジョニング(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-instances.html)
  - AWS(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-aws.html)
  - マイクロソフト アジュール
  - グーグル クラウド
  - VMware ブイセンター
- パブリッククラウド向けNetScalerグローバル負荷分散(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/glb-solution.html)

AWSでのアプリベースのプロビジョニング

NetScaler Console service は、「App based」プロビジョニングを導入しました。これは、クラウドデータセンターでのNetScaler展開を合理化および簡素化し、そこからアプリケーションを配信するように設計されています。

NetScaler Console service は、顧客のクラウド認証情報を受け入れ、NetScaler、エージェント、およびAWS上の必要なクラウドエンティティの起動をオーケストレーションすることで、アプリケーション配信に必要なインフラストラクチャをセットアップします。NetScaler管理者は、NetScalerのライセンスオプションの柔軟性を確保するために、FlexedライセンスとCloud marketplaceライセンスの両方を活用できます。

管理者は、NetScaler Console service から、シンプルでアプリ中心の方法で配信設定を定義することにより、クラウド上でアプリケーションを配信できます。その後、アプリケーションを配信するために、ADCsとAWSインフラストラクチャの両方の構成が行われます。アプリケーションが配信されると、NetScaler管理者はNetScaler Console service の豊富な分析および監視機能にアクセスできるようになり、アプリケーションを効果的に管理および監視できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

AWS Marketplaceで以下の製品を購読してください。

- NetScaler VPX - 以下のいずれかのバリアントを購読してください。
  - NetScaler VPX BYOL - Flexedライセンスを購入済みで、NetScalerインスタンスのライセンス供与のためにNetScaler Console service で利用可能な場合に購読してください。
  - NetScaler VPX Premium - 1000 Mbps AWS Marketplaceからサブスクリプションベースのライセンスが必要な場合に購読してください。
  - NetScalerエージェントサービス
- VPCを選択 - アプリケーション配信のためのインフラストラクチャをセットアップするVPCを選択します。VPCは/22以上のCIDRを持つ必要があります。インフラストラクチャの展開プロセス中に、選択された各アベイラビリティゾーンに対して/24のアドレス空間を消費するADCインフラストラクチャ専用のサブネットが作成されます。展開に基づいてリストからVPCを選択してください。
  - アプリケーションとは別の専用VPC。展開をDMZに似たものにしたい場合。
  - アプリケーションも存在する同じVPC。
- NAT Gateway - 自動プロビジョニングされるConsole agentなどの配信インフラストラクチャは、インターネット経由でNetScaler Console service にアクセスできる必要があります。NATゲートウェイはこのアクセスを提供できます。すでにNATゲートウェイがある場合は、展開時にそれを選択することで、配信インフラストラクチャのために再利用することもできます。NATゲートウェイが選択されていない場合、展開プロセスで作成されます。

クラウドアクセスプロファイル

クラウドアクセスプロファイルは、顧客のAWSアカウントの権限をNetScaler Consoleサービスに付与するために使用されます。クラウドアクセスプロファイルを作成する際に、管理者はAWSでCloudFormationTemplate (CFT) を実行する必要があります。CFTは、顧客のAWSアカウントにIAMロールとポリシーを作成します。

1. **インフラストラクチャ > プロビジョニング > アプリベース > クラウドアクセスプロファイル**に移動します。
2. 画面の指示に従って、サブスクリプションのクラウドアクセスプロファイルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

このプロファイルを作成するには、NetScaler管理者はAWSアカウント管理者でもあり、IAMエンティティを作成するために必要な権限を持っている必要があります。

アプリケーション環境

アプリケーション環境は、アプリケーションを配信するためにVPCに設定された配信インフラストラクチャを表します。管理者がNetScaler Consoleサービスでアプリケーション環境を作成すると、ゲートウェイ、セキュリティグループ、サブネット、NetScalerインスタンス、コンソールエージェントなど、アプリケーションの配信と監視に必要なすべてのリソースがアプリケーション環境の一部として展開されます。詳細については、FAQセクションを参照してください。

1. **InfraStructure > Provisioning > App based > Environments** に移動します。
2. 画面の指示に従って、アプリケーション環境を作成します。

注:

このサービスは、顧客がVPCで作成したリソースに変更を加えることはありません。アプリケーションを配信および監視するために必要なインフラストラクチャのみをプロビジョニングします。

アプリケーション配信

アプリケーション配信は、アプリケーションベースのプロビジョニング機能の主要コンポーネントであり、必須のアプリケーション配信およびセキュリティ情報が含まれています。 アプリケーション配信構成の一部として、次のエンティティを定義します。

- エンドポイントは、プロトコル、ポート、証明書、暗号など、クライアントがアプリケーションにアクセスする方法を表します。たとえば、エンドポイントのSSLプロファイルは、サポートされている暗号とプロトコルを含むSSL構成のセットを表します。事前定義されたA+ SSLプロファイルは、デフォルトで利用可能です。
- アプリケーションのコンポーネントを表すサービス。特定のHTTPリクエストに基づいてアクセスする必要があります。たとえば、eコマースアプリケーションのコンポーネントは、異なるアプリケーションサーバーにインストールされている注文サービス、カタログサービス、または決済サービスである可能性があり、アクセスされたURLに基づいてリクエストをルーティングする必要があります。アプリケーションサービスのサービスプロファイルは、ロードバランシング、SSL、ヘルスチェック設定など、配信インフラストラクチャがアプリケーションサービスにアクセスして監視する方法を表します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 特定のサービスに対するリクエストが到着したときに、L7コンテンツがどのように検査され、変更されるかを定義するコンテンツポリシー。ヘッダー、URL、またはIPアドレスに基づいてHTTPリクエストに対して事前定義されたアクションを実行するために使用されます。アクションには、ヘッダーのエンリッチメント、リクエストのリダイレクト、またはリクエストの破棄などがあります。

1. **InfraStructure > Provisioning > App based > App Delivery** に移動します。
2. 画面の指示に従って、新しいアプリケーションを作成します。

よくある質問

クラウドでアプリケーションを配信するために、NetScaler Consoleサービスによってどのようなエンティティが作成されますか?

NetScaler Consoleサービスは、顧客のVPCに以下のエンティティを作成します。

- 各アベイラビリティゾーンにNetScaler VPXクラスター。
  - VPXインスタンスはEC2 Autoscale™グループとしてデプロイされます。
  - アプリケーション環境の作成中にシングルノードクラスターが作成されます。このクラスターは最大8ノードまでスケールアップできます。
- 各アベイラビリティゾーンにコンソールエージェント。
- サブネット: 管理、クライアント、サーバーネットワーク用にそれぞれ1つのサブネット。
- セキュリティグループ: 管理、クライアント、サーバーNIC用にそれぞれ1つのセキュリティグループ。
  - 管理セキュリティグループ: このセキュリティグループは、NetScalerインスタンスおよびエージェントの管理NICに関連付けられています。NetScalerインスタンス、エージェント、およびその他のコントロールプレーンのトラフィック間の通信を許可するルールで構成されています。
  - クライアントセキュリティグループ: このセキュリティグループは、NetScalerインスタンスのクライアントNICに関連付けられており、NetScaler仮想サーバーへのデータトラフィックを許可するために使用されます。
  - サーバーセキュリティグループ: このセキュリティグループは、NetScalerインスタンスのサーバーNICに関連付けられており、デフォルトのルールは含まれていません。
- ルートテーブル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - クライアントルートテーブル: このルートテーブルは、インターネットへのトラフィックを容易にします。VPCに関連付けられたインターネットゲートウェイにトラフィックを誘導するルートが含まれており、これによりVPC内のリソースがインターネットに接続できるようになります。
  - 管理ルートテーブル: このルートテーブルは、NATゲートウェイによるネットワークアドレス変換 (NAT) のために、NetScalerおよびエージェントから発信されるトラフィックを容易にします。

- 各アベイラビリティゾーンのNATゲートウェイ: NATゲートウェイは、NetScalerおよびコンソールエージェントがインターネットにアクセスできるようにします。

  注:

  VPC内の既存のNATゲートウェイを再利用したい場合、NATゲートウェイは作成されません。

- シークレットマネージャー: シークレットマネージャーは、次の目的で使用されます。
  - NetScaler Consoleサービスにエージェントを登録するために使用されるエージェントトークンとURLを保存します。
  - 認証のためにADCパスワードを保存します。
- Lambda関数
  - ClusterLambdaFunction: このLambda関数は、NetScalerクラスターの作成と管理を担当します。
  - StatsLambdaFunction: このLambda関数は、オートスケーリングに使用されるNetScalerからのメトリクスを収集するために作成されます。

NetScalerをオートスケールするために使用されるメトリクスは何ですか?

NetScalerをオートスケールするために、以下のメトリクスが使用されます。

- オートスケールグループのインスタンスの最小数は1、最大数は8です。
- 1容量単位でスケールアウトします。つまり、 60秒間連続して5期間、cpu_use > 70% または throughput > 70% の場合です。
- 1容量単位でスケールインします。つまり、 60秒間連続して5期間、cpu_use =< 30% かつ throughput =< 30% の場合です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理者は、クラウドでNetScaler Consoleサービスによって作成されたリソースをどのように識別できますか?

すべてのAWSリソースは、デフォルトで「UsedFor: AppDeliveryByNetScaler」というタグで作成されます。さらに、App Environment作成ワークフロー中に指定されたタグを使用してリソースにタグが付けられます。

NetScaler管理者は、App EnvironmentでNetScalerをどのようにアップグレードできますか?

NetScalerをアップグレードするには、次の手順を実行します。

- AWSコンソールから、App Environment用に作成されたオートスケールグループの動的スケーリングを無効にします。命名規則: `Adc-<App Environment Name>-<Availability Zone>-<random alphanumeric string>`

- NetScaler Consoleサービスから、App Environmentの**編集**オプションを使用して、NetScalerがアップグレードされるADCバージョンにAMIの詳細を更新します。

- NetScaler Consoleサービスから、**アップグレードジョブ**機能を使用してADCをアップグレードします。

- AWSコンソールから、オートスケールグループの動的スケーリングを再度有効にします。

Azureでのアプリベースのプロビジョニング

NetScaler Consoleサービスは、「アプリベース」のプロビジョニングを導入しました。これは、クラウドデータセンターでのNetScaler展開を合理化および簡素化し、そこからアプリケーションを配信するように設計されています。

NetScaler Consoleサービスは、顧客のクラウド資格情報を受け入れ、NetScalerインスタンス、NetScaler Consoleエージェント、およびAzure内の必要なクラウドエンティティの起動をオーケストレーションすることで、アプリケーション配信に必要なインフラストラクチャをセットアップします。NetScaler管理者は、NetScalerインスタンスにFlexedライセンスとCloud Marketplaceライセンスの両方を活用でき、ライセンスオプションの柔軟性を確保します。

管理者は、NetScaler Consoleサービスから、シンプルでアプリ中心の方法で配信設定を定義することにより、クラウドに存在するアプリケーションを配信できます。その後、サービスはADCとAzureインフラストラクチャの両方を構成してアプリケーションを配信します。アプリケーション

© 1997–2026 Citrix Systems, Inc. All rights reserved.

が配信されると、NetScaler管理者はNetScaler Consoleサービスの豊富な分析機能と監視機能にアクセスできるようになり、アプリケーションを効果的に管理および監視できます。

Azureでのアプリプロビジョニング(/en-us/netscaler-console-service/media/app-provioning-in-azure.png)

前提条件

Azure Marketplaceで以下の製品のプログラムによる展開を構成します。

- NetScaler VPX - 以下のいずれかのバリアントのプログラムによる展開を構成します。
  - NetScaler VPX BYOL - Flexedライセンスを購入済みで、NetScalerインスタンスのライセンス供与のためにNetScaler Consoleサービスで利用可能な場合は、サブスクライブしてください。
  - NetScaler VPX Premium - 1 Gbps - Azure Marketplaceからサブスクリプションベースのライセンスが必要な場合は、サブスクライブしてください。
  - NetScaler エージェントサービス(https://portal.azure.com/#view/Microsoft_Azure_Marketplace/LegalTermsSkuProgrammaticAccessBlade/legalTermsSkuProgrammaticAccessData~/{"product":{"publisherId":"citrix","offerId":"netscaler_console","planId":"netscaler_agent_service","standardContract
- VNetを選択 - アプリケーション配信用のインフラストラクチャをセットアップするためのVNetを選択します。 VNetは/22以上のCIDRを持つ必要があります。インフラストラクチャ展開プロセス中に、ADCインフラストラクチャ専用のサブネットが作成され、/24のアドレス空間が消費されます。展開に基づいてリストからVNetを選択します。
  - 展開をDMZに似たものにしたい場合は、アプリケーションとは別の専用VNet。
  - アプリケーションも存在する同じVNet。

クラウドアクセスプロファイル

クラウドアクセスプロファイルは、顧客のAzureアカウントの権限をNetScaler Consoleサービスに付与するために使用されます。クラウドアクセスプロファイルを作成する際、管理者はAzure CLIでPowerShellスクリプトをダウンロードして実行する必要があります。このスクリプトは、サブスクリプションレベルで所有者権限を持つサービスプリンシパルを顧客のAzureアカウントに作成します。

1. **インフラストラクチャ > プロビジョニング > アプリベース > クラウドアクセスプロファイル**に移動します。
2. 画面の指示に従って、サブスクリプションのクラウドアクセスプロファイルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

このプロファイルを作成するには、NetScaler管理者がAzureサブスクリプションの所有者である必要があります。

アプリケーション環境

アプリケーション環境は、アプリケーションを配信するためにVNetに設定された配信インフラストラクチャを表します。管理者がNetScaler Consoleサービスでアプリケーション環境を作成すると、ゲートウェイ、セキュリティグループ、サブネット、NetScalerインスタンス、NetScaler Consoleエージェントを含む、アプリケーションの配信と監視のためのすべてのリソースがアプリケーション環境の一部として展開されます。詳細については、FAQセクションを参照してください。

1. **InfraStructure > Provisioning > App based > Environments** に移動します。
2. 画面の指示に従って、アプリケーション環境を作成します。

アプリケーション配信

アプリケーション配信は、アプリケーションベースのプロビジョニング機能の主要コンポーネントであり、必須のアプリケーション配信およびセキュリティ情報を含みます。 アプリケーション配信設定の一部として、次のエンティティを定義します。

- エンドポイントは、プロトコル、ポート、証明書、暗号など、クライアントがアプリケーションにアクセスする方法を表します。たとえば、エンドポイントのSSLプロファイルは、サポートされている暗号とプロトコルを含むSSL構成のセットを表します。事前定義されたA+ SSLプロファイルはデフォルトで利用可能です。
- サービスは、特定のHTTPリクエストに基づいてアクセスする必要があるアプリケーションのコンポーネントを表します。たとえば、eコマースアプリケーションのコンポーネントは、異なるアプリケーションサーバーにインストールされ、アクセスされたURLに基づいてリクエストをルーティングする必要がある注文サービス、カタログサービス、または支払いサービスである可能性があります。アプリケーションサービスのサービスプロファイルは、ロードバランシング、SSL、ヘルスチェック設定など、配信インフラストラクチャがアプリケーションサービスにアクセスして監視する方法を表します。
- コンテンツポリシーは、特定のサービスに対するリクエストまたはレスポンスが到着したときに、L7コンテンツがどのように検査および変更されるかを定義します。これは、ヘッダー、URL、またはIPアドレスに基づいてHTTPリクエストに対して事前定義されたアクションを実行するために使用されます。アクションの一部には、ヘッダーのエンリッチメント、リクエストのリダイレクト、またはリクエストの破棄などがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **InfraStructure > Provisioning > App based > App Delivery** に移動します。
2. 画面の指示に従って、新しいアプリケーションを作成します。

よくある質問

クラウドでアプリケーションを配信するためにNetScaler Consoleサービスによって作成されるエンティティは何ですか?

NetScaler Consoleサービスは、顧客のVNetに以下のエンティティを作成します。

- NetScaler VPXクラスター。
  - VPXインスタンスは、仮想マシン スケール セット (VMSS) として展開されます。
  - App Environmentの作成中に単一ノードクラスターが作成されます。このクラスターは最大10ノードまでスケールアップできます。
- NetScaler Consoleエージェント。
- サブネット: 管理用、クライアント用、サーバー用にそれぞれ1つずつサブネット。
- セキュリティグループ: NetScalerの管理用、クライアント用、サーバー用NICにそれぞれ1つずつセキュリティグループ。
  - 管理セキュリティグループ: このセキュリティグループは、NetScalerインスタンスおよびNetScaler Consoleエージェントの管理NICに関連付けられています。NetScalerインスタンス、NetScaler Consoleエージェント、およびその他のコントロールプレーンのトラフィック間の通信を許可するルールで構成されています。
  - クライアントセキュリティグループ: このセキュリティグループは、NetScalerインスタンスのクライアントNICに関連付けられており、NetScaler仮想サーバーへのデータトラフィックを許可するために使用されます。
  - サーバーセキュリティグループ: このセキュリティグループは、NetScalerインスタンスのサーバーNICに関連付けられており、デフォルトのルールは含まれていません。
- NATゲートウェイ: NATゲートウェイは、NetScaler ConsoleエージェントがNetScaler Consoleサービスにアクセスし、NetScalerインスタンスがインターネットにアクセスできるようにします。
- Azure Key Vault: NetScalerおよびエージェントのシークレットをすべてVaultに保存します。

NetScalerのオートスケールに使用されるメトリックは何ですか?

NetScalerをオートスケールするために、以下のメトリックが使用されます。

- VMSSのインスタンスの最小数は1、最大数は10です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 1容量単位でスケールアウトします。つまり、 cpu_use > 70% または throughput > 70% が60秒間連続して5回発生した場合です。
- 1容量単位でスケールインします。つまり、 cpu_use =< 30% かつ throughput =< 30% が60秒間連続して5回発生した場合です。

管理者は、クラウドでNetScaler Consoleサービスによって作成されたリソースをどのように識別できますか?

すべてのAzureリソースは、デフォルトで「UsedFor: AppDeliveryByNetScaler」というタグで作成されます。さらに、リソースはApp Environment作成ワークフロー中に指定されたタグを使用してタグ付けされます。

NetScaler管理者は、App EnvironmentでNetScalerをどのようにアップグレードできますか?

NetScalerをアップグレードするには、次の手順を実行します。

- Azureコンソールから、App EnvironmentのVMSSの現在のインスタンス数にスケーリングポリシーの値を設定して、VMSSのスケーリングを無効にします。

  命名規則: `vmss-adc-<App Environment Name>`

- NetScaler Consoleサービスから、App Environmentを編集し、アップグレードするバージョンを選択します。

- NetScaler Consoleサービスから、**アップグレードジョブ**機能を使用して、前の手順で選択したバージョンにADCをアップグレードします。

  ADCをアップグレードする(/en-us/netscaler-console-service/media/upgrade-job-in-app-provisioning-aws.png)

- Azure Consoleから、VMSSの動的スケーリングを再度有効にします。インスタンス制限は初期値に設定する必要があります。つまり、minimum=1、maximum=10、default=1です。

NetScaler VPXインスタンスのプロビジョニング

NetScaler Console を使用すると、パブリッククラウドおよび仮想化プラットフォーム全体でNetScaler VPXインスタンスの展開、セットアップ、および管理を自動化できます。NetScaler Console を使用した NetScaler VPXインスタンスのプロビジョニングは、クラウドの弾力性と柔軟性を、NetScaler の最適化、セキュリティ、および制御機能と組み合わせます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console が NetScaler インスタンスを監視することで、アプリケーションの健全性、パフォーマンス、およびセキュリティに関する可視性を得られ、ハイブリッドおよびマルチクラウド環境全体でアプリケーション配信インフラストラクチャを管理できます。

NetScaler VPXインスタンスは、次のプラットフォームでプロビジョニングできます。

- AWS
- マイクロソフト アジュール
- グーグル クラウド
- ヴイエムウェア vCenter

AWS 上での NetScaler VPX インスタンスのプロビジョニング

アプリケーションをクラウドに移行すると、アプリケーションの一部であるコンポーネントが増加し、より分散され、動的に管理する必要が生じます。

AWS 上の NetScaler VPX インスタンスを使用すると、L4-L7 ネットワークスタックを AWS にシームレスに拡張できます。NetScaler VPX を使用すると、AWS はオンプレミス IT インフラストラクチャの自然な拡張となります。AWS 上の NetScaler VPX を使用して、クラウドの弾力性と柔軟性を、世界で最も要求の厳しいウェブサイトやアプリケーションをサポートする最適化、セキュリティ、および制御機能と組み合わせることができます。

NetScaler Console が NetScaler インスタンスを監視することで、アプリケーションの健全性、パフォーマンス、セキュリティに関する可視性を得られます。ハイブリッドマルチクラウド環境全体で、アプリケーション配信インフラストラクチャのセットアップ、展開、および管理を自動化できます。

AWS 用語

以下のセクションでは、このドキュメントで使用されている AWS 用語について簡単に説明します。

用語	定義
Amazon マシンイメージ (AMI)	インスタンス (クラウド内の仮想サーバー) を起動するために必要な情報を提供するマシンイメージ。
エラスティック コンピュート クラウド (EC2)	クラウドで安全かつサイズ変更可能なコンピューティング容量を提供するウェブサービス。開発者にとってウェブスケールのクラウ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用語	定義
	ドコンピューティングを容易にすることを目的としています。
エラスティック ネットワーク インターフェース (ENI)	VPC 内のインスタンスにアタッチできる仮想ネットワークインターフェイス。
インスタンスタイプ	Amazon EC2は、さまざまなユースケースに合わせて最適化された幅広いインスタンスタイプを提供します。インスタンスタイプは、CPU、メモリ、ストレージ、ネットワーク容量のさまざまな組み合わせで構成されており、アプリケーションに適したリソースの組み合わせを柔軟に選択できます。
ID およびアクセス管理 (IAM) ロール	AWS内でそのIDができることとできないことを決定するアクセス許可ポリシーを持つAWS ID。IAMロールを使用すると、EC2インスタンスで実行されているアプリケーションがAWSリソースに安全にアクセスできるようになります。
セキュリティグループ	インスタンスに対する、許可されたインバウンドネットワーク接続の名前付きセット。
サブネット	EC2インスタンスをアタッチできるVPCのIPアドレス範囲のセグメント。サブネットを作成して、セキュリティおよび運用上のニーズに応じてインスタンスをグループ化できます。

前提条件

このドキュメントでは、以下を前提としています。

- AWSアカウントを所有していること。
- 必要なVPCを作成し、アベイラビリティゾーンを選択していること。
- AWSにエージェントを追加していること。

アカウントの作成方法やその他のタスクの詳細については、AWS Documentationを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AWS にエージェントをインストールする方法の詳細については、「AWS に NetScaler エージェントをインストールする」を参照してください。

アーキテクチャ図

次の図は、NetScaler Console が AWS と連携して AWS に NetScaler VPX インスタンスをプロビジョニングする仕組みの概要を示しています。

構成タスク

NetScaler Console で NetScaler VPX インスタンスをプロビジョニングする前に、AWS で次のタスクを実行します。

- サブネットを作成する
- セキュリティグループを作成する
- IAM ロールを作成し、ポリシーを定義する

AWS にインスタンスをプロビジョニングするには、NetScaler Console で次のタスクを実行します。

- サイトを作成する
- AWS に NetScaler VPX インスタンスをプロビジョニングする

サブネットを作成するには

VPC に 3 つのサブネットを作成します。VPC に NetScaler VPX インスタンスをプロビジョニングするために必要な 3 つのサブネットは、管理、クライアント、サーバーです。各サブネットについて、VPC で定義されている範囲から IPv4 CIDR ブロックを指定します。サブネットを配置するアベイラビリティゾーンを指定します。3 つすべてのサブネットを同じアベイラビリティゾーンに作成します。次の図は、リージョンに作成された 3 つのサブネットと、クライアントシステムへの接続を示しています。

VPCとサブネットの詳細については、「VPCs and Subnets」を参照してください。

セキュリティグループを作成するには

NetScaler VPXインスタンスのインバウンドおよびアウトバウンドトラフィックを制御するためのセキュリティグループを作成します。セキュリティグループは、インスタンスの仮想ファイアウォールとして機能します。セキュリティグループは、サブネットレベルではなく、インスタンスレベルで作成します。VPC内のサブネットにある各インスタンスに、異なるセキュリティグループのセットを割り当てることができます。各セキュリティグループにルールを追加して、クライアントサブネットを介してインスタンスに渡されるインバウンドトラフィックを制御します。また、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サーバーサブネットを介してアプリケーションサーバーに渡されるアウトバウンドトラフィックを制御する別のルールセットを追加することもできます。インスタンスにデフォルトのセキュリティグループを使用することもできますが、独自のグループを作成することをお勧めします。3つのセキュリティグループを作成します。各サブネットに1つずつです。制御したいインバウンドトラフィックとアウトバウンドトラフィックの両方のルールを作成します。必要なだけルールを追加できます。

セキュリティグループの詳細については、「Security Groups for your VPC」を参照してください。

IAMロールを作成し、ポリシーを定義するには

IAMロールを作成して、ユーザーとCitrixが信頼するAWSアカウントとの間に信頼関係を確立し、Citrixのアクセス許可を持つポリシーを作成できるようにします。

1. AWSで、**サービス**をクリックします。左側のナビゲーションペインで、**IAM > ロール**を選択し、**ロールの作成**をクリックします。
2. AWSアカウントをNetScaler ConsoleのAWSアカウントに接続します。そのため、NetScaler ConsoleがAWSアカウントでアクションを実行できるように、**別のAWSアカウント**を選択します。

   12桁のNetScaler Console AWSアカウントIDを入力します。Citrix IDは835822366011です。クラウドアクセスプロファイルを作成する際に、NetScaler ConsoleでCitrix IDを見つけることもできます。

   ☐
3. サードパーティアカウントに接続するには、**外部IDが必要**を有効にします。オプションの外部識別子を要求することで、ロールのセキュリティを強化できます。任意の文字の組み合わせであるIDを入力します。
4. **アクセス許可**をクリックします。
5. **アクセス許可ポリシーのアタッチ**ページで、**ポリシーの作成**をクリックします。
6. ビジュアルエディターまたはJSONを使用してポリシーを作成および編集できます。

   Citrixからのアクセス許可のリストを次のボックスに示します。

```
{

"Version": "2012-10-17",

"Statement":
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
[
    {
         "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeImageAttribute",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeRegions",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeHosts",
            "ec2:DescribeImages",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeAddresses",
            "ec2:DescribeKeyPairs",
            "ec2:DescribeTags",
            "ec2:DescribeVolumeStatus",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:DescribeVolumes",
            "ec2:DescribeVolumeAttribute",
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:CreateKeyPair",
            "ec2:DeleteKeyPair",
            "ec2:ResetInstanceAttribute",
            "ec2:RunScheduledInstances",
            "ec2:ReportInstanceStatus",
            "ec2:StartInstances",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:UnmonitorInstances",
            "ec2:MonitorInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:AssignPrivateIpAddresses",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:CreateNetworkInterface",
            "ec2:AttachNetworkInterface",
            "ec2:DetachNetworkInterface",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:DeleteNetworkInterface",
            "ec2:ResetNetworkInterfaceAttribute",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:AssociateAddress",
            "ec2:AllocateAddress",
            "ec2:ReleaseAddress",
            "ec2:DisassociateAddress",
            "ec2:GetConsoleOutput"
        ],
            "Resource": "*"
    }
]
}
```

7. JSONタブで権限のリストをコピーして貼り付け、**ポリシーの確認**をクリックします。
8. **ポリシーの確認**ページで、ポリシーの名前を入力し、説明を入力して、**ポリシーの作成**をクリックします。

NETSCALER CONSOLEでサイトを作成するには

NetScaler Consoleでサイトを作成し、AWSロールに関連付けられているVPCの詳細を追加します。

1. NetScaler Consoleで、**インフラストラクチャ > サイト**に移動します。
2. **追加**をクリックします。
3. サービスタイプとしてAWSを選択し、**既存のVPCをサイトとして使用**を有効にします。
4. クラウドアクセスプロファイルを選択します。
5. フィールドにクラウドアクセスプロファイルが存在しない場合は、**追加**をクリックしてプロファイルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **クラウドアクセスプロファイルの作成**ページで、AWSにアクセスするために使用するプロファイルの名前を入力します。
b. AWSで作成したロールに関連付けられているARNを入力します。
c. AWSでIdentity and Access Management (IAM) ロールを作成する際に指定した外部IDを入力します。「IAMロールを作成してポリシーを定義する」タスクのステップ4を参照してください。AWSで指定したIAMロール名が「Citrix-ADM-」で始まり、ロールARNに正しく表示されていることを確認してください。

AWSのサイトを作成する(/en-us/netscaler-console-service/media/aws-provisioning-vpx-standalone-4-new.png)

AWSのIAMロールに関連付けられているVPCの詳細（リージョン、VPC ID、名前、CIDRブロックなど）がNetScaler Consoleにインポートされます。

6. サイトの名前を入力します。
7. **作成**をクリックします。

AWSでNETSCALER VPXをプロビジョニングするには

以前に作成したサイトを使用して、AWSでNetScaler VPXインスタンスをプロビジョニングします。エージェントの詳細を指定して、そのエージェントにバインドされているインスタンスをプロビジョニングします。

1. NetScaler Consoleで、**Infrastructure > Instances > 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、**Provision NetScaler VPX on Cloud**ページが表示されます。

3. **Amazon Web Services (AWS)**を選択し、**次へ**をクリックします。
4. **基本パラメータ**タブで、,

a. リストから**インスタンスの種類**を選択します。

- **スタンドアロン:** このオプションは、AWSにスタンドアロンのNetScaler VPXインスタンスをプロビジョニングします。
- **HA:** このオプションは、AWSに高可用性NetScaler VPXインスタンスをプロビジョニングします。

同じゾーンにNetScaler VPXインスタンスをプロビジョニングするには、**ゾーンタイプ**で**シングルゾーン**オプションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

複数のゾーンにNetScaler VPXインスタンスをプロビジョニングするには、**ゾーンタイプ**で**マルチゾーン**オプションを選択します。**プロビジョニングパラメータ**タブで、AWSで作成された各ゾーンのネットワーク詳細を必ず指定してください。

高可用性NetScaler VPXインスタンス(/en-us/netscaler-console-service/media/ha-provisioning-on-cloud.png)

b. NetScaler VPXインスタンスの名前を指定します。

c. 「**サイト**」で、以前に作成したサイトを選択します。

d. 「**エージェント**」で、NetScaler VPXインスタンスを管理するために作成されたエージェントを選択します。

e. 「**クラウドアクセスプロファイル**」で、サイト作成時に作成されたクラウドアクセスプロファイルを選択します。

f. 「**デバイスプロファイル**」で、認証を提供するプロファイルを選択します。

NetScaler Consoleは、NetScaler VPXインスタンスにログオンする必要がある場合にデバイスプロファイルを使用します。

g. 「**次へ**」をクリックします。

5. 「**ライセンス**」タブで、NetScalerインスタンスにライセンスを適用するための次のいずれかのモードを選択します。

- **NetScaler Consoleを使用**: プロビジョニングするインスタンスは、NetScaler Consoleからライセンスをチェックアウトします。
- **AWS Cloudを使用**: 「**クラウドから割り当て**」オプションは、AWS Marketplaceで利用可能なNetScaler®製品ライセンスを使用します。プロビジョニングするインスタンスは、Marketplaceからライセンスを使用します。

  AWS Marketplaceからライセンスを使用することを選択した場合は、「**プロビジョニングパラメータ**」タブで製品またはライセンスを指定します。

詳細については、「ライセンス要件」を参照してください。

6. 「**ライセンス**」タブで「**NetScaler Consoleから割り当て**」を選択した場合は、以下を指定します。

- ライセンスの種類 - 帯域幅ライセンスまたは仮想CPUライセンスのいずれかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

帯域幅ライセンス: 「**帯域幅ライセンスの種類**」リストから、次のいずれかのオプションを選択できます。

- **プールされたキャパシティ:** インスタンスに割り当てるキャパシティを指定します。

  共通プールから、NetScalerインスタンスは1つのインスタンスライセンスをチェックアウトし、指定された帯域幅のみを使用します。
- **VPXライセンス:** NetScaler VPXインスタンスがプロビジョニングされると、インスタンスはNetScaler Consoleからライセンスをチェックアウトします。

仮想CPUライセンス: プロビジョニングされたNetScaler VPXインスタンスは、インスタンスで実行されているCPUの数に応じてライセンスをチェックアウトします。

注

プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスはNetScaler Consoleのライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用できます。

a. **ライセンスエディション**で、ライセンスエディションを選択します。NetScaler Consoleは、指定されたエディションを使用してインスタンスをプロビジョニングします。

7. **次へ**をクリックします。
8. **プロビジョニングパラメータ**タブで、,

   a. AWSで作成した**Citrix IAMロール**を選択します。IAMロールは、AWS内でそのIDができることとできないことを決定する権限ポリシーを持つAWS IDです。
   b. **製品**フィールドで、プロビジョニングするNetScaler製品バージョンを選択します。
   c. **インスタンスタイプ**リストからEC2インスタンスタイプを選択します。

      このリストには、選択したNetScalerインスタンスでサポートされているAMIインスタンスタイプが表示されます。
   d. プロビジョニングするNetScalerの**バージョン**を選択します。NetScalerの**メジャー**バージョンと**マイナー**バージョンの両方を選択します。
   e. **セキュリティグループ**で、仮想ネットワークで作成した管理、クライアント、およびサーバーのセキュリティグループを選択します。
   f. 「**ノードごとのサーバーサブネット内のIP**」で、セキュリティグループのノードごとのサーバーサブネット内のIPアドレス数を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. 「**サブネット**」で、AWSで作成された各ゾーンの管理、クライアント、サーバーサブネットを選択します。「**アベイラビリティゾーン**」リストからリージョンを選択することもできます。

h. 「**完了**」をクリックします。

NetScaler VPXインスタンスがAWSにプロビジョニングされました。

注

現在、NetScaler ConsoleはAWSからのNetScalerインスタンスのプロビジョニング解除をサポートしていません。

AWSでプロビジョニングされたNETSCALER VPXを表示するには

1. AWSのホームページから、「**サービス**」に移動し、「**EC2**」をクリックします。
2. 「**リソース**」ページで、「**実行中のインスタンス**」をクリックします。
3. AWSでプロビジョニングされたNetScaler VPXを表示できます。

NetScaler VPXインスタンスの名前は、NetScaler Consoleでインスタンスをプロビジョニングする際に指定したものと同じです。

NETSCALER CONSOLEでプロビジョニングされたNETSCALER VPXを表示するには

1. NetScaler Consoleで、「**インフラストラクチャ > インスタンス > NetScaler**」に移動します。
2. 「**NetScaler VPX**」タブを選択します。
3. AWSでプロビジョニングされたNetScaler VPXインスタンスがここに表示されます。

Microsoft Azure 上での NetScaler VPX インスタンスのプロビジョニング

Azure でホストされるアプリケーションやサービスは、クラウドの利点とともに、安全なトラフィック管理とネットワークリソースの効率的な最適化を必要とします。Microsoft Azure 上にプロビジョニングされた NetScaler VPX インスタンスは、安全なトラフィック管理、最適化されたリソース消費、およびウェブアプリケーションの所有コストの削減を提供します。

NetScaler Console を使用すると、Azure 上での NetScaler VPX インスタンスの展開、セットアップ、および管理を自動化できます。NetScaler Console を使用して NetScaler VPX インスタンスをプロビジョニングすることで、クラウドの弾力性と柔軟性が NetScaler の制御機能と組み合わされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console の展開アーキテクチャ

次の画像は、NetScaler Console が Azure とどのように接続して Microsoft Azure に NetScaler VPX インスタンスをプロビジョニングするかの概要を示しています。

NetScaler Console の展開アーキテクチャ (/en-us/netscaler-console-service/media/citrix-adm-deployment-provisioning-architecture.png)

Microsoft Azure で NetScaler VPX インスタンスをプロビジョニングおよび管理するには、3つのサブネットが必要です。各サブネットにはセキュリティグループを作成する必要があります。NetScaler Gateway で指定されたルールが、サブネット間の通信を管理します。

エージェントは、NetScaler VPX インスタンスのプロビジョニングと管理を支援します。

前提条件

このセクションでは、NetScaler VPX インスタンスをプロビジョニングする前に、Microsoft Azure および NetScaler Console で完了する必要がある前提条件について説明します。

このドキュメントでは、以下を前提としています。

- Azure Resource Manager 展開モデルをサポートする Microsoft Azure アカウントを所有していること。
- Microsoft Azure にリソースグループがあること。

アカウントの作成方法やその他のタスクの詳細については、Microsoft Azure Documentation を参照してください。

MICROSOFT AZURE コンポーネントのセットアップ

NetScaler ConsoleでNetScaler VPXインスタンスをプロビジョニングする前に、Azureで次のタスクを実行します。

1. 仮想ネットワークを作成する。
2. セキュリティグループを作成する。
3. サブネットを作成する。
4. Microsoft AzureでNetScaler VPXライセンスを購読する。
5. アプリケーションを作成して登録する。
6. エージェントをセットアップする。

仮想ネットワークを作成する

1. Microsoft Azureポータルにログオンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **リソースの作成**を選択します。
3. **ネットワーク**を選択し、**仮想ネットワーク**をクリックします。
4. 必要なパラメーターを指定します。

    - **リソースグループ**で、NetScaler VPX製品をデプロイするリソースグループを指定する必要があります。
    - **場所**で、次のような可用性ゾーンをサポートする場所を指定する必要があります。

        - 米国中部
        - 米国東部2
        - フランス中部
        - 北ヨーロッパ
        - 東南アジア
        - 西ヨーロッパ
        - 米国西部2

    注

    このリソースグループに存在するアプリケーションサーバー。

5. **作成**をクリックします。

詳細については、Microsoft Documentationの「Azure Virtual Network」を参照してください。
セキュリティグループを作成する
仮想ネットワーク (VNet) に3つのセキュリティグループを作成します。それぞれ管理用、クライアント用、サーバー接続用です。NetScaler VPXインスタンスのインバウンドおよびアウトバウンドトラフィックを制御するセキュリティグループを作成します。ルールは必要なだけ追加できます。

- **管理:** NetScaler VPXの管理専用のアカウント内のセキュリティグループ。NetScalerはAzureサービスに接続する必要があり、インターネットアクセスが必要です。インバウンドルールは、以下のTCPおよびUDPポートで許可されます。

    - TCP: 80, 22, 443, 3008–3011, 4001
    - UDP: 67, 123, 161, 500, 3003, 4500, 7000

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注**
>
> セキュリティグループがエージェントによるVPXへのアクセスを許可していることを確認してください。

- **クライアント:** NetScaler VPXインスタンスのクライアント側通信専用のアカウント内のセキュリティグループ。通常、インバウンドルールはTCPポート80、22、443で許可されます。
- **サーバー:** NetScaler VPXのサーバー側通信専用のアカウント内のセキュリティグループ。

Microsoft Azureでセキュリティグループを作成する方法の詳細については、「ネットワークセキュリティグループの作成、変更、または削除」を参照してください。

サブネットの作成

仮想ネットワーク (VNet) に3つのサブネットを作成します。それぞれ管理、クライアント、サーバー接続用です。各サブネットには、VNetで定義されているアドレス範囲を指定します。サブネットを配置するアベイラビリティゾーンを指定します。

- **管理:** 管理専用の仮想ネットワーク (VNet) 内のサブネット。NetScalerはAzureサービスに接続する必要があり、インターネットアクセスが必要です。
- **クライアント:** クライアント側専用の仮想ネットワーク (VNet) 内のサブネット。通常、NetScalerはインターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。
- **サーバー:** アプリケーションサーバーがプロビジョニングされるサブネット。すべてのアプリケーションサーバーはこのサブネットに存在し、このサブネットを介してNetScalerからアプリケーショントラフィックを受信します。

> **注**
>
> サブネットの作成時に、適切なセキュリティグループをサブネットに指定してください。

Microsoft Azureでサブネットを作成する方法の詳細については、「仮想ネットワークサブネットの追加、変更、または削除」を参照してください。

Microsoft AzureでNetScaler VPXライセンスをサブスクライブする

1. Microsoft Azureポータルにログオンします。
2. 「**リソースの作成**」を選択します。
3. 「**マーケットプレイスの検索**」バーで、`NetScaler` を検索し、必要な製品バージョンを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**ソフトウェアプランの選択**」リストで、次のいずれかのライセンスタイプを選択します。
   - 独自のライセンスを使用
   - アドバンスト
   - プレミアム

   注

   - 「**独自のライセンスを使用**」オプションを選択した場合、プロビジョニングするインスタンスは、NetScaler インスタンスのプロビジョニング中に NetScaler Console からライセンスをチェックアウトします。
   - NetScaler Console では、「**Advanced**」と「**Premium**」は、それぞれ「**Enterprise**」と「**Platinum**」に相当するライセンスタイプです。

5. 選択したNetScaler製品でプログラムによる展開が有効になっていることを確認してください。
   a. 「**プログラムで展開しますか？**」の横にある「**開始する**」をクリックします。

      NetScaler VPX をプログラムで展開(/en-us/netscaler-console-service/media/select-software-plan-azure.png)

   b. 「**サブスクリプションの選択**」で、「**有効にする**」を選択して、選択したNetScaler VPXエディションをプログラムで展開します。

      プログラムによる展開を有効にする(/en-us/netscaler-console-service/media/subscription.png)

      重要

      プログラムによるデプロイを有効にすることは、Azure で NetScaler VPX インスタンスをプロビジョニングするために必要です。

   c. 「**保存**」をクリックします。
   d. 「**プログラムによるデプロイの構成**」を閉じます。

6. 「**作成**」をクリックします。

アプリケーションの作成と登録

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console は、このアプリケーションを使用して Azure で NetScaler VPX インスタンスをプロビジョニングします。

Azure でアプリケーションを作成して登録するには：

1. Azure ポータルで、「**Azure Active Directory**」を選択します。 このオプションには、組織のディレクトリが表示されます。
2. 「**アプリの登録**」を選択します。
   a. 「**名前**」に、アプリケーションの名前を指定します。
   b. リストから「**アプリケーションの種類**」を選択します。
   c. 「**サインオン**」URL に、アプリケーションにアクセスするためのアプリケーション URL を指定します。
3. 「**作成**」をクリックします。

アプリの登録の詳細については、Microsoft ドキュメントを参照してください。

Azure はアプリケーションにアプリケーション ID を割り当てます。以下は、Microsoft Azure に登録されているアプリケーションの例です。

NetScaler VPX 用の Microsoft Azure に登録されたアプリケーション(/en-us/netscaler-console-service/media/app-registration.png)

以下のIDをコピーし、NetScaler Consoleでクラウドアクセスプロファイルを構成する際にこれらのIDを指定してください。

- **アプリケーションID:** アプリケーションまたはクライアントIDを取得する手順。
- **ディレクトリID:** ディレクトリ、テナント、またはオブジェクトIDを取得する手順。
- **キー:** キー値またはクライアントシークレットIDを取得する手順。

  登録済みアプリケーションのクライアントシークレットキー(/en-us/netscaler-console-service/media/key.png)
- **サブスクリプションID:** ストレージアカウントからサブスクリプションIDをコピーします。

詳細については、Microsoft ドキュメントを参照してください。
アプリケーションにロール権限を割り当てる
NetScaler Consoleは、サービスとしてのアプリケーションの原則を使用して、Microsoft AzureにNetScalerインスタンスをプロビジョニングします。この権限は、選択されたリソースグループにのみ適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

登録済みアプリケーションにロール権限を割り当てるには、Microsoft Azureサブスクリプションの所有者である必要があります。

1. Azureポータルで、**リソースグループ**を選択します。
2. ロール権限を割り当てるリソースグループを選択します。
3. **アクセス制御 (IAM)** を選択します。
4. **ロールの割り当て**で、**追加**をクリックします。
5. 「**Role**」リストから「**Owner**」を選択します。
6. NetScalerインスタンスのプロビジョニング用に登録されているアプリケーションを選択します。「アプリケーションの作成と登録」を参照してください。
7. 「**Save**」をクリックします。

NetScalerエージェントをセットアップする

管理サブネットにエージェントをインストールします。このエージェントは、NetScaler ConsoleとMicrosoft Azure内の管理対象インスタンスとの間の仲介役として機能します。Microsoft Azureにエージェントをインストールする方法の詳細については、「Microsoft AzureクラウドにNetScalerエージェントをインストールする」を参照してください。

NETSCALER CONSOLEコンポーネントをセットアップする

NetScaler ConsoleでNetScaler VPXインスタンスをプロビジョニングする前に、Azureで次のタスクを実行します。

1. サイトを作成する。
2. サイトをCitrixサービスエージェントにアタッチする。

NetScaler Consoleでサイトを作成する

NetScaler Consoleでサイトを作成し、Microsoft Azureリソースグループに関連付けられているVNetの詳細を追加します。

1. NetScaler Consoleで、「**Infrastructure > Instances > Sites**」に移動します。
2. 「**Add**」をクリックします。
3. 「**Select Cloud**」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「**Azure**」を選択します。
   c. 「**AzureからVNetをフェッチ**」チェックボックスをオンにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このオプションを使用すると、Microsoft Azureアカウントから既存のVNet情報を取得できます。

d. 「**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**」で、Microsoft Azureアカウント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**」をクリックします。

c. 「**名前**」で、NetScaler ConsoleでAzureアカウントを識別するための名前を指定します。

d. 「**テナントActive Directory ID / テナントID**」で、Microsoft Azureのテナントまたはアカウントの Active Directory IDを指定します。

e. 「**サブスクリプションID**」を指定します。

f. 「**アプリケーションID/クライアントID**」を指定します。

g. 「**アプリケーションキーパスワード/シークレット**」を指定します。

h. 「**作成**」をクリックします。

詳細については、アプリケーションの作成と登録およびクラウドアクセスプロファイルをAzureアプリケーションにマッピングするを参照してください。

i. **VNet**で、管理するNetScaler VPXインスタンスを含む仮想ネットワークを選択します。

j. **サイト名**を指定します。

k. **完了**をクリックします。

クラウドアクセスプロファイルをAzureアプリケーションにマッピングする

NETSCALER CONSOLEの用語	MICROSOFT AZUREの用語
テナントActive Directory ID / テナントID	ディレクトリID
サブスクリプションID	サブスクリプションID
アプリケーションID/クライアントID	アプリケーションID
アプリケーションキーパスワード / シークレット	キーまたは証明書またはクライアントシークレット

サイトをエージェントにアタッチする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Consoleで、**Infrastructure > Instances > Agents** に移動します。
2. サイトをアタッチするエージェントを選択します。
3. **Attach Site** をクリックします。
4. アタッチするサイトをリストから選択します。
5. **Save** をクリックします。

構成タスク

Microsoft Azureリソースグループ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。そのエージェントにバインドされているインスタンスをプロビジョニングするために、エージェントの詳細を指定します。

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler** に移動します。
2. **VPX** タブで、**Provision** をクリックします。

   このオプションにより、**Provision NetScaler VPX on Cloud** ページが表示されます。
3. **Microsoft Azure** を選択し、**Next** をクリックします。インスタンスをプロビジョニングするために必要なパラメータを指定します。

基本パラメータの構成

1. **Basic Parameters** タブで、以下を指定します。

   - **Type of Instance**: リストから以下のいずれかのオプションを選択します。

     - **Standalone** - このオプションは、Microsoft Azure上にスタンドアロンのNetScaler VPXインスタンスをプロビジョニングします。
     - **HA:** このオプションは、Microsoft Azure上に高可用性NetScaler VPXインスタンスをプロビジョニングします。

       同じゾーンにNetScaler VPXインスタンスをプロビジョニングするには、「**Zone Type**」の下にある「**Single Zone**」オプションを選択します。

       複数のゾーンにNetScaler VPXインスタンスをプロビジョニングするには、「**Zone type**」の下にある「**Multi Zone**」オプションを選択します。「**Cloud Parameters**」タブで、Microsoft Azure上に作成された各ゾーンのネットワーク詳細を必ず指定してください。

       高可用性NetScaler VPXインスタンス(/en-us/netscaler-console-service/media/ha-provisioning-on-cloud.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Name** - NetScaler VPXインスタンスの名前を指定します。
- **Site** - 以前に作成したサイトを選択します。
- **Agent** - NetScaler VPXインスタンスを管理するために作成されたエージェントを選択します。
- **Cloud Access Profile** - サイト作成時に作成されたクラウドアクセスプロファイルを選択します。
- **NetScaler Profile** - 認証を提供するためのプロファイルを選択します。

  NetScaler Consoleは、NetScaler VPXインスタンスにログオンする必要がある場合にデバイスプロファイルを使用します。

  注

  選択したデバイスプロファイルがMicrosoft Azureのパスワードルールに準拠していることを確認してください。

2. 「**Next**」をクリックします。

NetScaler VPXの基本パラメータのプロビジョニング(/en-us/netscaler-console-service/media/provision-citrix-adc-basic-parameters.png)

ライセンスを設定する

NetScalerインスタンスにライセンスを適用するには、次のいずれかのモードを選択します。

- **NetScaler Consoleを使用する**: プロビジョニングするインスタンスは、NetScaler Consoleからライセンスをチェックアウトします。
- **Microsoft Azureを使用する**: **クラウドから割り当てる**オプションは、Azure Marketplaceで利用可能なNetScaler®製品ライセンスを使用します。プロビジョニングするインスタンスは、マーケットプレイスからライセンスを使用します。

  Azure Marketplaceからライセンスを使用することを選択した場合は、**プロビジョニングパラメータ**タブで製品またはライセンスを指定します。

詳細については、「ライセンス要件」を参照してください。

NETSCALER CONSOLEからライセンスを使用する

このオプションを使用するには、Azureで**Bring your own license**ソフトウェアプランを使用してNetScaler製品を購読していることを確認してください。「Microsoft AzureでNetScaler VPXライセンスを購読する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **ライセンス**タブで、**NetScaler Consoleから割り当てる**を選択します。
2. **ライセンスタイプ**で、リストから次のいずれかのオプションを選択します。
   - **帯域幅ライセンス: 帯域幅ライセンスタイプ**リストから、次のいずれかのオプションを選択できます。
     - **プールされた容量:** インスタンスに割り当てる容量を指定します。

       共通プールから、NetScalerインスタンスは1つのインスタンスライセンスと、指定された帯域幅のみをチェックアウトします。
     - **VPXライセンス:** NetScaler VPXインスタンスがプロビジョニングされると、インスタンスはNetScaler Consoleからライセンスをチェックアウトします。
   - **仮想CPUライセンス:** プロビジョニングされたNetScaler VPXインスタンスは、インスタンスで実行されているCPUの数に応じてライセンスをチェックアウトします。

   注記

   プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスはNetScaler Consoleライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用できます。
3. 「**ライセンスエディション**」で、ライセンスエディションを選択します。NetScaler Consoleは、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. 「**次へ**」をクリックします。

プロビジョニングパラメータを設定する

1. 「**プロビジョニングパラメータ**」タブで、以下を指定します。
   a. NetScaler VPXインスタンスをプロビジョニングする「**リソースグループ**」を選択します。
   b. リストからサポートされている「**VMサイズ**」を選択します。

   注記

   このリストには、選択したNetScaler製品でサポートされているVMサイズが表示されます。

   c. NetScalerのクラウドアクセスプロファイルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. プロビジョニングするNetScalerの「**バージョン**」を選択します。NetScalerの「**メジャー**」バージョンと「**マイナー**」バージョンの両方を選択します。

e. 「**セキュリティグループ**」で、仮想ネットワークで作成した管理、クライアント、およびサーバーのセキュリティグループを選択します。

f. 「**サブネット**」で、Azureで必要な数の可用性ゾーンを指定します。

g. 「**サブネット**」で、仮想ネットワークで作成した管理、クライアント、およびサーバーのサブネットを選択します。

h. 「**完了**」をクリックします。

NetScaler VPX の基本パラメータのプロビジョニング(/en-us/netscaler-console-service/media/provision-citrix-adc-provision-parameters.png)

NetScaler VPX インスタンスが Microsoft Azure にプロビジョニングされました。

プロビジョニングされた NetScaler VPX インスタンスを表示する

NetScaler Console で表示するには：

1. NetScaler Console で、**インフラストラクチャ > インスタンス > NetScaler** に移動します。
2. **NetScaler VPX** タブを選択します。

Microsoft Azure でプロビジョニングされた NetScaler VPX インスタンスがここに表示されます。

Microsoft Azure で表示するには：

1. Azure ポータルにログオンします。
2. NetScaler VPX インスタンスをプロビジョニングするために作成されたリソースグループに移動します。

このページには、プロビジョニングされた NetScaler VPX インスタンスが表示されます。

注

NetScaler VPX インスタンスの名前は、NetScaler Console でインスタンスをプロビジョニングする際に指定したものと同じです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Cloud で NetScaler VPX インスタンスをプロビジョニングする

Google Cloud でホストされているアプリケーションまたはサービスは、クラウドの利点とともに、安全なトラフィック管理とネットワークリソースの効率的な最適化を必要とします。Google Cloud にプロビジョニングされた NetScaler VPX インスタンスは、安全なトラフィック管理、最適化されたリソース消費、およびウェブアプリケーションの所有コストの削減を提供します。

NetScaler Console を使用すると、Google Cloud 上の NetScaler VPX インスタンスの展開、セットアップ、および管理を自動化できます。NetScaler Console を使用して NetScaler VPX インスタンスをプロビジョニングすることで、クラウドの弾力性と柔軟性が NetScaler の制御機能と組み合わされます。

NetScaler Console の展開アーキテクチャ

次の画像は、NetScaler Console が Google Cloud と連携して Google Cloud に NetScaler VPX インスタンスをプロビジョニングする方法の概要を示しています。

NetScaler Console の展開アーキテクチャ (/en-us/netscaler-console-service/media/citrix-adm-deployment-provisioning-architecture-google-cloud.png)

Google Cloud で NetScaler VPX インスタンスをプロビジョニングおよび管理するには、3 つの Virtual Private Cloud (VPC) ネットワークが必要です。VPC ネットワークには、サブネットとファイアウォールが含まれます。ファイアウォールには、サブネットへの受信および送信トラフィックを管理するルールがあります。

エージェントは、NetScaler VPX インスタンスのプロビジョニングと管理を支援します。

前提条件

このセクションでは、NetScaler VPX インスタンスをプロビジョニングする前に Google Cloud および NetScaler Console で完了する必要がある前提条件について説明します。

このドキュメントは、Google Cloud アカウントをお持ちであることを前提としています。アカウントの作成方法の詳細については、Google Cloud Documentation を参照してください。

GOOGLE CLOUD コンポーネントのセットアップ

NetScaler Console で NetScaler VPX インスタンスをプロビジョニングする前に、Google Cloud で次のタスクを実行します。

1. API を有効にする
2. サービスアカウントを作成する
3. VPCネットワークを作成する
4. ファイアウォールを作成する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Google CloudでNetScaler VPXライセンスをサブスクライブする

APIを有効にする

NetScaler Consoleは、Google Cloudで必要なリソースを展開およびプロビジョニングするためにプログラムによるアクセスを必要とします。そのため、Google Cloudプロジェクトで以下のAPIを有効にしてください。

- コンピュート エンジン API
- クラウド DNS API

Google CloudでAPIを有効にする方法の詳細については、「APIの有効化」を参照してください。

サービスアカウントを作成する

NetScaler Consoleは、Google Cloudリソースにアクセスするためにサービスアカウントを使用します。サービスアカウントを作成するには、次の手順を実行します。

1. Google Cloudアカウントにログインします。
2. **IAMと管理 > サービスアカウント**に移動します。
3. **+サービスアカウントを作成**をクリックします。

   2つのサービスアカウントを作成します。1つはNetScaler Console用、もう1つはNetScalerインスタンス用です。サービスアカウントを作成するには、次の手順を実行します。

   a. 名前、ID、説明を指定し、「作成」をクリックします。

   b. 以下の事前定義されたロールを割り当てます。

   - NetScaler Console に必要な IAM ロール

     ```
     roles/iam.serviceAccountUser

     roles/compute.instanceAdmin.v1

     roles/compute.networkAdmin

     roles/dns.admin
     ```

   - NetScaler Console によって作成される NetScaler インスタンスに必要な IAM ロール:

     ```
     roles/compute.instanceAdmin.v1

     roles/compute.networkAdmin
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これらのロールにより、サービスアカウントは Google Cloud リソースにアクセスできます。

c. **完了**をクリックします。

VPC ネットワークを作成する
VPC ネットワークに 3 つのサブネットを作成します。それぞれ管理、クライアント、サーバー接続用です。カスタムオプションを選択してサブネットを作成します。各サブネットのアドレス範囲を指定します。サブネットを配置するリージョンを指定します。

- **管理**: 管理専用の管理 VPC ネットワーク内のサブネット。NetScaler は Google Cloud サービスに接続する必要があり、インターネットアクセスが必要です。
- **クライアント**: クライアント側専用のクライアント VPC ネットワーク内のサブネット。通常、NetScaler はインターネットからパブリックサブネット経由でアプリケーションのクライアントトラフィックを受信します。
- **サーバー**: アプリケーションサーバーがプロビジョニングされるサブネット。すべてのアプリケーションサーバーはこのサブネットに存在し、このサブネットを介して NetScaler からアプリケーショントラフィックを受信します。Google Cloud でサブネットを作成する方法の詳細については、VPC ネットワークの概要を参照してください。

ファイアウォールを作成する
ファイアウォールには、NetScaler VPX インスタンスのインバウンドおよびアウトバウンドトラフィックを制御するルールがあります。必要なだけルールを追加できます。NetScaler インスタンスを自動スケーリングするには、3 つのファイアウォールを作成する必要があります。

- **管理**: NetScaler VPX の管理専用のファイアウォール。NetScaler は Google Cloud サービスに接続する必要があり、インターネットアクセスが必要です。インバウンドルールは、以下の TCP および UDP ポートで許可されます。
  - TCP: 80, 22, 443, 3008–3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

  注

  ファイアウォールがエージェントによるVPXへのアクセスを許可していることを確認してください。

- **クライアント**: ファイアウォールは、NetScaler VPXインスタンスのクライアント側通信専用です。通常、インバウンドルールはTCPポート80、22、443で許可されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **サーバー**: ファイアウォールは、NetScaler VPXのサーバー側通信専用です。Google Cloudでファイアウォールを作成する方法の詳細については、VPCファイアウォールルール概要を参照してください。

Google CloudでNetScaler VPXライセンスをサブスクライブする

1. Google Cloudポータルにログインします。
2. **Marketplace**でNetScalerを検索し、必要な製品バージョンを選択します。
3. 次のいずれかのライセンスタイプを選択します。

    - 顧客ライセンス
    - エンタープライズ
    - プラチナ

    注

    顧客ライセンスオプションを選択した場合、AutoscaleグループはNetScalerインスタンスのプロビジョニング中にNetScaler Consoleからライセンスをチェックアウトします。

NETSCALER CONSOLEコンポーネントをセットアップする

NetScaler ConsoleでNetScaler VPXインスタンスをプロビジョニングする前に、NetScaler Consoleで次のタスクを実行します。

1. 「サイトを作成する」(#create-a-site)。
2. 「Google Cloud に NetScaler エージェントをプロビジョニングする」(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-google-cloud.html#provision-netscaler-agent-on-google-cloud)。
3. 「サイトを NetScaler エージェントにアタッチする」(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-google-cloud.html#attach-the-site-to-a-netscaler-agent)。

サイトを作成する
NetScaler Console でサイトを作成し、Google Cloud に関連付けられている VNet の詳細を追加します。

1. NetScaler Console で、**Infrastructure > Sites** に移動します。
2. **Add** をクリックします。
3. **Select Cloud** ペインで、,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. サイトタイプとして **Data Center** を選択します。
b. タイプリストから **Google Cloud** を選択します。
c. **Fetch regions from the Google Cloud** チェックボックスをオンにします。

   このオプションを使用すると、Google Cloud アカウントから既存のリージョン情報を取得できます。
d. **Next** をクリックします。

4. **Choose Region** ペインで、,

a. **Cloud Access Profile** で、Google Cloud アカウント用に作成したプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。
b. クラウドアクセスプロファイルを作成するには、**追加**をクリックします。
c. **名前**に、NetScaler ConsoleでGoogle Cloudアカウントを識別するための名前を指定します。
d. **サービスアカウントのキー**に、Google Cloudで作成したサービスアカウントのJSONを指定します。

   NetScaler ConsoleからGoogle Cloudアカウントにアクセスする](/en-us/netscaler-console-service/media/gcp-cap.png)
e. **作成**をクリックします。

   詳細については、「サービスアカウントの作成」を参照してください。
f. **リージョン**で、管理するNetScaler VPXインスタンスを含むVPCネットワークがあるリージョンを選択します。
g. **サイト名**を指定します。
h. **完了**をクリックします。

Google CloudでNetScalerエージェントをプロビジョニングする
エージェントは、NetScaler Consoleと、データセンターまたはクラウド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。

1. **インフラストラクチャ > インスタンス > エージェント**に移動します。
2. **プロビジョニング**をクリックします。
3. **Google Cloud**を選択し、**次へ**をクリックします。
4. **プロビジョニングパラメータ**タブで、以下を指定します。

   - **名前** - エージェント名を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **サイト** - エージェントとNetScaler VPXインスタンスをプロビジョニングするため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** - リストからクラウドアクセスプロファイルを選択します。
- **ゾーン** - Autoscale™ グループを作成するゾーンを選択します。選択したクラウドアクセスプロファイルに応じて、そのプロファイルのゾーンが入力されます。
- **ネットワーク** - Autoscaleグループを作成するVPCネットワークを選択します。
- **サブネット** - エージェントをプロビジョニングするための管理サブネットを選択します。
- **タグ** - Autoscaleグループタグのキーと値のペアを入力します。タグは、大文字と小文字を区別するキーと値のペアで構成されます。これらのタグを使用すると、Autoscaleグループを簡単に整理および識別できます。タグはGoogle CloudとNetScaler Consoleの両方に適用されます。

5. **完了** をクリックします。

または、Google Cloud Marketplaceからエージェントをインストールすることもできます。詳細については、「Google CloudにNetScalerエージェントをインストールする」を参照してください。
サイトをNetScalerエージェントにアタッチする

1. NetScaler Consoleで、**インフラストラクチャ > インスタンス > エージェント** に移動します。
2. サイトをアタッチするエージェントを選択します。
3. **サイトをアタッチ** をクリックします。
4. アタッチするサイトをリストから選択します。
5. **保存** をクリックします。

構成タスク

Google Cloud にスタンドアロンの NetScaler 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. NetScaler Console で、**Infrastructure > Instances > NetScaler** に移動します。
2. **Provision** をクリックします。
3. **Google Cloud** を選択し、**Next** をクリックします。インスタンスをプロビジョニングするために必要なパラメータを指定します。
4. 基本パラメータ、ライセンス、プロビジョニングパラメータ を指定します。

基本パラメータを構成する

1. **Basic Parameters** タブで、以下を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Name** - NetScaler VPX インスタンスの名前を指定します。
- **Site** - 以前に作成したサイトを選択します。
- **Agent** - NetScaler VPX インスタンスを管理するために作成されたエージェントを選択します。
- **Cloud Access Profile** - サイト作成時に作成されたクラウドアクセスプロファイルを選択します。
- **NetScaler Profile** - 認証を提供するプロファイルを選択します。

  NetScaler Console は、NetScaler VPX インスタンスにログオンする必要がある場合にデバイスプロファイルを使用します。

2. **Next** をクリックします。

NetScaler VPX の基本パラメータのプロビジョニング(/en-us/netscaler-console-service/media/provision-adc-on-gcp.png)

ライセンスの構成

NetScaler インスタンスにライセンスを適用するには、次のいずれかのモードを選択します。

- **NetScaler Console の使用**: プロビジョニングするインスタンスは、NetScaler Console からライセンスをチェックアウトします。
- **Google Cloud の使用**: **クラウドから割り当て**オプションは、Google Cloud Marketplace で利用可能な NetScaler® 製品ライセンスを使用します。プロビジョニングするインスタンスは、マーケットプレイスからライセンスを使用します。

  Google Cloud Marketplace からライセンスを使用することを選択した場合は、**プロビジョニングパラメータ**タブで製品またはライセンスを指定します。

詳細については、「ライセンス要件」を参照してください。
NetScaler Console からライセンスを使用する
このオプションを使用するには、Google Cloud で**独自のライセンスを持ち込む**ソフトウェアプランで NetScaler 製品を購読していることを確認してください。「Google Cloud で NetScaler VPX ライセンスを購読する」を参照してください。

1. **ライセンス**タブで、**NetScaler Console から割り当て**を選択します。
2. **ライセンスタイプ**で、リストから次のいずれかのオプションを選択します。

   - **帯域幅ライセンス: 帯域幅ライセンスタイプ**リストから、次のいずれかのオプションを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **プールされた容量:** インスタンスに割り当てる容量を指定します。

  共通プールから、NetScaler インスタンスは1つのインスタンスライセンスと、指定された帯域幅のみをチェックアウトします。

- **VPX ライセンス:** NetScaler VPX インスタンスがプロビジョニングされると、インスタンスは NetScaler Console からライセンスをチェックアウトします。

- **仮想CPUライセンス:** プロビジョニングされたNetScaler VPXインスタンスは、インスタンスで実行されているCPUの数に応じてライセンスをチェックアウトします。

> **注**
>
> プロビジョニングされたインスタンスが削除または破棄されると、適用されたライセンスはNetScaler Consoleライセンスプールに戻ります。これらのライセンスは、新しいインスタンスをプロビジョニングするために再利用できます。

3. **ライセンスエディション**で、ライセンスエディションを選択します。NetScaler Consoleは、指定されたエディションを使用してインスタンスをプロビジョニングします。
4. **次へ**をクリックします。

プロビジョニングパラメータの構成

1. **プロビジョニングパラメータ**タブで、以下を指定します。

   - **NetScalerサービスアカウント**: Google Cloudで作成したサービスアカウントを選択します。NetScaler Consoleは、サービスアカウントを使用してGoogle Cloudリソースにアクセスします。
   - **製品/ライセンス**: プロビジョニングするNetScaler製品バージョンを選択します。詳細については、「Google CloudでNetScaler VPXライセンスをサブスクライブする」を参照してください。
   - **マシンタイプ**: リストから必要なマシンタイプを選択します。

     このリストには、選択したNetScalerイメージでサポートされているマシンタイプが表示されます。

   - **イメージ**: 必要なNetScalerバージョンイメージを選択します。NetScalerイメージを追加するには、**新規追加**をクリックします。
   - **構成テンプレート** – NetScalerインスタンスに展開するために使用する構成テンプレートを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **インスタンスあたりのサーバーサブネット内のIP** – 各インスタンスがサーバーサブネット内で持つことができるSNIPアドレスの数を指定します。

NetScalerインスタンスのプロビジョニングパラメータ(/en-us/netscaler-console-service/media/autoscale-gcp-cloud.png)

このタブでは、必要なNICを指定して構成することもできます。各NICには専用のファイアウォールとサブネットが含まれています。

詳細については、「VPCネットワークの作成」および「ファイアウォールの作成」を参照してください。

NetScalerインスタンスのNIC(/en-us/netscaler-console-service/media/autoscale-cloud-nics.png)

2. **完了**をクリックします。

プロビジョニングされたNetScaler VPXインスタンスを表示する

NetScaler Consoleで表示するには：

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler**に移動します。
2. **NetScaler VPX**タブを選択します。

   Google Cloudでプロビジョニングされたインスタンスがここに表示されます。

Google Cloudで表示するには：

1. Google Cloudポータルにログオンします。
2. プロビジョニングされたNetScaler VPXインスタンスが表示される**Resources**タブに移動します。

注

NetScaler VPXインスタンスの名前は、NetScaler Consoleでインスタンスをプロビジョニングする際に指定したものと同じです。

VMware ESX 上に NetScaler VPX インスタンスをプロビジョニングする

NetScaler Console を使用すると、VMware ESX での NetScaler VPX インスタンスの展開と管理を自動化できます。NetScaler Console を使用して VMware ESX 上に NetScaler VPX インスタン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スをプロビジョニングすると、そのインスタンスは NetScaler Console GUI で管理できるようになります。

NetScaler Console は、すでに展開されているインスタンスの NetScaler テンプレートを使用して、VMware ESX に新しいインスタンスをプロビジョニングします。必要な VMware ESX サーバーの詳細が存在する VMware vCenter のデータセンターをサイトに保存します。また、クラウドアクセスプロファイルを使用して VMware vCenter にアクセスし、VMware ESX に VPX を展開します。

前提条件

VMware ESX に NetScaler VPX インスタンスをプロビジョニングする前に、以下を完了していることを確認してください。

1. サポートされている VMware ESXi バージョン (6.0、6.5、および 6.7) をインストールします。
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します(/ja-jp/citrix-adc/current-release/deploying-vpx/install-vpx-on-esx#downloading-the-netscaler-vpx-setup-files)。
4. ESX で NetScaler VPX ファイルをテンプレートに変換します(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-vmware.html#convert-netscaler-vpx-files-into-templates)。
5. NetScaler Console が VMware vCenter にアクセスするための権限を作成します(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-vmware.html#create-permissions-for-netscaler-console-to-access-vmware-vcenter)。
6. NetScaler Console でサイトを作成します(/ja-jp/netscaler-console-service/hybrid-multi-cloud-deployments/provisioning-vpx-vmware.html#create-a-site-in-netscaler-console)。

NetScaler VPX ファイルをテンプレートに変換する

NetScaler Console は、NetScaler VPX ファイルによって変換された ESX 内の NetScaler テンプレートを使用します。VPX ファイルをテンプレートに変換するには、次の手順を実行します。

1. NetScaler セットアップファイルを使用して、VMware 上に NetScaler VPX インスタンスを展開します。

   初回は、NetScaler セットアップファイルを使用して VPX インスタンスを展開します。詳細については、「VMware 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、**テンプレート**を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **テンプレートに変換**をクリックします。

VPXセットアップファイルをテンプレートに変換(/en-us/netscaler-console-service/media/convert-to-template.png)

NetScaler ConsoleがVMware vCenterにアクセスするための権限を作成する

VMware vCenterでNetScaler Consoleのプロビジョニングと管理を有効にするには、次の手順に従います。

1. 権限を持つカスタムロールを作成する
    a. VMware vCenterにログインし、**ロール**セクションに移動します。
    b. NetScaler Console用にカスタマイズされたカスタムロールを作成します。
    c. 次の権限を割り当てます。

```
Datastore.AllocateSpace

Resource.AssignVMToPool

VirtualMachine.Config.AdvancedConfig

VirtualMachine.Inventory.CreateFromExisting

VirtualMachine.Inventory.Delete

VirtualMachine.Interact.PowerOff

VirtualMachine.Interact.PowerOn

VirtualMachine.Provisioning.DeployTemplate
```

2. ユーザーを作成する
    a. ロールが定義されたら、**ユーザーとグループ**セクションに移動します。
    b. NetScaler ConsoleがVMware vCenterにアクセスするためのユーザーを作成します。
    c. 新しく作成したユーザーのパスワードを設定します。
3. ロールをユーザーに関連付ける
    a. **グローバル権限**セクションに移動し、カスタムロールをユーザーに関連付けます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. この関連付けにより、NetScaler Console は VMware vCenter で必要なアクションを実行するための特権を得られます。

注:

記載されている特権は、NetScaler Console が VMware vCenter にアクセスするための最小要件です。制限された特権を持つユーザーを作成することはオプションです。指定された特権のスーパーセットを含む特権を持つユーザーがいる場合、そのユーザーは代わりにそれらの資格情報を提供できます。

VMware vCenter で特権を持つユーザーロールを構成する方法の詳細については、「ユーザーアクセスを構成する」を参照してください。

NetScaler Console でサイトを作成する

NetScaler Console でサイトを作成し、VMware ESX の詳細を追加します。

1. NetScaler Console で、 **> >** の順に移動します。
2. をクリックします。
3. ペインで、,
   a. として を選択します。
   b. リストから を選択します。
   c. をクリックします。
4. ペインで、,
   a. ペインで、VMware ESX 用に作成したプロファイルを選択します。プロファイルがない場合は、プロファイルを作成します。
   b. クラウドアクセスプロファイルを作成するには、 をクリックして以下を指定します。
      - **名前** – NetScaler Console でクラウドアクセスプロファイルを識別するための名前を指定します。
      - **IPアドレス** – VMware vCenter の IP アドレスを指定します。
      - **ユーザー名** – VMware vCenter 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 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。
      - **エージェント** - NetScaler Console に登録されているエージェントを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラウドアクセスプロファイルの作成(/en-us/netscaler-console-service/media/cap-vmware.png)

c. **ネットワーク (データセンター)** で、NetScaler VPX テンプレートがあるデータセンターを選択します。

d. **サイト名** を指定します。

e. データセンターの地理的位置を識別するために、**リージョン**、**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-console-service/media/create-site.png)

VMware ESX で NetScaler VPX インスタンスをプロビジョニングする

VMware ESX に関連付けたサイトを使用して、NetScaler VPX インスタンスをプロビジョニングします。

注:

現在、NetScaler Console はスタンドアロンの NetScaler インスタンスのプロビジョニングのみをサポートしています。

1. NetScaler Consoleで、**Infrastructure > Instances > NetScaler**に移動します。
2. **VPX**タブで、**Provision**をクリックします。

   このオプションにより、**Provision NetScaler VPX on Cloud**ページが表示されます。
3. **Choose Cloud**タブで、**VMware vCenter**を選択し、**Next**をクリックします。

   VMware vCenterを選択(/en-us/netscaler-console-service//media/select-vmware.png)
4. **Basic Parameters**タブで、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NetScalerプロファイルを選択します。

   基本パラメータ(/en-us/netscaler-console-service/media/basic-parameters-vmware.png)
5. **Next**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. **License**タブでは、**Allocate from Cloud**オプションが自動的に選択され、VMware vCenterで利用可能なNetScaler製品ライセンスが使用されます。プロビジョニングするVPXインスタンスは、VMware vCenterのライセンスを使用します。

   a. **ライセンスタイプ** – ライセンスタイプとして、帯域幅ライセンスまたは仮想CPUライセンスを選択します。

      i. 帯域幅ライセンスタイプの場合、**Bandwidth License Type**リストから以下のいずれかのオプションを選択できます。

         - **プールされたキャパシティ** - **各NetScalerインスタンスに割り当てる帯域幅キャパシティ**で、インスタンスに割り当てるキャパシティを指定します。

           共通プールから、NetScalerインスタンスは1つのインスタンスライセンスと、指定された帯域幅のみをチェックアウトします。

         - **VPXライセンス** - NetScaler VPXインスタンスがプロビジョニングされると、インスタンスはNetScaler Consoleからライセンスをチェックアウトします。

      ii. **仮想CPUライセンス**: プロビジョニングされたNetScaler VPXインスタンスは、インスタンスで実行されているCPUの数に応じてライセンスをチェックアウトします。

   > **注:**
   >
   > プロビジョニングされたVPXインスタンスが削除または破棄されると、適用されたライセンスはNetScaler Consoleライセンスプールに戻ります。これらのライセンスは、新しいVPXインスタンスをプロビジョニングするために再利用できます。

   b. **ライセンスエディション** – リストからライセンスエディションを選択します。

      NetScaler Consoleは、指定されたエディションを使用してVPXインスタンスをプロビジョニングします。

7. **次へ**をクリックします。
8. **プロビジョニングパラメータ**タブで、次の詳細を指定します。

   - **クラスター** – インスタンスをプロビジョニングするクラスターを選択します。
   - **ホスト** – リストから必要なホストを選択します。
   - **テンプレート** – インスタンスに適用するテンプレートをリストから選択します。
   - **データストア** – リストからデータストアを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**構成テンプレート**」 - リストから構成テンプレートを選択します。
- 「**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。

9. 「**完了**」をクリックして、VPXインスタンスをプロビジョニングします。

NetScaler ハイブリッドおよびマルチクラウド展開のためのグローバル負荷分散

NetScaler のハイブリッドおよびマルチクラウドグローバル負荷分散 (GLB) ソリューションを使用すると、ハイブリッドクラウド、マルチクラウド、およびオンプレミス展開の複数のデータセンターにアプリケーショントラフィックを分散できます。NetScaler のハイブリッドおよびマルチクラウド GLB ソリューションは、既存のセットアップを変更することなく、ハイブリッドまたはマルチクラウドで負荷分散セットアップを管理するのに役立ちます。また、オンプレミスセットアップがある場合は、完全にクラウドに移行する前に、NetScaler のハイブリッドおよびマルチクラウド GLB ソリューションを使用して、一部のサービスをクラウドでテストできます。たとえば、トラフィックのごく一部のみをクラウドにルーティングし、ほとんどのトラフィックをオンプレミスで処理できます。NetScaler のハイブリッドおよびマルチクラウド GLB ソリューションは、単一の統合コンソールから地理的な場所を越えて NetScaler インスタンスを管理および監視することも可能にします。

ハイブリッドおよびマルチクラウドアーキテクチャは、「ベンダーロックイン」を回避し、パートナーや顧客のニーズを満たすために異なるインフラストラクチャを使用することで、企業全体のパフォーマンスを向上させることもできます。複数のクラウドアーキテクチャを使用すると、使用した分だけ支払うだけで済むため、インフラストラクチャコストをより適切に管理できます。また、オンデマンドでインフラストラクチャを使用するため、アプリケーションをより適切にスケーリングできます。さらに、各プロバイダーの最高のサービスを活用するために、あるクラウドから別のクラウドへ迅速に切り替える機能も提供します。

NetScaler ハイブリッドおよびマルチクラウド GLB ソリューションのアーキテクチャ

次の図は、NetScaler ハイブリッドおよびマルチクラウド GLB 機能のアーキテクチャを示しています。

NetScaler ハイブリッドおよびマルチクラウド GLB ソリューションのアーキテクチャの図(/en-us/netscaler-console-service/media/mas-hybrid-multicloud-glb-architecture_parent_child_topology-new.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler GLB ノードは DNS 名前解決を処理します。これらの GLB ノードのいずれも、任意のクライアントロケーションから DNS リクエストを受信できます。DNS リクエストを受信した GLB ノードは、設定された負荷分散方法によって選択された負荷分散仮想サーバーの IP アドレスを返します。メトリック (サイト、ネットワーク、および永続性メトリック) は、Citrix 独自のプロトコルであるメトリック交換プロトコル (MEP) を使用して GLB ノード間で交換されます。MEP プロトコルの詳細については、「メトリック交換プロトコルの構成」を参照してください。

GLB ノードで構成されたモニターは、同じデータセンター内の負荷分散仮想サーバーのヘルスステータスを監視します。親子トポロジでは、GLB ノードと NetScaler ノード間のメトリックは MEP を使用して交換されます。ただし、親子トポロジでは、GLB と NetScaler LB ノード間のモニタープローブの構成はオプションです。

エージェントは、NetScaler Console とデータセンター内の管理対象インスタンス間の通信を可能にします。エージェントとそのインストール方法の詳細については、「はじめに」を参照してください。

注

このドキュメントでは、次の前提条件を設けています。

- 既存の負荷分散設定がある場合、それが稼働していること。
- 各 NetScaler GLB ノードに SNIP アドレスまたは GLB サイト IP アドレスが構成されていること。この IP アドレスは、他のデータセンターとメトリックを交換する際のデータセンターソース IP アドレスとして使用されます。
- DNS トラフィックを受信するために、各 NetScaler GLB インスタンスに ADNS または ADNS-TCP サービスが構成されていること。
- 必要なファイアウォールとセキュリティグループがクラウドサービスプロバイダーで構成されていること。

セキュリティグループの設定

クラウドサービスプロバイダーで、必要なファイアウォール/セキュリティグループ設定を行う必要があります。AWSのセキュリティ機能の詳細については、AWSドキュメントを参照してください。Microsoft Azureネットワークセキュリティグループの詳細については、Microsoft Azureドキュメントを参照してください。

さらに、GLBノードでは、ADNSサービス/DNSサーバーIPアドレス用にポート53を、MEPトラフィック交換用にGSLBサイトIPアドレス用にポート3009を開く必要があります。ロードバランシ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ングノードでは、アプリケーションのトラフィックを受信するために適切なポートを開く必要があります。たとえば、HTTPトラフィックを受信するためにポート80を、HTTPSトラフィックを受信するためにポート443を開く必要があります。エージェントとNetScaler Console間のNITRO通信用にポート443を開きます。
動的ラウンドトリップ時間GLBメソッドの場合、設定されたLDNSプローブタイプに応じてUDPおよびTCPプローブを許可するためにポート53を開く必要があります。UDPまたはTCPプローブはSNIPのいずれかを使用して開始されるため、この設定はサーバー側サブネットにバインドされたセキュリティグループに対して行う必要があります。

NetScalerハイブリッドおよびマルチクラウドGLBソリューションの機能

NetScalerハイブリッドおよびマルチクラウドGLBソリューションの機能の一部をこのセクションで説明します。

他のロードバランシングソリューションとの互換性

NetScalerハイブリッドおよびマルチクラウドGLBソリューションは、NetScalerロードバランサー、Nginx、その他のサードパーティ製ロードバランサーなど、さまざまなロードバランシングソリューションをサポートしています。

注

NetScaler以外のロードバランシングソリューションは、近接ベースおよび非メトリックベースのGLBメソッドが使用され、親子トポロジが構成されていない場合にのみサポートされます。

GLBメソッド

NetScalerハイブリッドおよびマルチクラウドGLBソリューションは、以下のGLBメソッドをサポートしています。

- メトリックベースのGLBメソッド。メトリックベースのGLBメソッドは、メトリック交換プロトコルを介して他のNetScalerノードからメトリックを収集します。
  - 最小接続数：クライアント要求は、アクティブな接続数が最も少ないロードバランサーにルーティングされます。
  - 最小帯域幅：クライアント要求は、現在最も少ないトラフィックを処理しているロードバランサーにルーティングされます。
  - 最小パケット数: クライアント要求は、過去14秒間に受信したパケット数が最も少ないロードバランサーにルーティングされます。
- メトリックベースではないGLBメソッド

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ラウンドロビン: クライアント要求は、ロードバランサーのリストの最上位にあるロードバランサーのIPアドレスにルーティングされます。そのロードバランサーは、リストの最下位に移動します。
- 送信元IPハッシュ: このメソッドは、クライアントIPアドレスのハッシュ値を使用してロードバランサーを選択します。

- 近接性ベースのGLBメソッド
  - 静的近接性: クライアント要求は、クライアントIPアドレスに最も近いロードバランサーにルーティングされます。
  - ラウンドトリップタイム (RTT): このメソッドは、RTT値（クライアントのローカルDNSサーバーとデータセンター間の接続における時間遅延）を使用して、最もパフォーマンスの高いロードバランサーのIPアドレスを選択します。

ロードバランシングメソッドの詳細については、「ロードバランシングアルゴリズム」を参照してください。

GLBトポロジ

NetScalerハイブリッドおよびマルチクラウドGLBソリューションは、アクティブ-パッシブトポロジと親子トポロジをサポートしています。

- アクティブ-パッシブトポロジ - 障害点から保護することで、ディザスタリカバリを提供し、アプリケーションの継続的な可用性を確保します。プライマリデータセンターがダウンした場合、パッシブデータセンターが稼働状態になります。GSLBアクティブ-パッシブトポロジの詳細については、「ディザスタリカバリのためのGSLBの構成」を参照してください。
- 親子トポロジ – メトリックベースのGLBメソッドを使用してGLBおよびLBノードを構成する場合、およびLBノードが別のNetScalerインスタンスに展開されている場合に使用できます。親子トポロジでは、親サイトと子サイト間のメトリック交換がメトリック交換プロトコル (MEP) を介して行われるため、LBノード (子サイト) はNetScalerアプライアンスである必要があります。

親子トポロジの詳細については、「MEPプロトコルを使用した親子トポロジの展開」を参照してください。

IPv6のサポート

NetScalerハイブリッドおよびマルチクラウドGLBソリューションはIPv6もサポートしています。

監視

NetScalerのハイブリッドおよびマルチクラウドGLBソリューションは、セキュアな接続を有効にするオプションを備えた組み込みモニターをサポートしています。ただし、LBおよびGLB構成が

© 1997–2026 Citrix Systems, Inc. All rights reserved.

同じNetScalerインスタンス上にある場合、または親子トポロジが使用されている場合、モニターの構成はオプションです。

永続性

NetScalerのハイブリッドおよびマルチクラウドGLBソリューションは、以下をサポートしています。

- ソースIPベースの永続セッション。これにより、同じクライアントからの複数のリクエストが、設定されたタイムアウト期間内に到着した場合、同じサービスに転送されます。クライアントが次のリクエストを送信する前にタイムアウト値が期限切れになった場合、セッションは破棄され、設定された負荷分散アルゴリズムがクライアントの次のリクエストのために新しいサーバーを選択するために使用されます。
- スピルオーバー永続性。これにより、プライマリの負荷がしきい値を下回った後でも、バックアップ仮想サーバーは受信したリクエストの処理を継続します。詳細については、「スピルオーバーの構成」を参照してください。
- サイト永続性。これにより、GLBノードはクライアントリクエストを処理するデータセンターを選択し、後続のすべてのDNSリクエストに対して選択されたデータセンターのIPアドレスを転送します。設定された永続性がDOWN状態のサイトに適用される場合、GLBノードはGLBメソッドを使用して新しいサイトを選択し、その新しいサイトがクライアントからの後続のリクエストに対して永続的になります。

NetScaler Console StyleBookを使用した構成

NetScaler Consoleのデフォルトのマルチクラウド GLB StyleBookを使用して、ハイブリッドおよびマルチクラウドGLB構成でNetScalerインスタンスを構成できます。

デフォルトのマルチクラウドGLB StyleBook for LB Node StyleBookを使用して、アプリケーショントラフィックを処理する親子トポロジの子サイトであるNetScaler負荷分散ノードを構成できます。このStyleBookは、親子トポロジの場合にLBノードを構成したい場合にのみ使用してください。ただし、各LBノードは、このStyleBookを使用して個別に構成する必要があります。

NetScalerハイブリッドおよびマルチクラウドGLBソリューション構成のワークフロー

NetScaler Consoleに付属のマルチクラウドGLB StyleBookを使用して、ハイブリッドおよびマルチクラウドGLB構成でNetScalerインスタンスを構成できます。

次の図は、NetScalerハイブリッドおよびマルチクラウドGLBソリューションを構成するためのワークフローを示しています。ワークフロー図の各ステップについては、図の後に詳しく説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラウド管理者として、次のタスクを実行します。

1. Citrix Cloud™ アカウントにサインアップします。

   NetScaler Console の使用を開始するには、Citrix Cloud 企業アカウントを作成するか、社内の誰かが作成した既存のアカウントに参加します。

2. Citrix Cloud にログオンした後、**NetScaler Console** タイルで **Manage** をクリックし、NetScaler Console を初めてセットアップします。

3. 複数のエージェントをダウンロードしてインストールします。

   NetScaler Console とデータセンターまたはクラウド内の管理対象インスタンス間の通信を有効にするには、ネットワーク環境にエージェントをインストールして構成する必要があります。管理対象インスタンスで LB および GLB 構成を設定できるように、各リージョンにエージェントをインストールします。LB および GLB 構成は単一のエージェントを共有できます。上記の 3 つのタスクの詳細については、Getting Started を参照してください。

4. Microsoft Azure/AWS のクラウド環境、オンプレミスのデータセンターにロードバランサーを展開します。

   クラウドおよびオンプレミスに展開するロードバランサーの種類に応じて、それらを適切にプロビジョニングします。たとえば、Microsoft Azure Resource Manager (ARM) ポータル、Amazon Web Services (AWS) 仮想プライベートクラウド、およびオンプレミスデータセンターに NetScaler VPX インスタンスをプロビジョニングできます。仮想マシンを作成し、その他のリソースを構成することにより、NetScaler インスタンスをスタンドアロンモードで LB または GLB ノードとして機能するように構成します。NetScaler VPX インスタンスの展開方法の詳細については、以下のドキュメントを参照してください。

   - NetScaler VPX for AWS AMI の起動。
   - Azure Resource Manager でスタンドアロンモードの NetScaler VPX を構成する(http://docs.citrix.com/ja-jp/netscaler/12/deploying-vpx/deploy-vpx-on-azure/configure-vpx-standalone-arm.html)。

5. セキュリティ構成を実行します。

   インスタンスとサブネットのインバウンドおよびアウトバウンドトラフィックを制御するために、ARM または AWS でネットワークセキュリティグループとネットワーク ACL を構成します。

6. NetScaler Console に NetScaler インスタンスを追加します。

   NetScaler インスタンスは、NetScaler Console から検出、管理、監視したいネットワークアプライアンスまたは仮想アプライアンスです。これらのインスタンスを管理および監視するに

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、インスタンスをサービスに追加し、LB (LB に NetScaler を使用している場合) と GLB の両方のインスタンスを登録する必要があります。NetScaler Console で NetScaler インスタンスを追加する方法の詳細については、Getting Started を参照してください。

7. デフォルトの NetScaler Console StyleBook を使用して、GLB および LB 構成を実装します。

   - 選択した GLB NetScaler インスタンスで GLB 構成を実行するには、**Multi-cloud GLB StyleBook** を使用します。
   - ロードバランシング構成を実装します。(管理対象インスタンスにすでにLB構成がある場合は、この手順をスキップできます。)

   NetScalerインスタンスでロードバランサーを構成するには、次の2つの方法があります。

   - アプリケーションのロードバランシングのためにインスタンスを手動で構成します。インスタンスを手動で構成する方法の詳細については、「基本的なロードバランシングのセットアップ」を参照してください。
   - StyleBookを使用します。選択したNetScalerインスタンスでロードバランサー構成を作成するには、NetScaler Console StyleBookのいずれか（HTTP/SSL LoadBalancing StyleBookまたはHTTP/SSL LoadBalancing (with Monitors) StyleBook）を使用できます。独自のStyleBookを作成することもできます。StyleBookの詳細については、「StyleBook」を参照してください。

8. 次のいずれかのケースでGLB親子トポロジを構成するには、**Multi-cloud GLB StyleBook for LB Node**を使用します。

   - メトリックベースのGLBアルゴリズム（最小パケット、最小接続、最小帯域幅）を使用してGLBおよびLBノードを構成する場合、およびLBノードが別のNetScalerインスタンスに展開されている場合。
   - サイトの永続性が必要な場合。

StyleBook を使用した GLB の構成

マルチクラウド GLB StyleBook を使用して、データセンターにプロビジョニングされている NetScaler インスタンスで GLB 構成を設定できます。各データセンターの NetScaler GLB インスタンスでサイト IP アドレスが構成されていることを確認してください。

この StyleBook を使用して、GLB ノードに後で追加する可能性のある子サイトを受け入れる親サイトを作成することもできます。NetScaler インスタンスでマルチクラウド GLB 構成を設定するには。

1. **アプリケーション** > **構成** に移動し、**新規作成** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **StyleBook の選択** ページには、NetScaler Console で使用できるすべての StyleBook が表示されます。下にスクロールして、**マルチクラウド GLB StyleBook** を選択します。

   マルチクラウド GLB StyleBook は、複数のクラウドおよびオンプレミスサイトに展開されているアプリケーションの GLB を構成するために使用されます。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表示されます。

   注

   このドキュメントでは、データセンターとサイトという用語は同じ意味で使用されています。

3. 次のパラメータを設定します。

   - **アプリケーション名**。GLB サイトに展開されているアプリケーションの名前を入力します。
   - **GLB アルゴリズム**。クライアントにサービスを提供するサイトを選択するためのグローバル負荷分散アルゴリズム（メソッド）を選択します。ドロップダウンリストボックスで利用可能なオプションは、LEASTCONNECTION、LEASTBANDWIDTH、LEASTPACKETS、ROUNDROBIN、STATICPROXIMITY、SOURCEIPHASH、および RTT です。
   - **Geo データベースファイル**。GLB アルゴリズムとして STATICPROXIMITY を選択した場合は、静的近接データを含むデータベースファイルの完全なパスと名前を入力します。データベースファイルが、指定された場所にあるすべての GLB NetScaler インスタンスに存在することを確認してください。または、デフォルトファイルを保持することもできます。
   - **プロトコル**。展開されたアプリケーションのアプリケーションプロトコルをドロップダウンリストボックスから選択します。
   - **永続性設定**。仮想サーバーで構成された永続性は、その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ます（たとえば、eコマースで使用される接続）。仮想サーバーが選択されると、永続性は負荷分散メソッドを上書きします。永続性構成がダウンしているサービスに適用された場合、インスタンスは負荷分散メソッドを使用して新しいサービスを選択し、その新しいサービスはクライアントからの後続のリクエストに対して永続的になります。
   - **永続性タイプ**。このアプリケーションに使用する永続性タイプを選択します。たとえば、永続性として SOURCEIP を選択した場合、アプリケーションをホストするサイトの最初

© 1997–2026 Citrix Systems, Inc. All rights reserved.

の選択後、同じクライアントからの後続のすべてのリクエストは、アプリケーションのサービスにアクセスするためにそのサイトに送信されます。

- **永続性タイムアウト**。永続性タイプとしてSOURCEIPを選択した場合、最後のクライアント要求から永続性セッションが期限切れになるまでの分数値を入力します。範囲は2分から1440分です。分は秒単位で解決されます。

4. **スピルオーバー設定**。たとえば、プライマリ仮想サーバーの接続制限または帯域幅制限がしきい値に達した場合に、スピルオーバー接続をセカンダリまたはバックアップ仮想サーバーに転送するようにスピルオーバー機能を構成します。

   - **スピルオーバー方式**。ドロップダウンリストボックスから、スピルオーバーの方式を選択します。たとえば、CONNECTIONスピルオーバー方式は、プライマリサーバーでアクティブな接続数を監視します。この方式でスピルオーバーしきい値に達すると、新しい接続はバックアップチェーンで最初に利用可能な仮想サーバーに転送されます。HEALTHスピルオーバー方式では、しきい値が設定されたしきい値を下回った場合にスピルオーバーを許可します。たとえば、70%未満の場合です。

     注

     HEALTHスピルオーバー方式を除き、その他の方式は、NetScalerがロードバランサーインスタンスとして使用されている場合にのみ適用されます。

   - **スピルオーバーしきい値**。選択したスピルオーバー方式のしきい値を入力します。
   - **スピルオーバー永続性**。プライマリの負荷がしきい値を下回った後でも、バックアップ仮想サーバーが受信した要求の処理を継続するようにする場合は、スピルオーバー永続性を有効にします。
   - **スピルオーバー永続性タイムアウト**。スピルオーバー永続性が有効な期間を設定します。最小値は2分、最大値は1440分です。分は秒単位で解決されます。

5. **永続性/スピルオーバー永続性ID**。永続性タイプとしてSOURCEIPを選択した場合、またはスピルオーバー永続性が有効になっている場合は、すべてのGLBアプライアンスで同じドメインを識別するための一意の番号を入力します。範囲は1から65535です。

   - **GLBサービスエンドポイントのヘルスチェック (オプション)**
   - **ヘルスチェックタイプ**。ドロップダウンリストボックスから、サイト上のアプリケーションを表すロードバランサーVIPアドレスのヘルスチェックに使用されるプローブのタイプを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **セキュアモード**。(オプション) SSLベースのヘルスチェックが必要な場合は、このパラメーターを有効にするには「**はい**」を選択します。
- **HTTPリクエスト**。(オプション) ヘルスチェックタイプとしてHTTPを選択した場合、VIPアドレスをプローブするために使用される完全なHTTPリクエストを入力します。
- **HTTPステータス応答コードのリスト**。(オプション) ヘルスチェックタイプとしてHTTPを選択した場合、VIPが正常な場合にHTTPリクエストへの応答で予期されるHTTPステータスコードのリストを入力します。

6. **GLBドメイン名**。このセクションでは、このアプリケーションに関連付けられたDNSドメイン名のリストを設定できます。プラスアイコン (+) をクリックして、アプリケーションのDNSドメイン名を作成します。
7. **GLBサイト**。このセクションでは、このアプリケーションが展開されているサイトのリストを構成できます。

   GLBサイトは、GLB通信のトップレベルエンティティです。サイトを構成する際に指定された情報は、ローカルサイトをリモートサイトにリンクし、Citrix Metrics Exchange Protocol (MEP) を使用して監視データを共有するために使用されます。IPアドレスはGLB NetScalerインスタンスが所有し、TCPポート3009を使用します。StyleBookのGLBサイトセクションでは、必要な数のGLBサイトを指定できます。

   サイトを追加するには、プラスアイコン (+) をクリックします。

   - **サイト名**。サイトの名前を入力します。
   - **サイトIPアドレス**。他のサイトとメトリックを交換する際に、サイトが送信元IPアドレスとして使用するIPアドレスを入力します。このIPアドレスは、各サイトのGLBインスタンスにすでに構成されているものと見なされます。
   - **サイトのパブリックIPアドレス**。(オプション) サイトのIPアドレスがNATされている場合、メトリックの交換に使用されるサイトのパブリックIPアドレスを入力します。
8. **子サイト**。プラスアイコン (+) をクリックして、必要な子サイトを構成します。
   - **子サイト名**。サイトの名前を入力します。
   - **子サイトIPアドレス**。子サイトのIPアドレスを入力します。ここでは、子サイトとして構成されているNetScalerノードのプライベートIPアドレスまたはSNIPを使用します。
   - **サイトのパブリックIPアドレス**。(オプション) サイトのIPアドレスがNATされている場合、メトリックの交換に使用されるサイトのパブリックIPアドレスを入力します。
9. **サービスサイトの永続性**。サイト上のGLBサービスに使用する永続性の種類をドロップダウンリストボックスから選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ConnectionProxyを選択すると、サイトはサイトクッキーを挿入したGLBサイトへの接続を作成し、クライアント要求を元のサイトにプロキシし、元のGLBサイトから応答を受信し、応答をクライアントに中継し、接続を閉じることができます。
- `HTTPRedirect` を選択すると、サイトは要求を最初にクッキーを挿入したサイトにリダイレクトできます。永続性の詳細については、「永続接続の構成」を参照してください。

10. **アクティブなGLBサービス**: このセクションでは、アプリケーションが展開されているサイトのアクティブなサービスのリストを構成できます。

    サービスIP。このサイトのGLBサービスのIPアドレスを入力します。

    - **サービスパブリックIPアドレス**。仮想IPアドレスがプライベートで、パブリックIPアドレスがNATされている場合は、そのパブリックIPアドレスを指定します。
    - **サービスポート**。このサイトのGLBサービスのポートを入力します。
    - **サービスウェイト**。GLBサービスに割り当てられるウェイトを入力します。

      注

      クラウドに送信する必要があるトラフィックの割合と、オンプレミスで処理する必要があるトラフィックの割合に応じて、サービスに相対的なウェイトを割り当てることができます。たとえば、クラウドベースのGLBサービスに3、オンプレミスのGLBサービスに7のウェイトを割り当てた場合、トラフィックの30%がクラウドに転送され、70%がオンプレミスで処理されます。

    - **サイト名**。GLBサービスが配置されているサイトの名前を入力します。
    - **サイトプレフィックス**。GLBサービスが構成されているサイトのプレフィックスを入力します。これは、サイトの永続性が有効で、メソッドが `httpredirect` の場合に適用されます。サイトプレフィックスの値は、アプリケーションのすべてのGLBサービスで一意である必要があります。
    - **最大クライアント接続数**。**Spillover Persistence**設定でスピルオーバーメソッドとしてDYNAMICCONNECTIONを選択した場合、GLBサービスで構成されている最大クライアント接続数を入力します。値を指定しない場合、システムはデフォルトで、構成可能な最大クライアント接続数に数値を割り当てます。

11. **パッシブGLBサービス**: このセクションでは、アプリケーションがアクティブ/パッシブトポロジで展開されているサイトで、パッシブサービスのリストを構成できます。アクティブGLBサービスに提供した情報と同様に、すべてのバックアップGLBサービスの情報を提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. **Target Instances**をクリックし、GLB構成を展開する各サイトでGLBインスタンスとして構成されているNetScalerインスタンスを選択します。
13. 選択したNetScalerインスタンスにGLB構成を作成するには、**Create**をクリックします。**Dry Run**をクリックして、ターゲットインスタンスに作成されるオブジェクトを確認することもできます。作成したStyleBook構成（config pack）は、Configurationsページの構成リストに表示されます。この構成（config pack）は、NetScaler Console GUIを使用して、確認、更新、または削除できます。

StyleBook を使用して NetScaler LB ノードで GLB を構成する

メトリックベースの GLB アルゴリズム (最小パケット、最小接続、最小帯域幅) を使用して GLB および LB ノードを構成し、LB ノードが別の NetScaler インスタンスに展開されている場合は、**LB ノード用マルチクラウド GLB StyleBook** を使用できます。

既存の親サイトに追加の子サイトを構成するために、この StyleBook を使用することもできます。この StyleBook は、一度に 1 つの子サイトを構成します。したがって、子サイトの数だけ、この StyleBook から構成 (構成パック) を作成してください。StyleBook は、子サイトに GLB 構成を適用します。最大 1024 の子サイトを構成できます。

注

親サイトを構成するには、マルチクラウド GLB StyleBook を使用します。

この StyleBook は、以下の前提条件に基づいています。

- SNIP アドレスまたは GLB サイト IP アドレスが構成されていること。
- 必要なファイアウォールとセキュリティグループがクラウドサービスプロバイダーで構成されていること。

LB ノード用マルチクラウド GLB StyleBook を使用して、親子トポロジで子サイトを構成する

1. **アプリケーション** > **構成** に移動し、**新規作成** をクリックします。
2. **StyleBook の選択** ページには、NetScaler Console で使用できるすべての StyleBook が表示されます。下にスクロールして、**LB ノード用マルチクラウド GLB 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注**
>
> このドキュメントでは、データセンターとサイトという用語は同じ意味で使用されています。

3. 次のパラメータを設定します。

   - **アプリケーション名**。子サイトを作成するGLBサイトに展開されているGLBアプリケーションの名前を入力します。
   - **プロトコル**。展開されているアプリケーションのアプリケーションプロトコルをドロップダウンリストボックスから選択します。
   - **LBヘルスチェック (オプション)**
     - **ヘルスチェックタイプ**。ドロップダウンリストボックスから、サイト上のアプリケーションを表すロードバランサーVIPアドレスのヘルスチェックに使用されるプローブのタイプを選択します。
     - **セキュアモード**。(オプション) SSLベースのヘルスチェックが必要な場合は、このパラメータを有効にするために**はい**を選択します。
     - **HTTPリクエスト**。(オプション) ヘルスチェックタイプとしてHTTPを選択した場合は、VIPアドレスのプローブに使用される完全なHTTPリクエストを入力します。
     - **HTTPステータス応答コードのリスト**。(オプション) ヘルスチェックタイプとしてHTTPを選択した場合は、VIPが正常なときにHTTPリクエストへの応答で予期されるHTTPステータスコードのリストを入力します。

4. 親サイトの構成。

   子サイト (LBノード) を作成する親サイト (GLBノード) の詳細を指定します。

   - **サイト名**。親サイトの名前を入力します。
   - **サイトIPアドレス**。親サイトが他のサイトとメトリックを交換する際にsourceIPアドレスとして使用するIPアドレスを入力します。このIPアドレスは、各サイトのGLBノードにすでに構成されているものとします。
   - **サイトパブリックIPアドレス**。(オプション) 親サイトのIPアドレスがNATされている場合、メトリックの交換に使用される親サイトのパブリックIPアドレスを入力します。

5. 子サイトの構成。

   子サイトの詳細を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **サイト名**。サイトの名前を入力します。
- **サイトIPアドレス**。子サイトのIPアドレスを入力します。ここでは、子サイトとして構成されているNetScalerノードのプライベートIPアドレスまたはSNIPを使用します。
- **サイトパブリックIPアドレス**。(オプション) サイトのIPアドレスがNATされている場合、メトリクス交換に使用される子サイトのパブリックIPアドレスを入力します。

6. アクティブなGLBサービスの構成 (オプション)

   LB仮想サーバーのIPアドレスがパブリックIPアドレスでない場合にのみ、アクティブなGLBサービスを構成します。このセクションでは、アプリケーションが展開されているサイトでローカルGLBサービスのリストを構成できます。

   - **サービスIP**。このサイトのロードバランシング仮想サーバーのIPアドレスを入力します。
   - **サービスパブリックIPアドレス**。仮想IPアドレスがプライベートで、それにNATされたパブリックIPアドレスがある場合は、そのパブリックIPアドレスを指定します。
   - **サービスポート**。このサイトのGLBサービスのポートを入力します。
   - **サイト名**。GLBサービスが配置されているサイトの名前を入力します。

7. **ターゲットインスタンス**をクリックし、GLB構成を展開する各サイトでGLBインスタンスとして構成されているNetScalerインスタンスを選択します。
8. **作成**をクリックして、選択したNetScalerインスタンス（LBノード）にLB構成を作成します。また、「**ドライラン**」をクリックして、ターゲットインスタンスで作成されるオブジェクトを確認することもできます。作成したStyleBook構成は、ページの構成リストに表示されます。この構成は、NetScaler Console GUIを使用して確認、更新、または削除できます。

オーケストレーション

NetScaler Consoleのオーケストレーション機能を使用すると、NetScalerと統合されたコンテナオーケストレーションプラットフォームを管理できます。サービスグラフに使用されるKubernetesクラスターを監視および管理できます。

以下のトピックは、オーケストレーションの管理に役立ちます。

- クーバネティス

サービスグラフ用のKubernetesクラスターを管理する

Kubernetes (K8s) は、クラウドネイティブアプリケーションのデプロイ、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.

注

- NetScaler Consoleは、Kubernetesバージョン1.14～1.23のサービスグラフ用クラスターの可視性をサポートしています。

NetScaler ConsoleでKubernetes統合の以下の側面を指定できます。

- **クラスター** – NetScaler Consoleがすべてのマイクロサービスを監視し、サービスグラフにデータを入力するKubernetesクラスターを登録または登録解除できます。NetScaler Consoleでクラスターを登録する際は、Kubernetes APIサーバー情報を指定します。その後、Kubernetesクラスターに到達できるエージェントを選択します。

開始する前に

Kubernetesクラスター上のマイクロサービスを監視および視覚化し、サービスグラフを開始するには、以下を準備してください。

- Kubernetesクラスターが準備されていること。
- NetScaler ConsoleとKubernetesクラスターまたは管理対象インスタンス間の通信を可能にするエージェントがインストールおよび構成されていること。データセンターまたはクラウドに存在する管理対象インスタンスを使用できます。
- NetScaler ConsoleにKubernetesクラスターが登録されていること。

NetScalerエージェントを構成してKubernetesクラスターに登録する

KubernetesクラスターとNetScaler Console間の通信を有効にするには、エージェントをインストールして構成する必要があります。エージェントは以下のプラットフォームにデプロイできます。

- ハイパーバイザー (ESX、XenServer®、KVM、Hyper-V)
- パブリッククラウドサービス (Microsoft Azure、AWSなど)

エージェントを構成するには、手順に従ってください。

注

既存のエージェントがすでに展開されている場合は、それを使用することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kubernetesクラスターを管理するために、NetScaler Consoleをシークレットトークンで構成する

NetScaler ConsoleがKubernetesからイベントを受信できるようにするには、NetScaler Console用のサービスアカウントをKubernetesに作成する必要があります。そして、クラスター内で必要なRBAC権限を持つサービスアカウントを構成します。

1. NetScaler Console用のサービスアカウントを作成します。たとえば、サービスアカウント名は`citrixadm-sa`にすることができます。サービスアカウントの作成については、「複数のサービスアカウントを使用する」を参照してください。
2. `cluster-admin`ロールを使用してNetScaler Consoleアカウントをバインドします。このバインディングにより、クラスター全体にわたる`ClusterRole`がサービスアカウントに付与されます。以下は、`cluster-admin`ロールをサービスアカウントにバインドするコマンドの例です。

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   NetScaler Console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 ConsoleにKubernetesクラスターを追加する

エージェントを構成し、静的ルートを構成したら、NetScaler ConsoleにKubernetesクラスターを登録する必要があります。

Kubernetesクラスターを登録するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Orchestration** > **Kubernetes** > **Cluster** 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マスターノードからAPIサーバーURLの詳細を取得できます。

      i. Kubernetesマスターノードで、コマンド `kubectl cluster-info` を実行します。

      ii. 「**Kubernetes master is running at.**」と表示されるURLを入力します。

   c. **認証トークン** - NetScaler Consoleを構成してKubernetesクラスターを管理する際に取得した認証トークン文字列を指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信アクセスを検証するために必要です。認証トークンを生成するには：

      i. Kubernetesマスターノードで、次のコマンドを実行します。

      ```
      kubectl describe secret <token-name>
      ```

      ii. 生成されたトークンをコピーし、認証トークンとして貼り付けます。

      詳細については、Kubernetes ドキュメントを参照してください。

   d. リストからエージェントを選択します。

   e. 「**Create**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® ライセンス

NetScaler Consoleのライセンス機能により、NetScalerライセンスを管理および監視できます。ライセンスのアクティブ化と管理、ベストプラクティスの適用、Flexedライセンスの構成、ライセンスダッシュボードとレポートの表示、およびレガシーライセンスの管理が可能です。

以下のトピックは、NetScalerライセンスの管理に役立ちます。

- ライセンスアクティベーションサービス
- ベストプラクティス
- ライセンス管理
- 最小および最大容量のチェックアウト
- NetScalerエージェントの動作
- Flexedライセンス
- ライセンスの構成
- ライセンスダッシュボード
- ライセンスレポート
- Flexedライセンスへの移行
- Flexedまたはプールされたライセンスの有効期限切れと接続の問題の動作シナリオ
- NetScaler ConsoleサーバーのみをFlexedまたはプールされたライセンスサーバーとして構成する
- レガシーライセンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスアクティベーションサービス

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。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（Citrix Platform License/Universal Hybrid Multi-Cloud）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-prem リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

NetScaler仮想CPUライセンス（Pooled vCPU）、NetScaler VPX Check-In and Check-Out (CICO)、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負う

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ことなくCitrix 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。
LASへの移行を開始する前に、NetScaler向けLAS を読むことをお勧めします。これにより、一般的な前提条件、サポートされているライセンスタイプとサポートされていないライセンスタイプ、特定のライセンスおよび展開タイプに対する正確なワークフロー、その他の重要な情報を理解できます。

License Activation Service (LAS) は、従来のファイルベースのライセンスに代わるクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品をアクティベートするための新しいモジュールを導入し、ライセンス管理に対する合理化された最新のアプローチを提供します。

注:

- LASはライセンスメカニズムであり、ライセンスタイプではありません。
- ファイルベースのライセンスは、手動エンタイトルメントを使用した古いライセンス方法を指します。このドキュメントでは、「ファイルベースのライセンス」と「手動で管理されるエンタイトルメント」は、同じ概念を説明しているため、互換的に使用されます。

LASの主な利点は次のとおりです。

- エンタイトルメントブロブを介した自動エンタイトルメント配信。
- ライセンス通信用の外部エージェントはオプションです。
- LASは、NetScaler MPX™およびSDXインスタンス上のZ-Capソフトウェアライセンスファイルの必要性を排除します。

注：

NetScaler Consoleを初めて使用する場合は、はじめにから始めてください。

次の図は、Consoleサービスを使用したLASのものです。

前提条件

LASを使用するには、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 有効なCitrix Cloudアカウントが必要です。既存のクラウドアカウントまたは新しいクラウドアカウントのオンボーディングの詳細については、アカウント管理を参照してください。
- LASアクティベーションワークフローに使用されるCitrix Cloudアカウントにリンクされている組織ID（Org ID）は、有効な購入済みエンタイトルメントを所有している必要があります。現在のエンタイトルメントを表示するには、エンタイトルメントを参照してください。
- NetScalerインスタンスがLAS互換バージョンを実行していること。
- NetScalerインスタンスは、NetScaler Consoleで管理対象インスタンスとして追加されます。

自動有効化と互換性

LASはNetScaler Consoleサービスで自動的に有効になります。有効になると、すべてのNetScaler FlexedおよびPooledライセンスエンタイトルメントがNetScaler Console GUIに表示されます。

NetScaler Licensing > License management > License Activation Service (LAS) タブに移動して、エンタイトルメントを表示できます。

注：

- 新しい「ライセンスの同期」オプションを使用すると、この同期をオンデマンドで手動でトリガーし、エンタイトルメントを即座に最新の状態に保つことができます。
- エンタイトルメント同期のデフォルトの頻度は、LASエンタイトルメントがNetScaler Consoleサービスと同期されていない場合は8時間ごと、その後は24時間ごとです。オンデマンド同期の場合は、`Sync Now`をクリックします。

LASのNetScalerバージョン互換性

LASを使用するには、NetScalerインスタンスが次のいずれかの最小バージョンを実行している必要があります。

- NetScaler: 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サービス: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- LASを使用するには、以下の前提条件を満たしていることを確認してください。
  - NetScalerインスタンスがLAS互換バージョンで実行されていること。
  - NetScalerインスタンスがNetScaler Consoleに管理対象インスタンスとして追加されていること。
- SDXアプライアンスの場合、Management Service (SVM) をLAS対応ビルドにアップグレードし、LASベースのライセンスに移行してください。VPXビルドバージョンはLAS互換性に影響しません。

ファイルベースのライセンスでは、適用されたエンタイトルメントと構成は、**NetScaler Licensing > License management > Manual License File management** の下に表示されます。

注:

LASは、Flexedライセンス (UHMC/CPL)、プール帯域幅ライセンス、および固定期間帯域幅ライセンスをサポートしています。Pooled vCPUやCICOなど、その他のレガシーNetScalerライセンス形式はLASではサポートされていません。

LASへの移行

NetScaler Licensing > License management > License Activation Service (LAS) に移動すると、NetScaler GUIはNetScalerインスタンスの互換性に基づいて動的に更新されます。

LAS互換バージョンではないNetScalerインスタンスがない場合、GUIにメッセージが表示されます。このメッセージは、NetScalerインスタンスをアップグレードまたは追加するよう促します。

注:

NetScalerインスタンスの一部が互換バージョンにアップグレードされている場合、それらの特定のインスタンスに対してLASを使用できます。

1つ以上のNetScalerインスタンスがLASと互換性がある場合、それらは次の2つのグループのいずれかに分類されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- LASでNetScalerインスタンスをライセンスする
- ライセンスされたNetScalerインスタンスをLASに移行します

GUIは、初めてのLASユーザー（移行されたインスタンスがゼロ）であるか、既存のユーザー（すでに一部のインスタンスをLASに移行しており、さらに追加している）であるかに応じて動的に調整されます。

注:

ライセンス供与またはLASへの移行が完了したら、SVM上のローカルファイルベースライセンスを削除します。ファイルベースライセンスはSVMフォルダー`/mpsconfig/license`にあり、シェルプロンプトを使用してこのフォルダーから削除する必要があります。この注記は、初めてのユーザーと既存のユーザーの両方に対する**LASでのライセンス供与**および**LASへの移行**ワークフローに適用されます。

初めてのLASユーザー

初めてのユーザーには次の画像が表示されます。

LASでNetScalerインスタンスをライセンス供与する

LASでNetScalerインスタンスをライセンス供与するセクションには、現在ライセンスされていないNetScalerインスタンス、またはFlexed帯域幅ライセンスやPooled帯域幅ファイルベースライセンスを使用していないNetScalerインスタンスが一覧表示されます。

インスタンスをライセンス供与するには、次の手順を実行します。

1. **LASでNetScalerインスタンスをライセンス供与する**を選択し、**次へ**をクリックします。
2. インスタンスを選択し、**続行**をクリックします。
3. 詳細を入力し、**送信**をクリックします。 このプロセスを各インスタンスに対して繰り返します。

注:

選択したインスタンスは、SDXインスタンスを除き、ライセンスを有効にするために再起動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既存のライセンスインスタンスをLASに移行する

「**既存のライセンスインスタンスをLASに移行する**」セクションには、FlexedまたはPooledファイルベースライセンスを持つすべてのNetScalerインスタンスが一覧表示されます。これらは次のように分類されます。

- **移行準備ができたインスタンス:** LAS互換バージョンまたはビルドにあり、LASへの移行準備ができたインスタンスを一覧表示します。

移行するには、次の手順を実行します。

```
1.  Select **Migrate your existing licensed NetScaler instances to LAS**
and click **Next**.

2.  Select the instances and click **Migrate**.
```

- **移行前にアップグレードが必要なインスタンス:** 移行前に互換性のあるバージョンまたはビルドにアップグレードする必要があるインスタンスを一覧表示します。

  前提条件:

  LASベースのライセンスを使用するには、NetScalerインスタンスのエディションが、PooledまたはFlexedファイルベースライセンスのエディションと一致している必要があります。移行を開始する前に、インスタンスのエディションを新しいライセンスと一致するように変更してください。

  a. **既存のライセンス済みNetScalerインスタンスをLASに移行する**を選択し、**アップグレード**をクリックします。

  b. **NetScalerのアップグレード**ページで、インスタンスを選択し、インスタンスをLASと互換性のあるバージョンまたはビルドにアップグレードします。

注:

「LASへの移行」ワークフローにあり、レガシーファイルベースからLASベースのPooled帯域幅またはFlexedライセンスに移行するNetScalerインスタンスの場合、再起動は不要です。

既存のLASユーザー

既存のユーザーには次の画像が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既存のLASユーザー(/en-us/netscaler-console-service/media/existing-las-user.png)

注： LASでライセンスされたCPXインスタンスを表示するには、Flexed Dashboard GUIを参照してください。CPXインスタンスは「**LASを使用するNetScalerインスタンス**」の下には表示されません。

LASでNetScalerインスタンスをライセンスする

「**LASでNetScalerインスタンスをライセンスする**」セクションには、現在ライセンスされていない、またはFlexed帯域幅またはPooled帯域幅のファイルベースライセンス以外のライセンスを使用しているNetScalerインスタンスが一覧表示されます。

インスタンスをライセンスするには、次の手順を実行します。

1. 「**License Activation Service (LAS) でライセンスする**」の下で、「**LASでライセンスする**」をクリックします。
2. インスタンスを選択し、「**続行**」をクリックします。
3. 詳細を入力し、「**送信**」をクリックします。

   LASでライセンスする各NetScalerインスタンスについて、この手順を繰り返します。

注：

ライセンスを有効にするには、選択したインスタンスが再起動します。

LASでライセンス(/en-us/netscaler-console-service/media/las-existing.png)

ライセンスされたNetScalerインスタンスをLASに移行する

「**ライセンスされたNetScalerインスタンスをLASに移行する**」セクションには、FlexedまたはPooledのファイルベースライセンスを持つすべてのNetScalerインスタンスが一覧表示されます。これらは次のように分類されます。

- **LAS内のインスタンス**：LASベースのライセンスをすでに使用しているインスタンスを一覧表示します。
- **移行準備ができたインスタンス**: 移行準備ができた互換性のあるインスタンスを一覧表示します。

  移行するには、次の手順を実行します。

  a. **ライセンスされたNetScalerインスタンスをLASに移行**を選択し、**移行**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 1つ以上のNetScalerインスタンスを選択し、選択したインスタンスをLASに移行します。

- **移行前にアップグレードが必要なインスタンス:** 互換性のあるバージョンにアップグレードする必要があるインスタンスを一覧表示します。アップグレードするには、次の手順を実行します。

  前提条件:

  LASベースのライセンスを使用するには、NetScalerインスタンスのエディションが、プールまたはフレックスライセンスのエディションと一致している必要があります。移行を開始する前に、インスタンスのエディションを新しいライセンスと一致するように変更してください。

  a. **ライセンスされたNetScalerインスタンスをLASに移行**を選択し、**アップグレード**をクリックします。

  b. 1つ以上のNetScalerインスタンスを選択し、インスタンスを互換性のあるバージョンまたはビルドにアップグレードします。

注:

「LASへの移行」ワークフローにあり、レガシーのファイルベースからLASベースのプール帯域幅またはフレックスライセンスに移行するNetScalerインスタンスの場合、再起動は不要です。

LASライセンスワークフロー中にLASに送信される情報

このセクションでは、初回リクエストごと、および各LASアクティベーションブロブ更新リクエスト中に、アクティベーションブロブのLASへのリクエストの一部として送信されるすべての情報について詳しく説明します。 次の表は、ライセンスワークフロー中にLASに送信されるパラメーターをまとめたものです。

パラメーター	説明	LASワークフローにおける必要性
エルエスジーユーアイディー	Consoleサービステナントの一意のID	LASバインディングパラメータ
エルエスアイディー	Consoleサービステナントの一意のID	LASバインディングパラメータ
パブキー	Consoleサービスデプロイメントの公開キー	LASがこのConsoleを承認していることを保証します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター	説明	LASワークフローにおける必要性
シーシーアイディー	Consoleサービスをオンボーディングするために使用されるCitrix Cloud ID	LASバインディングパラメータ
エルエスビルド	ビルドバージョンまたはサンプル値	LASアクティベーション要件
ホスト名	コンソールサービスホスト名(POP名)	LASアクティベーション要件
エルピーイーID	アクティベートされるNetScalerの一意のID。	LASバインディングパラメータ
エルピーイーホスト名	アクティベートされるNetScalerのホスト名	LASバインディングパラメータ
burnin_date	NetScalerのソフトウェアバーンイン日付	LASバインディングパラメータ
製品	アクティベーションライセンスを生成するためにLASが検証する機能	LASエンタイトルメント検証パラメータ

LASに移行したNetScaler Consoleサービス環境を監視するためのベストプラクティス

このドキュメントでは、LASを使用するNetScaler環境を監視するために従うことができるベストプラクティスに焦点を当てています。このドキュメントは、ConsoleサービスでLASを使用する展開に適用されます。

前提条件

- NetScaler用LAS ページを読み、ConsoleサービスでのLASに関するFAQを含めてください。
- ライセンスアクティベーションサービス を読み、LAS移行を完了してください。
- 関連する通知を設定し、NetScaler GUIとCLIを定期的に監視するようにしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

Citrixは通知の継続的な改善を行い、このドキュメントもそれに応じて更新していく予定です。

LASアクティベーションBLOBの有効期限の監視

NetScaler Consoleサービスの場合、LASアクティベーションBLOBは、NetScaler Consoleサービスをライセンスサーバーとして使用するNetScalerインスタンスにLASから直接提供されます。このBLOBは30日間、またはライセンスエンタイトルメントの有効期限が切れるまでのいずれか早い方まで有効で、8時間ごとに更新されます。

NetScalerとNetScaler Consoleサービス間の接続が切断されると、NetScaler ConsoleサービスはNetScalerインスタンスのLASアクティベーションBLOBを更新できません。NetScaler Consoleサービスは8時間ごとに再試行し、3回の失敗（8時間 x 3 = 24時間）の後、NetScalerは**猶予**ステータスになります。NetScaler ConsoleサービスのGUIは、そのようなNetScalerインスタンスを猶予ステータスで表示します。

このセクションでは、LASアクティベーションBLOBの有効期限が近づいている（30日未満）場合にトリガーされる通知について詳しく説明します。これは、展開に注意が必要であることを示しています。これを解決するには、接続の問題を確認して修復するか、Citrixサポートに連絡して支援を受けてください。

GUIを使用してNetScalerインスタンスを表示する

猶予ステータスにあるNetScalerインスタンスを表示するには、**Console Service GUI > NetScaler Licensing > Flexed Licensing > Dashboard** に移動します。

CLIを使用してNetScalerインスタンスのステータスを表示する

GraceステータスのNetScalerインスタンスと残りのグレース期間を表示するには、`sh licenseserver`コマンドを実行します。

例:

```
> sh licenseserver

     License Server: 10.102.123.31 Status: Disconnected

        Grace: Yes         Grace Time Left: 652
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Done
```

通知

NetScaler Consoleサービス上のバナー:

NetScaler ConsoleサービスGUIには、LASアクティベーションブロブがx日後に期限切れになるNetScalerインスタンスを一覧表示するバナーが表示されます（xは30日未満）。

NetScaler Consoleサービス上のバナー(/en-us/netscaler-console-service/media/blob-service-gui-banner.png)

NetScaler GUI上のバナー:

NetScalerインスタンスがグレースステータスの場合、NetScaler ConsoleサービスGUIにバナーが表示されます。

NetScaler GUI上のバナー(/en-us/netscaler-console-service/media/blob-gui-banner.png)

グレースステータスの場合にNetScalerによって生成されるSNMPトラップ:

NetScalerインスタンスがグレースステータスの場合、NetScalerは次のSNMPトラップを生成します。

- `pooledLicenseGraceStarted`: インスタンスがグレース期間に入ったときにトリガーされます。
- `pooledLicenseGraceNormal`: 30日間のグレース期間が終了したときにトリガーされます。これは、デプロイメントに影響があり、インスタンスがライセンスなしになることを意味します。
- `pooledLicenseGracePeriodOver`: グレース期間が終了したときにトリガーされます。

例：

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceStarted
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceNormal
(nsPartitionName = default)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGracePeriodOver
(nsPartitionName = default)
```

ライセンスエンタイトルメントの有効期限切れの監視

ライセンスエンタイトルメントの有効期限は、顧客のライセンスエンタイトルメントまたは契約の有効期限を指します。

GUI を使用してライセンスエンタイトルメントの有効期限情報を表示するには、**Console Service GUI > NetScaler Licensing > License Management > LAS** に移動します。

有効期限までの日数には、対応するライセンスのエンタイトルメントの有効期限が表示されます。

通知

NetScaler Console service GUI のバナー表示：

NetScaler Console service GUI には、ライセンスエンタイトルメントの有効期限が x 日後に近づいていることを示すバナーが表示されます。

メールベースの通知：

ライセンスエンタイトルメントの有効期限に関する通知を設定するには：

1. 以下のパスに沿って移動します：**Console Service GUI > NetScaler Licensing > License Management > Notification Settings.**
2. **ライセンスの有効期限が切れる何日前に通知を受け取りますか？** に必要な値を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンス管理

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026 にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026 以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASになり、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026 をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026 までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026 までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他の従来のNetScalerライセンスはすべてLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

負うことなくCitrix 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。

LASベースのライセンス

License Activation Service (LAS) を使用すると、エンタイトルメントがNetScaler Console UIに自動的に反映されるため、手動での操作は不要です。

ライセンスサーバーポート

LAS は、すべてのライセンス通信にポート 443 を使用します。

注:

LAS を使用するには、NetScaler インスタンスを管理対象インスタンスとして追加します。

ライセンスの有効期限情報

ライセンスの有効期限を表示

1. **NetScaler Licensing > License Management** に移動します。
2. **License entitlement expiry information** セクションには、有効期限が近づいているライセンスの詳細が表示されます。
   - **機能**: 有効期限が切れるライセンスの種類。
   - **カウント**: 影響を受けるインスタンスの数、または帯域幅 (Mbps)。
   - **有効期限までの日数**: ライセンスの有効期限 (契約終了日) までの日数。

注:

新しく購入したプールまたはフレックスのエンタイトルメントは、**License entitlement expiry information** セクションに自動的に表示されます。

ライセンスの有効期限切れの動作

NetScaler Console を介して管理されているライセンスの有効期限が切れると、関連する NetScaler インスタンスはトラフィックの処理を停止し、その構成が失われる可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンス終了日の通知メールとポップアップバナー

NetScaler Console GUI に、ライセンス終了日に関するポップアップメッセージが表示されます。デフォルトでは、ライセンス終了日の30日前（デフォルト）から、GUI にポップアップメッセージ（ログイン後毎回）が表示されます。日数は、 **>** で設定できます。

管理者として、 でメール通知が設定されている場合、ライセンス終了日の通知メールも受信します。通知メールは、ライセンス終了日の60日前、30日前、20日前、10日前の頻度で送信されます。

通知設定

LAS で管理されている Flexed または Pooled ライセンスの有効期限に関する通知を設定するには、次の手順に従います。

1. **NetScaler ライセンス > ライセンス管理 > 通知設定** に移動します。
2. セクションで、 を選択します。通知を送信するために割り当てる Flexed または Pooled ライセンス容量の割合として、アラートしきい値を設定します。
3. ライセンスがしきい値に達したとき、または有効期限が近づいているときに送信する通知の種類を、適切なチェックボックスをオンにして選択します。通知の種類は次のとおりです。
   - : 通知を送信するためのメールプロファイルまたは配布リスト。詳細については、「メール配布リストの作成」を参照してください。
   - : 通知を送信するための Slack プロファイルの詳細。
   - : 通知を送信するための PagerDuty プロファイル。
   - : Citrix ServiceNow プロファイルはデフォルトで指定されており、利用可能な唯一のオプションです。 これらのプロファイルの作成の詳細については、「通知の構成」を参照してください。
   - 通知の種類を選択し、 をクリックして詳細を追加します。設定を保存する前に、各通知システムをテストすることもできます。
4. を指定します。これは、ライセンスの有効期限について通知を受けたい日数です。
5. をクリックします。

メール配信リストを作成する

メール配信リストを作成するには、次の手順を実行します。

1. を選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. で、次の詳細を指定します。

   - - 配信リスト名を指定します。
   - - NetScaler Console がメッセージを送信するメールアドレスを指定します。
   - - NetScaler Console がメッセージをコピーするメールアドレスを指定します。
   - - NetScaler Console がメッセージをブラインドカーボンコピーする（メールアドレスを表示しない）メールアドレスを指定します。

3. をクリックします。

Slack プロファイルを作成する

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. で、 をクリックします。
2. で、次の詳細を指定します。

   - - 有効にすると、アラートとイベント通知が指定された Slack チャネルに直接送信されます。
   - **添付ファイル付き通知** - 有効にすると、トリガーされたアラートとイベントに関する詳細情報が、電子メールの添付ファイルまたはWebhook内のJSONペイロードとして送信されます。
   - **プロファイル名** - プロファイル名を指定します。この名前はSlackのプロファイルリストに表示されます。
   - **チャネル名** - NetScaler Consoleが通知を送信するSlackチャネル名を指定します。
   - **Webhook URL** - チャネルのWebhook URLを指定します。受信Webhookは、外部ソースからSlackにメッセージを投稿する簡単な方法です。URLは内部的にチャネル名にリンクされています。このURLに送信されるすべてのイベント通知は、指定されたSlackチャネルに投稿されます。Webhookの例は次のとおりです。`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`。

PagerDutyプロファイルの作成

PagerDutyを使用すると、登録済みの番号で電子メール、プッシュ通知、電話を介して通知を設定できます。NetScaler ConsoleにPagerDutyプロファイルを追加する前に、PagerDutyで必要な設定が完了していることを確認してください。PagerDutyの使用を開始するには、PagerDutyのドキュメントを参照してください。

PagerDutyプロファイルを作成するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **PagerDuty**で、**追加**をクリックします。
2. **PagerDutyプロファイルの作成**で、次の詳細を指定します。
   - **プロファイル名** - プロファイル名を指定します。この名前は、イベントルールやSSL通知などのさまざまなモジュールでPagerDutyアラートを送信するために使用されます。
   - **統合キー** - 統合キーを指定します。このキーはPagerDutyポータルから取得できます。PagerDutyで統合用のサービスを作成する際は、**Generic Events API Integration**オプションを使用してください。
3. **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。

ServiceNowプロファイルの表示

NetScalerイベントのServiceNow通知を有効にするには、ITSMコネクタを使用してNetScaler ConsoleをServiceNowと統合する必要があります。詳細については、NetScaler ConsoleとServiceNowインスタンスの統合を参照してください。

ServiceNowプロファイルを表示および確認するには、次の手順を実行します。

1. **ServiceNow**では、**Citrix_Workspace_SN**プロファイルがデフォルトで選択されています。
2. **Test**をクリックして、ServiceNowチケットを自動生成し、構成を確認します。

注

> NetScalerライセンスのさまざまな種類については、「ライセンスの概要」を参照してください。

LASのRBACサポート

ロールベースのアクセス制御 (RBAC) を使用して、次の制御レベルでLASアプリケーションアクセスを管理できます。

- **機能レベル**: 特定の管理者に対してライセンス機能の可視性を制限します。
- **インスタンスレベル**: 承認された管理者が選択したNetScalerインスタンスにのみライセンスを適用できるように制限します。

構成の詳細については、「ロールベースのアクセス制御」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

手動で管理されるエンタイトルメント (ファイルベースのライセンス)

以下のセクションは、手動で管理されるエンタイトルメント (ファイルベースのライセンス) に適用されます。

注:

Universal Hybrid Multi-Cloud (UHMC) またはCitrix Platform License (CPL) を購入すると、提供されるNetScalerライセンスはFlexedライセンスと呼ばれます。詳細については、「UHMC/CPLの提供」を参照してください。

ライセンスファイル

NetScaler Flexedライセンスには、MyCitrixポータルからダウンロードする必要がある次のファイルが含まれています。現在のNetScalerライセンスの種類からFlexedライセンスへの移行の詳細については、「Flexedライセンスへの移行」を参照してください。

NetScalerに存在するライセンスファイルは、このセクションに記載されています。

ファイル名に含まれるもの	説明	ダウンロード情報	ライセンスのアップロード/適用先
NetScaler Flexed VPX SWインスタンス	VPX/CPX/BLXソフトウェアインスタンスの利用を許可します	NetScaler ConsoleホストIDを使用してこのファイルをダウンロードします	ネットスケーラー コンソール上
NetScaler Flexed MPX SWインスタンス	MPXソフトウェアインスタンスの利用を許可します	NetScaler ConsoleホストIDを使用してこのファイルをダウンロードします	ネットスケーラー コンソール上
NetScaler Flexed SDX SWインスタンス	SDXソフトウェアインスタンスの利用権を付与します。	NetScaler ConsoleホストIDを使用してこのファイルをダウンロードします。	ネットスケーラー コンソール上
ネットスケーラー フレックス プラチナ BW	Flexed Platinumスループット容量の利用権を付与します。	NetScaler ConsoleホストIDを使用してこのファイルをダウンロードします。	ネットスケーラー コンソール上

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ファイル名に含まれるもの	説明	ダウンロード情報	ライセンスのアップロード/適用先
NetScaler Flexed VPX FIPS SWインスタンス	VPX FIPSソフトウェアインスタンスの利用権を付与します。	NetScaler ConsoleホストIDを使用してこのファイルをダウンロードします。	ネットスケーラー コンソール上
Zero Capacity MPX-Zプラットフォームライセンス	NetScaler MPX HW/ NetScaler MPX FIPS HWをFlexedライセンスに参加させる権利を付与します。	このファイルをダウンロードします。	NetScaler MPX上
ゼロキャパシティ SDX-Z プラットフォームライセンス	NetScaler SDX HW/ NetScaler SDX FIPS HW を Flexed ライセンスに参加させる権利を与えます	このファイルをダウンロードします	NetScaler SDX 上で

注意すべき重要な点

- 複数のNetScaler Consoleサービステナント、または複数のNetScaler Consoleオンプレミスインスタンスにライセンスをアップロードできます。
- プールライセンスからFlexedライセンスへ移行しており、MPXおよびSDXインスタンスにすでにZ-Cap永続ライセンスが適用されている場合、Flexedライセンスとともに受け取ったZ-Capライセンスを適用する必要はありません。ただし、NetScaler MPXまたはNetScaler SDXに適用されている現在のZ-Capライセンスが特定の期間有効である場合は、Flexedライセンスとともに受け取ったZ-Capライセンスを適用する必要があります。
- Flexedライセンスの一部として提供されるMPX-ZまたはSDX-Zプラットフォームライセンスは永続的です。特定のインスタンスにMPX-ZまたはSDX-Zプラットフォームライセンスファイルが適用された後、そのインスタンスのライフサイクル終了 (EOL) まで使用できます。
- デプロイメントで使用しているNetScalerフォームファクターに対して、NetScaler ConsoleでFlexedライセンスを適用する必要があります。例:

  NetScaler SDXフォームファクターを使用している場合は、以下のライセンスを適用します。

  |ライセンスファイル|適用先| |-|-| |NetScaler Flexed SDX SW インスタンス|ネットスケーラー コンソール| |NetScaler Flexed VPX SW インスタンス|ネットスケーラー コンソール| |ネットス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ケーラー フレックスド プラチナ BW|ネットスケーラー コンソール| |ADC ゼロキャパシティ SDX-Z プラットフォーム|NetScaler SDX|

NetScaler MPX フォームファクターを使用している場合は、次のライセンスを適用します。

|ライセンスファイル|適用先| |-|-| |ネットスケーラー フレックスド MPX SW インスタンス|ネットスケーラー コンソール| |ネットスケーラー フレックスド プラチナ BW|ネットスケーラー コンソール| |ADC ゼロキャパシティ MPX-Z プラットフォーム|NetScaler MPX|

NetScaler VPX、NetScaler BLX、または NetScaler CPX フォームファクターを使用している場合は、次のライセンスを適用します。

|ライセンスファイル|適用対象| |-|-| |NetScaler Flexed VPX SWインスタンス|NetScaler コンソール| |ネットスケーラー フレックスド プラチナ BW|NetScaler コンソール|

NetScaler VPX FIPSフォームファクターを使用している場合は、以下のライセンスを適用してください

|ライセンスファイル|適用対象| |-|-| |NetScaler Flexed VPX FIPS SWインスタンス|NetScaler コンソール| |ネットスケーラー フレックスド プラチナ BW|NetScaler コンソール|

ライセンスファイルを適用する

ライセンスの追加、削除、ダウンロードが可能です。ライセンスを使用する前に適用する必要があります。

1. 「**NetScaler Licensing > License Management**」に移動します。
2. 「**License Files**」セクションで、「**Add License File**」をクリックし、次のいずれかのオプションを選択します。
   - **ローカルコンピューターからライセンスファイルをアップロード**: ライセンスファイルがすでにローカルコンピューターにある場合は、NetScaler Consoleにアップロードできます。
   - **ライセンス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。「**Get Licenses**」をクリックし、次に「**Finish**」をクリックします。
3. 「Finish」をクリックします。 ライセンスファイルがNetScaler Consoleに追加されます。「**License Expiry Information**」セクションには、NetScaler Consoleに存在するライセンス、その数、および有効期限までの残り日数が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> ライセンスの終了日は、契約が有効である日付であり、その終了日までに更新する必要があります。

次のスクリーンショットは、Flexed NetScaler VPX、NetScaler MPX、NetScaler SDX、およびNetScaler VPX FIPSソフトウェアインスタンスライセンスの数、存在するFlexedプレミアム帯域幅容量、および有効期限までの日数（契約終了日）を示しています。

次のスクリーンショットは、利用可能なPooled Standard、Advanced、およびPremium帯域幅と、有効期限までの日数（契約終了日）を示しています。

4. ライセンスファイルを選択し、「**Apply licenses**」をクリックします。

ライセンスファイルを削除する

ライセンスファイルを削除するには、1つ以上のファイルを選択し、「**Delete**」をクリックします。ライセンスを削除する場合、まずライセンスを追加し、その後でのみ適用できます。

ライセンスファイルをダウンロードする

ライセンスファイルをダウンロードするには、ファイルを選択し、**ダウンロード**をクリックします。ライセンスファイルをオフラインでバックアップとして保存できます。

ライセンスサーバーのポート設定

ポートは、NetScalerインスタンスがライセンスサーバーと通信するために使用されます。**編集**アイコンをクリックし、次のパラメーターの値を指定します。

- **ライセンスサーバーポート**: NetScalerインスタンスがライセンス割り当てのためにCitrixライセンスポータルにアクセスするために使用するプロキシサーバーポート。デフォルト値: 27000。
- **ベンダーデーモンポート**: NetScalerインスタンスがライセンスサーバーと通信するために使用するライセンスサーバーポート。デフォルト値: 7279。

ライセンスの有効期限情報

フレックスまたはプールされたキャパシティライセンスのライセンス有効期限しきい値を構成できます。しきい値が設定されている場合、ライセンスの有効期限が近づくと、NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は電子メールで通知を送信します。ライセンスがNetScaler Consoleで期限切れになった場合も、SNMPトラップと通知が送信されます。

ライセンス有効期限通知が送信されるとイベントが生成され、このイベントはNetScaler Consoleの**インフラストラクチャ > イベント**から表示できます。

ライセンスの有効期限を表示

1. **NetScaler Licensing > License Management**に移動します。
2. **ライセンス設定**ページで、**ライセンス有効期限情報**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（契約終了日）までの日数。

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。

ライセンス終了日の通知メールとポップアップバナー

NetScaler Console GUIでは、ライセンス終了日に関するポップアップメッセージが表示されます。管理者として、ライセンス終了日の通知メールも受信します。デフォルトでは、ライセンス終了日の60日前にGUIにポップアップメッセージ（ログイン後毎回）が表示され、ライセンス終了日の60、30、20、10日前に通知メールが届きます。

ライセンスの有効期限切れの動作

NetScaler Consoleを通じて管理されている、有効期限が切れたライセンスを持つNetScalerインスタンスは、トラフィックの処理を停止し、構成の損失につながる可能性があります。

通知設定

ライセンスの割り当てと有効期限までの日数に関する通知が送信される設定を指定します。

1. 「**通知設定**」セクションで、「**編集**」アイコンをクリックし、「**ライセンス使用状況を通知する**」を選択します。通知を送信するために割り当てられる、フレックスまたはプールされたライセンス容量の割合としてアラートしきい値を設定します。
2. 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そうなときに送信する通知の種類を、適切なチェックボックスを選択して選びます。通知の種類は次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **メール**: 通知を送信するためのメールプロファイルまたは配布リスト。詳細については、「メール配布リストの作成」を参照してください。
- **Slack**: 通知を送信するためのSlackプロファイルの詳細。
- **PagerDuty**: 通知を送信するためのPagerDutyプロファイル。
- **ServiceNow**: Citrix ServiceNowプロファイルはデフォルトで指定されており、利用可能な唯一のオプションです。 これらのプロファイルの作成の詳細については、「通知の構成」を参照してください。

通知の種類を選択し、**追加**をクリックして詳細を追加します。設定を保存する前に、各通知システムをテストすることもできます。

3. **有効期限までの日数**を指定します。これは、ライセンスの有効期限について通知を受けたい日数です。
4. 「**保存**」をクリックします。

メール配信リストを作成する

メール配信リストを作成するには、次の手順を実行します。

1. 「**メール**」を選択し、「**追加**」をクリックします。
2. 「**メール配信リストの作成**」で、次の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **メールサーバー** - メール通知を送信するメールサーバーを選択します。メールサーバーを追加するには、「追加」をクリックします。サーバー名/IPアドレスとポートを指定します。メールサーバーへのアクセスに認証を必須にするには、「認証」を選択します。メールサーバーがSSL認証をサポートしている場合は、「セキュア」を選択します。「作成」をクリックします。
   - **差出人** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
   - **宛先** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
   - **CC** - NetScaler Consoleがメッセージをコピーするメールアドレスを指定します。
   - **BCC** - NetScaler Consoleがメッセージをブラインドカーボンコピー（メールアドレスは表示されません）するメールアドレスを指定します。
3. 「**作成**」をクリックします。

Slackプロファイルを作成する

Slack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. 「**Slack**」で、「**追加**」をクリックします。
2. 「**Slackプロファイルの作成**」で、次の詳細を指定します。

   - **プロファイル名** - プロファイル名を指定します。この名前はSlackプロファイルリストに表示されます。
   - **チャネル名** - NetScaler Consoleが通知を送信するSlackチャネル名を指定します。
   - **Webhook URL** - チャネルのWebhook URLを指定します。受信Webhookは、外部ソースからのメッセージを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。このURLに送信されるすべてのイベント通知は、指定されたSlackチャネルに投稿されます。Webhookの例は次のとおりです: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`。

PagerDutyプロファイルの作成

PagerDutyを使用すると、登録された番号への電子メール、プッシュ通知、電話による通知を設定できます。NetScaler Consoleで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のドキュメントを参照してください。

PagerDutyプロファイルを作成するには、次の手順を実行します。

1. 「**PagerDuty**」で「**追加**」をクリックします。
2. 「**PagerDutyプロファイルの作成**」で、次の詳細を指定します。

   - **プロファイル名** - プロファイル名を指定します。この名前は、イベントルールやSSL通知などのさまざまなモジュールでPagerDutyアラートを送信するために使用されます。
   - **統合キー** - 統合キーを指定します。このキーはPagerDutyポータルから取得できます。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てください。

3. 「**作成**」をクリックします。

詳細については、PagerDutyのドキュメントにある「サービスと統合」を参照してください。

ServiceNowプロファイルの表示

NetScalerイベントのServiceNow通知を有効にするには、ITSMコネクタを使用してNetScaler ConsoleをServiceNowと統合する必要があります。詳細については、「NetScaler ConsoleとServiceNowインスタンスの統合」を参照してください。

ServiceNow プロファイルを表示および確認するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **ServiceNow** では、**Citrix_Workspace_SN** プロファイルがデフォルトで選択されています。
2. **Test** をクリックして ServiceNow チケットを自動生成し、構成を確認します。

注:

NetScaler ライセンスのさまざまな種類の詳細については、ライセンスの概要 を参照してください。

チェックアウトの最小および最大容量

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-prem リリース14.1-51.x以降および13.1-60.x以降から非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScaler Flexedライセンスは、ライセンスサーバーとして構成されたNetScaler Consoleを使用して、Flexedライセンス（帯域幅プールライセンスとインスタンスプールライセンス）を管理します。

帯域幅プールおよび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、ゼロ容量ハードウェア上のNetScalerフォームファクターとハードウェアモデル番号によって、以下が決定されます。

- NetScalerインスタンスが機能する前にチェックアウトする必要がある最小帯域幅とインスタンス数。
- NetScalerがチェックアウトできる最大帯域幅とインスタンス数。
- 各帯域幅チェックアウトの最小帯域幅単位。最小帯域幅単位とは、NetScalerがプールからチェックアウトする必要がある帯域幅の最小単位です。すべてのチェックアウトは、最小帯域幅単位の整数倍である必要があります。たとえば、NetScalerの最小帯域幅単位が1 Gbpsの場合、1000 Mbpsはチェックアウトできますが、200 Mbpsや150.5 Gbpsはチェックアウトできません。最小帯域幅単位は、最小帯域幅要件とは異なります。NetScalerインスタンスは、少なくとも最小帯域幅でライセンスが付与された後にのみ動作できます。最小帯域幅が満たされると、インスタンスは最小帯域幅単位の倍数でより多くの帯域幅をチェックアウトできます。

表1から5は、サポートされているすべてのNetScalerインスタンスの最大帯域幅/インスタンス数、最小帯域幅/インスタンス数、および最小帯域幅単位をまとめたものです。表6は、サポートされているすべてのNetScalerインスタンスの異なるフォームファクタに対するライセンス要件をまとめたものです。以下の表はシステム要件を示しています。

注:

NetScaler CPX/BLX/VPX の最小帯域幅チェックアウト単位は 10 Mbps です。NetScaler MPX/SDX の最小帯域幅チェックアウト単位は 1 Gbps です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表1. MPXでサポートされるFlexed容量

製品ライン	最小帯域幅 (GBPS)	最大帯域幅 (GBPS)	最小帯域幅単位
MPX 5900Z	1	10	1 ギガbps
MPX 8900Z	5	30	1 ギガビット/秒
MPX 8900Z FIPS	5	20	1 ギガビット/秒
MPX 9100Z	10	95	1 ギガビット/秒
MPX 9100Z FIPS	10	95	1 ギガビット/秒
MPX 14000Z	20	100	1 ギガビット/秒
MPX 14000Z-40G	20	100	1 ギガビット/秒
MPX 14000Z-40S	40	100	1 ギガビット/秒
MPX 14000Z FIPS	30	80	1 ギガbps
MPX 15000Z	20	120	1 ギガbps
MPX 15000Z-50G	20	120	1 ギガbps
MPX 15000Z FIPS	30	120	1 ギガbps
MPX 16000Z	30	250	1 ギガビット/秒
MPX 22000Z	40	120	1 ギガビット/秒
MPX 24000Z	100	150	1 ギガビット/秒
MPX 25000Z	100	160	1 ギガビット/秒
MPX 25000Z-40G	100	200	1 ギガビット/秒
MPX 26000Z	100	200	1 ギガビット/秒
MPX 26000Z-50S	100	200	1 ギガビット/秒
MPX 26000Z-100G	100	200	1 ギガビット/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表2A。ビルド13.0-47.xより前のNetScaler SDXバージョンでサポートされるFlexed容量

製品ライン	最小帯域幅 (GBPS)	最大帯域幅 (GBPS)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 8900Z	10	30	2	7	1 ギガビット/秒
SDX 14000Z	20	100	5	25	1ギガビット/秒
SDX 14000Z-40G	40	100	20	25	1ギガビット/秒
SDX 15000Z	20	120	5	55	1 ギガbps
SDX 15000Z-50G	20	120	5	55	1 ギガbps
SDX 22000Z	40	120	80	80	1 ギガbps
SDX 24000Z	100	150	80	80	1 ギガビーピーエス
SDX 25000Z	100	200	20	115	1 ギガビーピーエス
SDX 25000Z-40G	100	200	20	115	1 ギガビット/秒
SDX 26000Z	100	200	20	115	1 ギガビット/秒
SDX 26000Z-50S	100	200	20	115	1 ギガビット/秒
SDX 26000Z-100G	100	200	20	115	1 ギガビーピーエス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表 2B. NetScaler SDX バージョン 13 (ビルド 13.0-47.x 以降)、バージョン 13.1 (ビルド 51.x より前)、およびバージョン 14.1 (ビルド 12.x より前) でサポートされるFlexed容量

製品ライン	最小帯域幅 (GBPS)	最大帯域幅 (GBPS)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 8900Z	5	30	1	7	1ギガビット/秒
SDX 9100Z	10	95	2	7	1ギガビット/秒
SDX 14000Z	10	100	2	25	1ギガビット/秒
SDX 14000Z-40G	20	100	10	25	1 ギガビット/秒
SDX 15000Z	10	120	2	55	1 ギガビット/秒
SDX 15000Z-50G	10	120	2	55	1 ギガビーピーエス
SDX 16000Z	15	250	10	55	1 ギガビーピーエス
SDX 22000Z	20	120	40	80	1 ギガビーピーエス
SDX 24000Z	50	150	40	80	1 ギガbps
SDX 25000Z	50	200	10	115	1 ギガbps
SDX 25000Z-40G	50	200	10	115	1 ギガビット/秒
SDX 26000Z	50	200	10	115	1 ギガビット/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

製品ライン	最小帯域幅 (GBPS)	最大帯域幅 (GBPS)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 26000Z-50S	50	200	10	115	1 ギガビット/秒
SDX 26000Z-100G	50	200	10	115	1 ギガビット/秒

表2C. NetScaler SDX バージョン 13.1 (ビルド 51.x 以降) およびバージョン 14.1 (ビルド 12.x 以降) のサポートされるFlexed容量

製品ライン	最小帯域幅 (GBPS)	最大帯域幅 (GBPS)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 8900Z	5	30	1	7	1 ギガビット/秒
SDX 9100Z	10	95	1	7	1 ギガビット/秒
SDX 14000Z	10	100	1	25	1 ギガビット/秒
SDX 14000Z-40G	20	100	1	25	1 ギガビット/秒
SDX 15000Z	10	120	1	55	1 ギガビット/秒
SDX 15000Z-50G	10	120	1	55	1 ギガビット/秒
SDX 16000Z	15	250	1	55	1 ギガビット/秒
SDX 22000Z	20	120	1	80	1 ギガビット/秒
SDX 24000Z	50	150	1	80	1ギガビーピーエス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

製品ライン	最小帯域幅 (GBPS)	最大帯域幅 (GBPS)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
SDX 25000Z	50	200	1	115	1ギガビーピーエス
SDX 25000Z-40G	50	200	1	115	1 ギガビット/秒
SDX 26000Z	50	200	1	115	1 ギガビット/秒
SDX 26000Z-50S	50	200	1	115	1 ギガビット/秒
SDX 26000Z-100G	50	200	1	115	1ギガbps

注記:

- 最小購入数量は、最小システム要件とは異なる場合があります。
- ビルド14.1-12.x以降を実行しているNetScaler SDXでは、Flexedライセンスを使用すると、インスタンスライセンスの最小数をチェックアウトするという制限がなくなります。つまり、最小1つのインスタンスライセンスをチェックアウトできます。

表 3. NetScaler CPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

製品ライン	最大帯域幅 (GBPS)	最小帯域幅 (MBPS)	最小インスタンス数	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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表4. ハイパーバイザーおよびクラウドサービス上のNetScaler VPXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

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	最大インスタンス	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 ギガビット/秒	10 メガビット/秒	1	1	10 メガビット/秒
AWS	30 ギガビット/秒	10 メガビット/秒	1	1	10 メガビット/秒
アジュール	10ギガビット/秒	10メガビット/秒	1	1	10 メガビット/秒
グーグル クラウド	10 ギガビット/秒	10 メガビット/秒	1	1	10 メガビット/秒

注

最小購入数量は、最小システム要件とは異なります。

表5. NetScaler BLXインスタンスでサポートされる最小/最大帯域幅と最小/最大インスタンス

製品ライン	最大帯域幅 (GBPS)	最小帯域幅 (MBPS)	最小インスタンス数	最大インスタンス数	最小帯域幅単位
BLX	100	10	1	1	10 メガビット/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表6. 異なるフォームファクターのゼロキャパシティライセンス要件

製品ライン	ゼロキャパシティハードウェア
MPX	ライセンスが必要
SDX	ライセンスが必要
VPX	-
CPX	-
BLX	-

NetScalerエージェントの動作

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、NetScalerインスタンスをアクティベートしてライセンスを付与する唯一の方法はLASになり、NetScaler Flexedライセンス（Citrix Platform License/Universal Hybrid Multi-Cloud）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console オンプレミス のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console オンプレミス リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console オンプレミス リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

センスを引き続き使用できます。ただし、Console オンプレミス 13.1はLASをサポートしていないため、15th April 2026までにConsole オンプレミス リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

NetScaler仮想CPUライセンス（Pooled vCPU）、NetScaler VPX Check-In and Check-Out (CICO)、永続ライセンスなど、その他のすべての従来のNetScalerライセンスは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。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScalerエージェントは、NetScaler Consoleと、さまざまなデータセンターおよびパブリッククラウド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。NetScaler Consoleサービスでは、FlexedまたはPooledライセンスが機能するために、テナントごとに最低1つのエージェントが必要です。サイトごとまたはマルチサイトで複数のNetScalerエージェントを展開できますが、テナント全体の展開に対してLicense Server Agent (LSA) の役割を持つことができるエージェントは1つだけです。

LASベースのライセンス

LASベースのライセンスを使用する場合、NetScaler内の組み込みエージェントがライセンス通信を処理します。外部エージェントは、ライセンス通信のプロキシとして機能するようにアーキテクチャ内に展開できるオプションコンポーネントです。

LAS 用の NetScaler 組み込みエージェントを構成するには、インスタンスを管理するための組み込みエージェントを構成するを参照してください。

エージェントのフェールオーバーを有効にするには、netscaler-console-service/getting-started/initiate-built-in-agentを参照してください。

注:

組み込みエージェントを使用している場合、LAS ベースのライセンスへの移行は NetScaler Console GUI を介してのみ可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

手動で管理されるエンタイトルメント (ファイルベースのライセンス)

LSA は、NetScaler Console サービスベースのプールライセンス展開でライセンスサーバーとして機能するエージェントです。LSA がダウンした場合、サービスは新しい LSA を選出するために 24 時間待機します。

それまでは、プールライセンスまたはフレックスライセンスを使用している NetScaler インスタンスは猶予期間に入ります。管理者として、LSA を手動で選出することもできます。

次の例は、2つのエージェントが展開され、そのうちの1つがLSAロールを持っていることを示しています。

以下のセクションは、手動で管理されるエンタイトルメント (ファイルベースのライセンス) に適用されます。

NetScaler Console エージェントを LSA として手動で選択する

管理者は、NetScaler プールライセンスまたは NetScaler フレックスライセンスの LSA として、NetScaler Console エージェントを手動で選択できます。LSA がダウンした場合、NetScaler Console サービスは次の LSA を自動選出する前に 24 時間待機します。管理者はこの機能を使用して、その間に新しい LSA を手動で選出できます。ただし、管理者は選出される新しい LSA のステータスが UP であり、診断ステータスが OK であることを確認する必要があります。

管理者が新しい LSA を手動で選択すると、ライセンス機能が正しく動作するまでに最大 5 分かかる場合があります。この間、NetScaler インスタンスは猶予期間にあり、ライセンスの新規チェックアウトは失敗します。

LSA を選択するには:

1. **Infrastructure > Instances Dashboard > Agents** に移動し、エージェントを選択します。
2. 「**アクションの選択**」リストで、「**LSAとして設定**」を選択します。
3. 「**はい**」をクリックして確定します。選択したエージェントがLSAロールを引き継ぎます。

複数のNetScalerエージェントの動作

複数のエージェントと複数のサイトを組み合わせた展開では、NetScalerエージェントはクライアント/サーバーアーキテクチャに従います。

UP状態に登録された最初または最も古いエージェントにLSAロールが割り当てられます。後から追加された他のエージェントはプロキシとして機能し、ライセンス割り当てのためにメインのLSA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ロールをホストするエージェントと通信します。プロキシロールをホストする各エージェントは、NetScaler Consoleサービスを介して現在のLSAロールを持つエージェントと通信します。

注：

LSAロールを持つエージェントと他の（非LSA）エージェントとの間に直接の通信はありません。すべての接続はNetScaler Consoleサービスのみを介して行われます。

NetScalerエージェントのフェールオーバー動作

エージェントのフェールオーバーは、マルチエージェント展開で次のように機能します。

同じデータセンターに2つのエージェント、AG1とAG2があると仮定します。

- AG1は、ADC11、ADC12、ADC13をリモートライセンスホストまたはLSAとして使用するように構成されています。
- AG2は、ADC21、ADC22、ADC23をリモートライセンスホストまたはLSAとして使用するように構成されています。
- AG2はライセンスサーバーとして機能しています。
    - AG1が失敗した場合、ADC11、ADC12、およびADC13は、ライセンス調整のためにAG2を介して自動的に接続します。
        - この再接続が行われている間、いくつかのハートビートが失われた場合でも、ADC11、ADC12、およびADC13は短い猶予期間を認識する可能性があります。
    - AG2 が失敗した場合、すべての ADC は、次のいずれかの状態になるまで猶予期間を継続します。
        - AG2 が復旧するか、復旧されるか、または NetScaler Console サービスによって 24 時間後に自動的に、あるいは管理者によって手動で、AG1 が新しい LSA として選択される。
        - または AG2 が NetScaler Console サービスから削除される。登録解除されると、NetScaler Console サービスは AG1 を LSA ロールを持つエージェントとして指定します。
        - 選出が完了すると、AG1 は構成されたインスタンスに対してリソースの割り当てと調整を開始します。

LSA に関する質問については、ライセンスサーバーエージェントに関する FAQ を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 組み込みエージェントを介したライセンスサーバーの構成

あるサイトでライセンスサーバーエージェント (LSA) を構成しており、他のサイトから同じ LSA を使用したい場合、NetScaler 組み込みエージェントを使用できます。組み込みエージェントを使用している間は、NetScaler インスタンスで次のコマンドを使用してライセンスサーバーを構成する必要があります。

```
add licenseserver 127.0.0.1 -port 27000
```

この構成では、NetScaler は Console サービスを介してライセンスサーバーエージェント (LSA) に到達できます。

注:

NetScaler 組み込みエージェントには LSA ロールを割り当てることはできません。

Flexed 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。ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降にNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。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には適用されません。
NetScaler Flexedライセンスは、ライセンス管理プロセスを簡素化することを目的とした新しいライセンスフレームワークです。Flexedライセンスには、ソフトウェアインスタンスライセンス (VPX/CPX/BLX、SDX、MPX、VPX FIPS) と帯域幅容量ライセンスが含まれます。Flexedライセンスは、NetScaler ConsoleサービスまたはNetScaler ADM on-premに適用する必要があります。また、MPX Z-CapおよびSDX Z-Capライセンスをそれぞれ NetScaler MPXおよびNetScaler SDXハードウェアに適用する必要があります。その後、クラウドまたはオンプレミスに展開されているすべてのNetScalerフォームファクターにそれらを割り当てることができます。

LASベースのライセンス - LASベースのライセンスを使用する場合、Flexedエンタイトルメントは自動的にNetScaler Consoleサービスにプルされ、ユーザーインターフェイスに表示されます。

手動で管理されるエンタイトルメント (ファイルベースのライセンス):

手動で管理されるエンタイトルメント（ファイルベースのライセンス）を使用する場合は、次の手順を実行します。

1. FlexedライセンスをNetScaler ConsoleサービスまたはNetScaler Console On-premに適用します。
2. 特定のMPX Z-CapおよびSDX Z-Capライセンスを、それぞれNetScaler MPX™およびSDXハードウェアに適用します。
3. ライセンスが適用されると、クラウドまたはオンプレミスに展開されているかどうかにかかわらず、すべてのNetScalerフォームファクターにそれらを割り当てることができます。

Flexedライセンスは、無制限の仮想サーバーに対する分析も提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以前にPooledライセンスを所有していて、Flexedライセンスを購入した場合、Flexedライセンスダッシュボードでライセンスの詳細を表示できます。結合された帯域幅とインスタンスは、Flexedライセンスダッシュボードに表示されます。

帯域幅ライセンスには通常Premiumエディションのみが含まれますが、以前にPooled StandardまたはAdvancedライセンスを所有していた場合は、Standard、Advanced、およびPremiumエディションがFlexedライセンスダッシュボードに表示されます。

FlexedおよびPooled帯域幅とインスタンスライセンス(/en-us/netscaler-console-service/media/flexed-pooled-bw-instance-license.png)

詳細については、Flexed license dashboardを参照してください。

Flexedライセンスを使用すると、インスタンスに必要な帯域幅を割り当て、必要以上に割り当てないことで、帯域幅の使用率を最大化できます。トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられた帯域幅を増減できます。

ゼロキャパシティハードウェア

NetScaler Flexedライセンスを通じて管理される場合、MPXおよびSDXインスタンスは「ゼロキャパシティハードウェア」と呼ばれます。これは、これらのインスタンスが帯域幅プールからリソースをチェックアウトするまで機能できないためです。したがって、これらのプラットフォームはMPX-ZおよびSDX-Zアプライアンスとも呼ばれます。

ゼロキャパシティハードウェアは、共通プールから帯域幅をチェックアウトするためにZ-capライセンスを必要とします。

注:

- ゼロキャパシティライセンスのインストールは、他のNetScalerローカルライセンスと同じように機能します。ゼロキャパシティライセンスの取得とインストール方法の詳細については、Licensing guide for NetScalerを参照してください。
- LASベースのライセンスを使用する場合、Z-Capライセンスを適用する必要はありません。

Z-capライセンスの管理とインストール

Z-capライセンスは、ハードウェアのシリアル番号またはライセンスアクセスコードを使用して手動でインストールする必要があります。Z-capライセンスがインストールされると、ハードウェアにロックされ、オンデマンドでNetScalerハードウェアインスタンス間で共有することはできませ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ん。ただし、Z-capライセンスを別のNetScalerハードウェアインスタンスに手動で移動することはできます。

NetScalerソフトウェアリリース11.1ビルド54.14以降を実行するNetScaler MPXインスタンスと、11.1ビルド58.13以降を実行するNetScaler SDXインスタンスは、NetScaler Flexedライセンスをサポートしています。詳細については、FlexedおよびPooledライセンスの最小および最大容量の表1および2を参照してください。

スタンドアロンNetScaler VPXインスタンス

NetScalerソフトウェアリリース11.1ビルド54.14以降を以下のハイパーバイザーで実行するNetScaler VPXインスタンスは、Flexedライセンスをサポートしています。

- ヴイエムウェア ESX 6.0
- シトリックス Hypervisor™
- リナックス KVM

NetScalerソフトウェアリリース12.0ビルド51.24以降を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実行するNetScaler VPXインスタンスは、Flexedライセンスをサポートしています。

- マイクロソフト Hyper-V
- AWS
- マイクロソフト Azure
- グーグル Cloud

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実行するNetScaler VPXインスタンスは、Flexedライセンスをサポートしています。

- ヴイエムウェア ESX 6.0
- シトリックス ハイパーバイザー
- リナックス KVM
- マイクロソフト Hyper-V
- AWS
- マイクロソフト Azure
- グーグル クラウド

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、Flexedライセンスをサポートしています。ゼロキャパシティハードウェアとは異なり、NetScaler CPXはZ-capライセンスを必要としません。最大1 Gbpsのスループットを消費する単一のNetScaler CPXインスタンスは、ライセンスプールから1インスタンスのみをチェックアウトし、帯域幅は消費しません。たとえば、20 Gbpsの帯域幅プールを持つ20個のNetScaler CPXインスタンスがあるとします。NetScaler CPXインスタンスの1つが500 Mbpsのスループットを消費しても、残りの19個のNetScaler CPXインスタンスに対して帯域幅プールは20 Gbpsのままです。

同じNetScaler CPXインスタンスが1500 Mbpsのスループットを消費し始めた場合、帯域幅プールは残りの19個のNetScaler CPXインスタンスに対して19.5 Gbpsになります。

Flexedライセンスの場合、帯域幅は10 Mbpsの倍数でのみ追加できます。

スタンドアロンのNetScaler BLXインスタンス

NetScaler BLXインスタンスはFlexedライセンスをサポートしています。NetScaler BLXインスタンスはZ-capライセンスを必要としません。トラフィックを処理するには、NetScaler BLXインスタンスはプールから帯域幅とインスタンスライセンスをチェックアウトする必要があります。

帯域幅プール

帯域幅プールは、物理および仮想の両方のNetScalerインスタンスで共有できる合計帯域幅です。帯域幅プールには、Premiumソフトウェアエディション用のプールが含まれています。プール型ライセンスからFlexedライセンスに移行すると、Standard、Advanced、Premiumの各ソフトウェアエディションが混在している場合があります。特定のNetScaler MPX/VPX/CPX/BLXインスタンスは、異なるプールから帯域幅を同時にチェックアウトすることはできません。帯域幅をチェックアウトできる帯域幅プールは、ライセンスされているソフトウェアエディションによって異なります。

インスタンスプール

ソフトウェアインスタンスプールには、次の3種類があります。

- VPX/CPX/BLXソフトウェアインスタンス
- MPXソフトウェアインスタンス（MPX FIPSにも同じプールが適用されます）
- SDXソフトウェアインスタンス（SDX FIPSにも同じプールが適用されます）
- VPX FIPSソフトウェアインスタンス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プールからチェックアウトされると、ライセンスによって、CPU/PE、SSLコア、1秒あたりのパケット数、帯域幅など、ソフトウェアインスタンスのリソースがロック解除されます。

ライセンスの構成

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。License Activation Service（LAS）は、Citrix製品スイート全体で製品アクティベーションを行う次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexed licenses (Citrix Platform License/Universal Hybrid Multi-Cloud)、従来のNetScaler Pooled licenses、およびNetScaler Fixed term Bandwidth licensesをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-premリリース14.1-51.x以降および13.1-60.x以降から非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、April 15 2026までファイルベースのライセンスを継続して使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、April 15 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

NetScaler仮想CPUライセンス（Pooled vCPU）、NetScaler VPX Check-InおよびCheck-Out（CICO）、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンス契約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。

© 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提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、法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。
NetScaler Flexedまたはプールライセンスを使用すると、異なるNetScalerフォームファクター間で帯域幅またはインスタンスライセンスを共有できます。インスタンスがリソースを必要としなくなると、割り当てられた容量を共通プールにチェックインします。解放された容量は、リソースを必要とする他のNetScalerインスタンスで再利用できます。

注:

プールライセンスをお持ちで、Flexedライセンスを購入して適用した場合、結合されたエンタイトルメントはFlexedライセンスダッシュボードに表示されます。

Flexedライセンスまたはプールライセンスを使用すると、インスタンスに必要な帯域幅を、必要以上に割り当てないようにすることで、帯域幅の使用率を最大化できます。トラフィックに影響を与えることなく、実行時にインスタンスに割り当てられる帯域幅を増減できます。プールされた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。

LASベースのライセンス

LASを使用する場合、外部エージェントはオプションです。ライセンスエンタイトルメントはNetScaler Consoleサービスに自動的にプルされ、NetScaler Console GUIに反映されます。

前提条件

- インスタンスがNetScaler Consoleからライセンスをチェックアウトできるように、ポート443が利用可能であることを確認してください。詳しくは、「システム要件」を参照してください。

ステップ1 - エンタイトルメントの反映を検証する

1. **ライセンス管理 > LAS** に移動して、NetScalerエンタイトルメントが反映されていることを確認します。

ステップ2 - NetScalerインスタンスをコンソールサービスに追加する

1. NetScalerインスタンスをコンソールサービスに追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳しくは、「NetScalerインスタンスの追加」を参照してください。

```
-  **Using an External Agent**: If you are using an external agent for
proxying licensing communication, you must explicitly add the NetScaler
instances to the Console.



-  **Using a Built-in Agent**: If you are using a built-in agent, the
NetScaler instance is automatically added to the NetScaler Console service
when you configure the agent. For more informatiion about built-in agent,
see Configure Built-in Agent for NetScaler Console On-Prem.
```

ステップ3 - LASでライセンスをアクティブ化する

1. **ライセンス管理 > LAS** に移動します。
2. **LASでライセンス** または **LASに移行** をクリックします。
3. インスタンスを選択し、**続行** をクリックします。

   詳しくは、「ライセンスアクティベーションサービス」を参照してください。

ステップ4 - NetScalerインスタンスのフレックススループット容量を編集する

1. **NetScaler ライセンス > フレックスライセンス > ダッシュボード > LAS 管理対象エンタイトルメント** に移動します。
2. **Licensed NetScalers** セクションで、インスタンスを選択し、**Edit Throughput Capacity** をクリックします。
3. **Allocate*** 列に、希望するスループット値を入力します。
4. **Submit** をクリックします。

外部エージェントを使用するライセンスなしのMPXアプライアンスの特別なライセンス

ライセンスのないMPXで外部エージェントを使用する場合、Console ServiceへのHTTPS接続はサポートされていません。そのため、ステップ2は実行できません。代わりに、NetScalerに移動して以下の手順を完了してください。

1. **システム > ライセンス > ADC ライセンス > ライセンスの管理 > 新しいライセンスの追加** に移動します。
2. Licensesページで、**Use remote licensing** ラジオボタンを選択し、Remote Licensing ModeからLASモードを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Server Name/IP address** フィールドに、NetScaler Console外部エージェントのIPアドレスを入力します。
4. インスタンスを登録するためにNetScalerエージェントの資格情報を入力し、**Continue** をクリックします。

注記:

- NetScalerエージェントに有効なデジタル証明書（認証局（CA）によって発行されたもの）をアップロードした場合にのみ、**Validate Certificate** チェックボックスを選択します。
- NetScaler Consoleのエージェントの1つがライセンスサーバーとして機能します。

5. **Device Profile Name** フィールドに、NetScaler Consoleがインスタンスにアクセスするために使用するインスタンスプロファイルを入力します。このプロファイルには、追加するインスタンスのユーザー名とパスワードが保持されます。デフォルトのプロファイルはns_nsroot_profileです。ただし、デフォルトの管理者資格情報を変更した場合は、カスタムインスタンスプロファイル名を作成して指定してください。
6. 「**ライセンスの割り当て**」セクションで、ライセンスエディションを選択し、必要な帯域幅を指定します。NetScalerで初めてライセンスを割り当てる場合、後でNetScaler Console GUIから直接割り当てを変更または解放できます。
7. 「**ライセンスの取得**」をクリックします。

注:

ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。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。

手動で管理されるエンタイトルメント（ファイルベースのライセンス）

NetScaler Flexedまたはプールライセンスを使用するには、NetScaler Consoleエージェントを NetScalerインスタンスにアタッチする必要があります。NetScalerインスタンスは、エージェントを介してNetScaler Consoleからライセンスをチェックインおよびチェックアウトします。

NetScaler FIPSインスタンスには、プールされたキャパシティライセンスを使用することもできます。NetScaler Consoleでは、次のタスクを実行できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Flexedまたはプールされたライセンスファイル（帯域幅プールまたはソフトウェア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。
2. ライセンスプールからNetScalerインスタンスにオンデマンドで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容量に基づいて、NetScalerインスタンス（MPX-Z /SDX-Z/ VPX/CPX/BLX）からライセンスをチェックアウトします。

帯域幅、インスタンス、Z-capライセンスを含むFlexedまたはプールされたライセンスは、citrix.comからダウンロードできます。詳細については、「NetScalerのライセンスガイド」を参照してください。

開始する前に

Flexedライセンスを構成する前に、次の前提条件が満たされていることを確認してください。

- NetScaler Consoleにエージェントをインストールして登録します。エージェントのインストールと登録については、「はじめに」を参照してください。
- Flexedライセンスが適切に機能するように、登録されているすべてのエージェントがUP状態であることを確認してください。エージェントがDOWN状態であるが、まだ廃止または終了されていない場合は、UP状態にします。DOWN状態のエージェントが廃止または終了されたか、もう使用されていない場合は、NetScaler Consoleから削除します。
- `27000`および`7279`ポートは、NetScaler Consoleからインスタンスにライセンスをチェックアウトするために利用できます。「システム要件」を参照してください。

ステップ1 - NetScaler Consoleでライセンスを適用する

1. **NetScaler Licensing > License Management**に移動します。
2. **License Files**セクションで、**Add License File**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、NetScaler Consoleにアップロードできます。
    - **ライセンスアクセスコードを使用する**。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を指定します。次に、**Get Licenses**を選択します。次に、**Finish**を選択します。

> **注：**
>
> いつでも、**License Settings**からNetScaler Consoleにライセンスを追加できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Finish**をクリックします。

   ライセンスファイルがNetScaler Consoleに追加されます。**License Expiry Information**セクションには、NetScaler Consoleに存在するライセンスと有効期限までの残り日数が表示されます。

4. **License Files**で、適用したいライセンスファイルを選択し、**Apply licenses**をクリックします。

   この操作により、NetScalerインスタンスは選択したライセンスをFlexedライセンスまたはプールライセンスとして使用できるようになります。

ステップ2 - NetScaler Consoleをライセンスサーバーとして登録し、ライセンスを割り当てる

エージェントを使用して、NetScaler ConsoleをNetScalerインスタンスのライセンスサーバーとして登録できます。

GUIを使用してNetScaler Consoleエージェントを登録する

NetScaler Console GUIで、NetScalerインスタンスに関連付けられたNetScaler Consoleエージェントを登録します。

1. NetScaler GUIにログインします。
2. **> >** の順に移動します。
3. をクリックします。
4. を選択し、 でリストから を選択します。
5. フィールドに、NetScaler Consoleに登録されている関連するNetScaler ConsoleエージェントのIPアドレスを指定します。
6. デフォルトのライセンスポートは27000です。
7. NetScaler Consoleにインスタンスを登録するためにNetScalerエージェントの資格情報を入力し、 をクリックします。NetScaler Consoleでは、エージェントの1つがライセンスサーバーです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

- NetScalerエージェントに有効なデジタル証明書（認証局（CA）によって発行されたもの）をアップロードした場合にのみ、 チェックボックスを選択します。NetScaler Consoleで、 > > に移動し、 リストから を選択して証明書をアップロードします。
- NetScalerがNAT IP経由でのみ到達可能な場合、デバイス登録が失敗する可能性があります。ライセンスをチェックアウトすることはできますが、NetScaler Consoleはそれらの NetScalerインスタンスを管理対象外インスタンスとして表示します。

8. で、NetScaler Consoleがインスタンスにアクセスするために使用できるインスタンスプロファイルを指定します。このインスタンスプロファイルには、NetScaler Consoleに追加するインスタンスのユーザー名とパスワードが含まれています。デフォルトのプロファイルは **ns_nsroot_profile** です。インスタンスのデフォルトの管理者資格情報を変更した場合は、カスタムインスタンスプロファイル名を定義できます。

   ADCでのライセンス管理(/en-us/netscaler-console-service/media/pooled-licenses-manage-licenses-2.png)

9. で、ライセンスエディションを選択し、必要な帯域幅を指定します。

   初めてNetScalerでライセンスを割り当てます。後でNetScaler Console GUIからライセンスの割り当てを変更または解放できます。

   NetScaler GUIからライセンスを割り当てる(/en-us/netscaler-console-service/media/allocate-licenses-from-adc-gui.png)

10. **ライセンスを取得**をクリックします。

重要

ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。インスタンスを再起動するまで、構成の変更は有効になりません。

CLIを使用してエージェントを追加する

NetScalerインスタンスにGUIがない場合は、次のCLIコマンドを使用して、インスタンスに関連付けられたエージェントを追加します。

1. NetScalerコンソールにログインします。
2. NetScaler Consoleに登録されている関連付けられたエージェントのIPアドレスを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. ライセンスサーバーで利用可能なライセンス帯域幅を表示します。

```
> sh ns licenseserverpool
```

4. 必要なライセンスエディションからライセンス帯域幅を割り当てます。

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth> edition <specify-license-edition>
```

重要

ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。

`reboot -w`
インスタンスを再起動するまで、構成の変更は有効になりません。

ステップ3 - ライセンスの種類に基づいて、関連するライセンス手順に進みます

NetScalerインスタンスのFlexedスループット容量を編集する

1. **NetScaler Licensing > Flexed Licensing > Dashboard**に移動します。
2. **Licensed NetScalers**セクションで、インスタンスを選択し、**Edit Throughput Capacity**をクリックします。
3. **Edit Throughput Capacity**ページで、**Allocate**列に数値を入力します。
4. **Submit**をクリックします。

NetScalerインスタンスにプールされたライセンスを割り当てる

NetScaler Console GUIからプールされた容量ライセンスを割り当てるには：

1. NetScaler Consoleにログインします。
2. **インフラストラクチャ > プールライセンス > 帯域幅ライセンス > プール容量**に移動します。

   FIPSインスタンス容量は、FIPSインスタンスライセンスをNetScaler Consoleにアップロードした場合にのみ表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 管理したいライセンスプールをクリックします。

   注：

   Allocated Capacityフィールドは、変更された帯域幅をすぐに反映しません。帯域幅の変更は、NetScalerのウォームリスタート後に有効になります。

   Allocation Detailsでは、インスタンスの帯域幅割り当てを変更すると、**Requested**フィールドと**Applied**フィールドが更新されます。

4. 利用可能なインスタンスのリストからNetScalerインスタンスを選択するには、**>**ボタンをクリックします。

   NetScaler Consoleのプールされたインスタンス(/en-us/netscaler-console-service/media/pooled-licenses-manage-licenses-3.png)

   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、検出されたもののNetScaler Consoleで管理されていないインスタンスが表示されます。

5. ライセンス割り当てを変更するには、**割り当ての変更**または**割り当ての解放**をクリックします。
6. ライセンスサーバーで利用可能なライセンスを含むポップアップウィンドウが表示されます。
7. 割り当てリストオプションを設定することで、インスタンスへの帯域幅またはインスタンスの割り当てを選択できます。選択後、**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。

   注：

   ライセンスエディションを変更した場合は、インスタンスをウォームリスタートしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスでフレキシブルまたはプールされたキャパシティを構成する

以下のNetScalerインスタンスでプールされたキャパシティライセンスを構成できます。

- NetScaler MPX-Zインスタンス
- NetScaler SDX-Zインスタンス
- NetScaler VPX インスタンス
- NetScaler 高可用性ペア

NetScaler MPX-Z

MPX-Z は、フレックスキャパシティ対応の NetScaler MPX アプライアンスです。MPX-Z は、Premium Edition ライセンスのみの帯域幅プールをサポートします。

MPX-Z は、ライセンスサーバーに接続する前にライセンスが必要です。MPX-Z ライセンスは、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** セクションからのライセンスアクセスコード。

MPX-Z ライセンスを削除すると、MPX はライセンスなしの状態になります。インスタンスライセンスはライセンスサーバーに解放されます。

再起動なしで MPX-Z インスタンスの帯域幅を動的に変更できます。ライセンスエディションを変更する場合にのみ再起動が必要です。

注:

インスタンスを再起動すると、設定された容量に必要なフレックスライセンスが自動的にチェックアウトされます。

NetScaler SDX-Z

SDX-Z は、フレックスキャパシティ対応の NetScaler SDX アプライアンスです。SDX-Z は、Premium Edition ライセンスの帯域幅とインスタンスプールをサポートします。

SDX-Z は、ライセンスサーバーに接続する前にライセンスが必要です。SDX-Z ライセンスは、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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。

SDX-Zライセンスを削除すると、SDXはライセンスなしの状態になります。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。

SDX-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:

インスタンスを再起動すると、構成された容量に必要なFlexedライセンスが自動的にチェックアウトされます。

NetScaler高可用性ペアのライセンス要件（LASとファイルベースライセンスの両方に共通）

注:

これらの要件は、手動で管理されるエンタイトルメント（ファイルベースライセンス）とLASの両方に適用されます。

NetScaler高可用性（HA）ペアを構成する際は、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が以下の要件を満たしていることを確認してください。

開始する前に、NetScaler Consoleサーバーがライセンスサーバーとして構成されていることを確認してください。詳細については、「NetScaler Consoleをライセンスサーバーとして構成する」を参照してください。

NetScaler HAペアに帯域幅を割り当てると、NetScaler Consoleは割り当てられた帯域幅をプライマリインスタンスにチェックアウトします。セカンダリインスタンスに対してもこのプロセスを繰り返す必要があります。

NetScaler HAペアにプールライセンスを割り当てるには、「Allocate Flexed licenses to NetScaler instances」を参照してください。

Flexed Capacityページには、インスタンスとその割り当てられた容量が個別に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Flexedライセンスの状態 (LASとファイルベースライセンスの両方に共通)

Flexedライセンスの状態は、NetScalerインスタンスのライセンス要件を示します。Flexedライセンスで構成されたNetScalerインスタンスは、次のいずれかの状態を表示します。

- **割り当て済み**: インスタンスは適切なライセンス容量で稼働しています。
- **猶予**: インスタンスは猶予ライセンスで稼働しています。 **注**: この状態は、手動で管理されるエンタイトルメント (ファイルベースライセンス) にのみ適用されます。
- **接続喪失**: NetScaler Consoleからインスタンスへの通信が機能していません。 **注**: NetScalerとConsole Service間の接続が24時間以上失われた場合、NetScalerの状態は猶予に変わります。

ライセンスダッシュボード

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、レガシーなNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを継続して使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

プール型vCPU、CICO、永続ライセンスなど、その他のすべてのレガシーな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、法律または衡平法上Citrixが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には適用されません。
先に進む前に、以下の注記をお読みください。

注:

- 以前にプールライセンスをお持ちで、今回Flexedライセンスを購入して適用した場合、結合されたエンタイトルメントがFlexedライセンスダッシュボードに表示されます。
- プールライセンスのみをお持ちの場合は、プールライセンスダッシュボードを確認してください。
- Flexedライセンスのみをお持ちの場合、またはFlexedライセンスとプールライセンスの両方をお持ちの場合は、Flexedライセンスダッシュボードを確認してください。
- **ライセンス方法に基づく注意点:**
  - LASベースのライセンスを表示するには、**NetScaler licenses > Flexed Licensing > Dashboard > LAS managed entitlements tab** に移動します。
  - 手動で管理されているエンタイトルメント（ファイルベースのライセンス）を表示するには、**NetScaler licenses > Flexed Licensing > Dashboard > Manually managed entitlements tab** に移動します。
  - 両方のライセンスメカニズムを使用する場合は、両方のタブを参照してください。

Flexedライセンスダッシュボードでは、購入した帯域幅容量とインスタンスの包括的なビューが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このページには、エディション全体の帯域幅容量と、MPX、VPX、SDXなどの異なるフォームファクターのインスタンスの詳細が表示されます。MPXとMPX FIPSは同じライセンスファイルを持っています。同様に、SDXとSDX FIPSも同じライセンスファイルを持っています。ただし、VPX FIPSはVPXとは異なるファイルを持ち、個別に表示されます。また、VPX（SDX上のVPXを含む）、BLX、CPXはVPXライセンスを必要とし、VPXのエンタイトルメントと割り当ての一部です。Flexedライセンスはプレミアムエディションのみをサポートします。ただし、Flexedライセンスを購入し、以前にプールされた標準またはアドバンストの帯域幅容量を持っていた場合、帯域幅容量（標準またはアドバンスト）に関連する詳細もFlexedライセンスダッシュボードに表示されます。

VPX（SDX上のVPXを含む）、BLX、CPXのフォームファクターには、NetScaler Flexed VPX SW Instanceライセンスファイルが必要です。つまり、これらのフォームファクターは、Flexed VPX SW Instanceライセンスのエンタイトルメントと割り当ての一部です。

ライセンスされたNetScalerインスタンスの詳細は、**Licensed NetScalers** セクションで確認できます。インスタンスを選択し、帯域幅を編集したり、そのインスタンスのライセンスを解放したりできます。

次のパラメータに基づいて結果をフィルタリングできます。

- 帯域幅/スループット容量でフィルタリング
  - プレミアム
  - アドバンスト
  - 標準
- フォームファクター
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- ライセンスステータス
  - 接続が失われました
  - 猶予
  - 割り当て済み

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerインスタンスで割り当てられたスループット容量を編集する

1. **NetScaler Licensing > Flexed Licensing > Dashboard** に移動します。
2. **Licensed NetScalers** セクションで、インスタンスを選択し、**Edit Throughput Capacity** をクリックします。
3. **Edit Throughput Capacity** ページで、**Allocate** 列に数値を入力します。
4. **Submit** をクリックします。

NetScalerインスタンスでライセンスを解放する

ライセンスを別のインスタンスに転送するには、現在のインスタンスでライセンスを解放し、その後、新しいインスタンスにライセンスを適用する必要があります。**ライセンスの解放**を選択すると、次の処理が行われます。

- そのインスタンスでチェックアウトされているすべてのライセンスをライセンスサーバーに解放します。
- そのインスタンス上のライセンスサーバー構成を削除します。

「**はい**」を選択すると、NetScalerインスタンスはライセンスなしの状態になり、トラフィックを処理できなくなります。

ライセンスの問題のトラブルシューティング

トラブルシューティングオプションを使用して、いくつかのライセンス関連の問題を表示および分析できます。

発生する可能性のあるライセンスの問題には、Consoleからインスタンスへの通信、ライセンスサーバーエージェント (LSA) の可用性などがあります。**トラブルシューティング**オプションは、ライセンスサーバー、LSA、プロセス、通信などの問題カテゴリとそのステータスの一覧を提供します。管理者として、ライセンスの問題が見つかった場合は、これらのカテゴリを分析してトラブルシューティングできます。

以下は、注意が必要なシナリオの例です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスレポート

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、LASはNetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  注: ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスがない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負

© 1997–2026 Citrix Systems, Inc. All rights reserved.

うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
このダッシュボードでは、次の詳細を表示できます。

注:

以前にプールされたライセンスをお持ちで、現在Flexedライセンスを購入して適用した場合、結合されたエンタイトルメントがFlexedライセンスダッシュボードに表示されます。

- ソフトウェアインスタンス (VPX、MPX、SDX、およびVPX FIP) の資格と割り当て
- 帯域幅/スループット容量の資格、割り当て、および実際の使用状況
- すべての管理対象または選択されたインスタンスにおけるピークおよび平均割り当て
- すべての管理対象または選択されたインスタンスにおけるピークおよび平均使用状況

機能 (NETSCALERインスタンスの場合)	説明
資格	ソフトウェアインスタンスタイプ (VPX、SDX、MPX) の合計インスタンス資格。
割り当て	ソフトウェアインスタンスタイプ (VPX、SDX、MPX) の合計インスタンス割り当て。

機能 (帯域幅/スループット容量の場合)	説明
資格	すべての管理対象NetScalerインスタンスにおける合計帯域幅/スループット容量資格。合計資格は、ライセンス管理 (**NetScaler Licensing > License Management**) で適用されたライセンスから計算されます。
割り当て	フレックスライセンスダッシュボード (**ネットスケーラーライセンス > フレックスライセンス > ダッシュボード**) で、**ライセンスされたネットスケーラー**に割り当てられる帯域幅/スループット容量。
使用状況	NetScalerインスタンスによって消費される総スループット。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

フレックスライセンスはプレミアムエディションのみをサポートします。ただし、フレックスライセンスを購入して適用し、以前に標準またはアドバンストの帯域幅容量をプールしていた場合、帯域幅/スループット容量（標準またはアドバンスト）に関連する詳細も表示されます。例えば、1000 Gbpsのフレックスライセンス（プレミアム）を適用し、さらに100 Gbpsのアドバンスト帯域幅の有効なプールライセンスを持っている場合、レポートダッシュボードにはプレミアム1000 Gbpsと100アドバンスト帯域幅の両方が表示されます。

次の例は、ダッシュボードがピーク使用量と平均使用量をどのように表示するかを理解するのに役立ちます。

3つの管理対象NetScalerインスタンス（NetScaler A、NetScaler B、NetScaler C）がフレックスライセンス（プレミアム帯域幅）を使用しており、選択された期間が1日であるとします。計算のために、NetScaler ConsoleはNetScalerインスタンスごとに1時間あたりのデータポイント（Mbps単位）を考慮します。1日あたり、各NetScalerインスタンスには24個のデータポイントがあります。したがって、3つのNetScalerインスタンスの場合、(24 * 3)個のデータポイントがあります。

- **ピーク使用量** = すべてのNetScalerインスタンスの24時間における最高のデータポイント（Mbps）の合計。例えば、NetScaler Aの24時間における最高のデータポイントが30 Mbps、NetScaler Bが45 Mbps、NetScaler Cが120 Mbpsの場合、ピーク使用量は195 Mbps（30 + 45 + 120）と表示されます。
- **平均使用量** = 各NetScalerインスタンスの24時間すべてのデータポイントの合計を24で割った値。したがって、3つのNetScalerインスタンスの場合、3つのNetScalerインスタンスすべての合計平均を3で割った値。例えば、NetScaler Aの平均が25 Mbps、NetScaler Bの平均が20 Mbps、NetScaler Cの平均が45 Mbpsの場合、平均使用量は30 Mbps（25 + 20 + 35を3で割った値）と表示されます。

同様に、ピークおよび平均割り当ての詳細も同じロジックを使用して表示されます。

リストから期間を1時間から1年まで選択し、詳細を表形式ビューとグラフィカルビューの両方で表示できます。

次の例は、フレックスライセンス（プレミアム帯域幅）を使用しているインスタンスの表形式ビューを示しています。

ダッシュボードには次の詳細が表示されます。

- **ピーク使用量** - 選択した期間における最高の使用量（Mbps単位）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **平均使用量** - 選択した期間の平均使用量 (Mbps)。
- **ピーク割り当て** - 選択した期間の最大割り当て。
- **平均割り当て** - 選択した期間の平均割り当て。
- **フィルター** - 特定のインスタンスの使用状況と割り当ての詳細を表示するために、1つ以上のインスタンスを選択できます。
- **エクスポート** - 詳細をPDF、JPEG、PNG形式でエクスポートできます。

次の例は、Flexedライセンス (プレミアム帯域幅) を使用しているインスタンスのグラフィカルビューを示しています。

Flexedライセンスへの切り替え

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換の最小要件となるNetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-prem リリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのないperpetualライセンスを利用している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。
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。
続行する前に、以下の注記をお読みください。

注:

現在のライセンスの有効期限が切れる前に、Flexedライセンスに切り替える必要があります。移行を計画する際は、以下の手順を念頭に置き、ライセンスの再構成やNetScalerの再起動を伴う場合はメンテナンス期間を計画してください。

LASベースのライセンス

注:

NetScaler (ADCおよびSDX) インスタンスがLAS互換バージョンであることを確認してください。

以下のライセンスの移行に関する情報については、「既存のライセンスインスタンスの移行」(/ja-jp/netscaler-console-service/manage-licenses/license-activation-service.html#migrate-existing-licensed-instances)を参照してください。

- Flexedライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)
- プールライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)

以下のライセンスの移行に関する情報については、「ライセンスアクティベーションサービス」(/ja-jp/netscaler-console-service/manage-licenses/license-activation-service.html#license-netscaler-instances-with-las)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プールvCPUライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)
- 固定サブスクリプションまたは永続ライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)
- 固定vCPUライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)
- CICOライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)
- セルフマネージドライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)
- セルフマネージドvCPUライセンス (ファイルベースライセンス) からFlexedライセンス (LASベースライセンス)

手動で管理されるエンタイトルメント (ファイルベースライセンス)

以下のセクションでは、既存のライセンスタイプからFlexedライセンス (ファイルベースライセンス) への移行手順について説明します。

プール型帯域幅ライセンスからFlexedライセンスへの移行

一部の手順はMPX、SDX、VPXに共通です。これらの手順を最初に示し、次にMPX、SDX、またはVPXに固有の手順を示します。

VPX/MPX/SDXの共通手順

1. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。ライセンスファイルを参照してください。
2. 特定の期間有効なZ-Capソフトウェアライセンスをお持ちの場合は、そのライセンスをNetScalerハードウェア（MPX/SDX）に適用してください。

VPX/MPXの場合

以下の追加手順が必要です。

1. プール型Premium (Platinum) 帯域幅ライセンスをお持ちの場合、古いライセンスの有効期限が切れると、ライセンスは自動的にFlexedに切り替わります。
2. プール型Standardまたはプール型Advanced帯域幅ライセンスをお持ちの場合は、手動でPremium帯域幅をチェックアウトし、NetScalerをウォームリブートしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDXの場合

注記：

現在のライセンスの有効期限が切れる前に、Flexedライセンスに切り替えてください。

以下の追加手順が必要です。

1. 必要なインスタンスと帯域幅ライセンスをFlexedライセンスからSDXにチェックアウトします。SDXのリブートは不要です。
2. SDX上のすべてのVPXがPremiumエディションである場合、古いライセンスの有効期限が切れると、ライセンスは自動的にFlexedに切り替わります。
3. StandardまたはAdvancedのすべてのVPX (SDX上) のエディションをPremiumに変更します。これらのVPXインスタンスは自動的に再起動されます。
4. SDX上のStandardおよびAdvancedの帯域幅容量をゼロに削減します。

プールされたvCPUからFlexedライセンスへ

VPXの場合

1. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。「ライセンスファイル」を参照してください(/ja-jp/netscaler-console-service/manage-licenses/license-management.html#license-files)。
2. NetScaler GUIを使用して既存のライセンスサーバーを削除します。すべての手順が完了するまで、NetScalerはライセンスなしの状態になります。
3. Flexed/Pooledオプションでライセンスサーバーを追加します。
4. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
5. NetScalerをウォームリブートします。

固定サブスクリプションまたは永続ライセンスからFlexedライセンスへ

一部の手順はMPX、SDX、VPXに共通です。これらの手順を最初に示し、次にMPX、SDX、またはVPXに固有の手順を示します。

VPX/MPX/SDXの共通手順

1. NetScaler Consoleにオンボードします。
2. NetScalerエージェントを展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。「ライセンスファイル」を参照してください(/ja-jp/netscaler-console-service/manage-licenses/license-management.html#license-files)。
4. NetScalerハードウェア (MPX/SDX) にZ-Capソフトウェアライセンスを適用します。

VPX/MPXの場合

以下の追加手順が必要です。

1. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
2. NetScalerをウォームリブートします。
3. NetScalerの再起動後、固定サブスクリプションライセンスを削除します。

SDXの場合

以下の追加手順が必要です。

1. SDX上のFlexedライセンスから、必要なインスタンスおよび帯域幅ライセンスをチェックアウトします。
2. SDX上のすべてのVPXがプレミアムエディションである場合、SDXの再起動は不要です。
3. いずれかのVPXがAdvancedまたはStandardエディションである場合、そのVPXをプレミアムエディションに移行する必要があります。VPXは自動的に再起動します。
4. NetScaler SDXにZ-Capソフトウェアライセンスを適用します。
5. SDX上のFlexedライセンスから、必要なインスタンスおよび帯域幅ライセンスをチェックアウトします。
6. NetScalerの再起動後、固定サブスクリプションライセンスを削除します。

固定vCPUからFlexedライセンスへ

VPXの場合

1. NetScaler Consoleにオンボードします。
2. NetScalerエージェントを展開します。
3. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。ライセンスファイルを参照してください。
4. NetScalerでライセンスサーバーをFlexed/Pooledモードで構成します。
5. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
6. NetScalerをウォームリブートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. NetScalerの再起動後、Fixedライセンスを削除します。

CICOからFlexedライセンスへ

VPXの場合

1. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。ライセンスファイルを参照してください。
2. NetScaler GUIを使用して既存のライセンスサーバーを削除します。すべての手順が完了するまで、NetScalerはライセンスなしの状態になります。
3. Flexed/Pooledオプションでライセンスサーバーを追加します。
4. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
5. NetScalerをウォームリブートします。

セルフマネージド帯域幅ライセンスからFlexedライセンスへ

一部の手順はMPX、SDX、VPXに共通です。これらの手順を最初に示し、次にMPX、SDX、またはVPXに固有の手順を示します。

VPX/MPX/SDXの共通手順

1. NetScaler ConsoleにFlexedライセンスをアップロードして適用します。「ライセンスファイル」を参照してください。
2. 特定の期間有効なZ-Capソフトウェアライセンスをお持ちの場合は、そのライセンスをNetScalerハードウェア（MPX/SDX）に適用します。

VPX/MPXの場合

1. セルフマネージドプレミアムライセンスをお持ちの場合は、NetScaler GUIを使用して、ライセンスモードをセルフマネージドプールからFlexed/Pooledに変更します。
2. NetScalerの再起動は不要です。
3. セルフマネージドスタンダードまたはアドバンストライセンスをお持ちの場合は、NetScaler GUIを使用して既存のライセンスサーバーを削除します。
4. Flexed/Pooledオプションを使用してライセンスサーバーを追加します。
5. VPX/MPX に Flexed Premium 帯域幅容量を割り当てる。
6. NetScalerをウォームリブートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDXの場合

1. SDX上のすべてのVPXがセルフマネージドプレミアムライセンスを持っている場合は、NetScaler GUIを使用して、ライセンスモードをセルフマネージドプールからFlexed/Pooledに変更します。
2. NetScalerの再起動は不要です。
3. SDX上のVPXの一部がSelf Managed StandardまたはAdvancedライセンスを持っている場合は、Citrixサポートに連絡してください。

セルフマネージドvCPUからFlexedライセンスへの移行

VPXの場合

1. NetScaler ConsoleでFlexedライセンスをアップロードして適用します。「ライセンスファイル」を参照してください(/ja-jp/netscaler-console-service/manage-licenses/license-management.html#license-files)。
2. NetScaler GUIを使用して、既存のライセンスサーバーを削除します。すべてのステップが完了するまで、NetScalerはライセンスなしの状態になります。
3. Flexed/Pooledオプションでライセンスサーバーを追加します。
4. 必要なインスタンスおよび帯域幅ライセンスをNetScalerにチェックアウトします。
5. NetScalerをウォームリブートします。

FlexedまたはPooledライセンスの有効期限切れと接続性の問題の動作シナリオ

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console オンプレミス のLASサポートはリリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console オンプレミス リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console オンプレミス リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを継続して使用できます。ただし、Console オンプレミス 13.1はLASをサポートしていないため、15th April 2026までにConsole オンプレミス リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、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。

LASベースのライセンス

期間満了前

ライセンスが有効期限前に更新された場合：

- NetScalerインスタンスは、デバイスが稼働している場合、古いライセンスの期限が切れた後、新しいライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScalerは手動でのキャパシティ再構成を必要としません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

期間の満了後

ライセンスが期間満了前に更新されない場合、NetScalerインスタンスは通常の動作を停止します。

- 設定が失われます。
- すべてのトラフィック処理が完全に停止します。

接続の問題の動作シナリオ

NetScalerとNetScaler Consoleサービス間の接続が失われた場合、デバイスは30日間の猶予期間に入ります。

猶予期間中、ライセンスは正常に機能します。ただし、31日目には以下の事象が発生します。

- NetScaler VPX™、CPX、BLX、およびMPXインスタンスは強制的に再起動され、ライセンスなしの状態になります。
- NetScaler SDX™上のすべてのVPXインスタンスのスループットは1 Mbpsに削減されます。

手動で管理されるライセンス（ファイルベースライセンス）

このドキュメントでは、NetScaler MPX、NetScaler SDX、およびNetScaler VPX/NetScaler BLX/NetScaler CPXにおけるライセンスの有効期限切れと接続の問題の動作に関するさまざまなシナリオを提示します。

Flexedライセンスのコンポーネント

- ソフトウェアインスタンス (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- 帯域幅容量

シナリオ: MPXフォームファクター

FlexedまたはPooledライセンスを使用しており、ライセンスの有効期限が間もなく切れます。以下のシナリオでは、期間の満了前と満了後にNetScaler Consoleに新しいライセンスがアップロードされた場合、またはライセンスファイルが存在しない場合の動作について説明します。

期間の満了前

新しいライセンスが期間の満了前にアップロードされ、古いライセンスがまだ有効な場合、2つの異なる容量プール（旧と新）が利用可能です。

- NetScalerが稼働中の場合、古いライセンスの有効期限が切れた後、新しいFlexedまたはPooledライセンスにシームレスに切り替わります。
- 再起動は不要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScalerは手動での容量再構成を必要としません。

期間の満了後

ライセンスの有効期限が切れると、NetScalerインスタンスは通常の動作を停止します。これには、構成の損失やトラフィック処理の完全な停止が含まれます。

古いライセンスと新しいライセンスのエディションが異なる場合の期間満了前または満了後

古いライセンスと新しいライセンスのエディションが異なる場合、期間の満了前か後かに関わらず、以下を実行する必要があります。

- 帯域幅は手動で再構成する必要があります。NetScaler GUIで:

  a. **System > Licenses > Manage Licenses** に移動します。

  b. 「**割り当ての解放**」をクリックして、割り当てを解放します。

  c. 「**割り当ての変更**」をクリックして、帯域幅を再割り当てし、帯域幅をプレミアムに変更します。

- NetScalerを再起動します。

シナリオ: SDXフォームファクター

FlexedまたはPooledライセンスを使用しており、ライセンスの有効期限が間もなく切れます。以下のシナリオでは、期間の満了前と満了後にNetScaler Consoleに新しいライセンスがアップロードされた場合、またはライセンスファイルが存在しない場合の動作について説明します。

期間の満了前

新しいライセンスが期間の満了前にアップロードされ、古いライセンスがまだ有効な場合、2つの異なる容量プール（旧と新）が利用可能です。

- NetScalerが稼働中の場合、古いライセンスの有効期限が切れた後、新しいFlexedまたはPooledライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScalerは手動での容量再構成を必要としません。

期間の満了後

ライセンスの有効期限が切れると、NetScalerインスタンスは通常の動作を停止し、設定の損失やトラフィック処理の完全な停止が発生します。

新旧のライセンスエディションが異なる場合

© 1997–2026 Citrix Systems, Inc. All rights reserved.

期間の満了前

- 古いライセンスファイルと新しいライセンスファイルの両方がConsoleに存在することを確認してください。
- 帯域幅は手動で再構成する必要があります。NetScaler SDX GUIで、次の手順を実行します。
  a. **> >** の順に移動します。
  b. をクリックして割り当てを解放します。
  c. をクリックして帯域幅を再割り当てし、帯域幅をプレミアムに変更します。
- VPXのすべてのエディションをプレミアムに変更して、VPXインスタンスを再起動します。
- をクリックし、プレミアム帯域幅のみを保持します。他のすべての帯域幅割り当てを削除します。

期間の満了後

ライセンスの有効期限が切れると、NetScalerインスタンスは通常の操作を停止します。これには、構成の損失やトラフィック処理の完全なシャットダウンが含まれます。

- SDX上のVPXインスタンスを削除します。
- をクリックして、ConsoleでSDXの帯域幅を再割り当てします。
- SDXでVPXをプレミアムエディションで再プロビジョニングします。

シナリオ：VPX/BLX/CPXフォームファクター

FlexedまたはPooledライセンスを使用しており、ライセンスの有効期限が間もなく切れます。以下のシナリオでは、期間の満了前または満了後にNetScaler Consoleに新しいライセンスがアップロードされた場合、またはライセンスファイルが存在しない場合の動作について説明します。

期間の満了前

期間の満了前に新しいライセンスがアップロードされ、古いライセンスがまだ有効な場合、2つの異なる容量プール（旧と新）が利用可能です。

- NetScalerが稼働中の場合、古いライセンスの有効期限が切れた後、新しいFlexedまたはPooledライセンスにシームレスに切り替わります。
- 再起動は不要です。
- NetScalerは手動でのキャパシティ再構成を必要としません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

期間の満了後

NetScaler Consoleを通じて管理されている、ライセンスの有効期限が切れたNetScalerインスタンスは、トラフィックの処理を停止し、構成の損失につながる可能性があります。

期間満了前または満了後で、古いライセンスと新しいライセンスのエディションが異なる場合

古いライセンスと新しいライセンスのエディションが異なる場合、期間満了前か後かに関わらず、以下を実行する必要があります。

- 帯域幅は手動で再構成する必要があります。NetScaler VPX/BLX/CPX GUIで：
  a. **System > Licenses > Manage Licenses**に移動します。
  b. **Release Allocation**をクリックして割り当てを解除します。
  c. **Change Allocation**をクリックして帯域幅を再割り当てし、帯域幅をプレミアムに変更します。
- VPX/BLX/CPXインスタンスを再起動します。

接続の問題の動作シナリオ

NetScalerとエージェント間、またはエージェントとNetScaler Consoleサービス間の接続が切断された場合、動作は次のとおりです。

- NetScalerは30日間猶予期間に入ります。
- この猶予期間中、ライセンス機能は30日目まで引き続き動作します。
- 31日目には、,
  - NetScaler VPX/NetScaler CPX/NetScaler BLXおよびNetScaler MPXは強制的に再起動され、ライセンスが解除されます。
  - NetScaler SDX上のすべてのVPXのスループットは1 Mbpsに低下します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ConsoleサーバーをFlexedまたはPooledライセンスサーバーとしてのみ構成する

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS)は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexed licenses (Citrix Platform License/Universal Hybrid Multi-Cloud)、従来のNetScaler Pooled licenses、およびNetScaler Fixed term Bandwidth licensesをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScalerの最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  注: ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

NetScaler仮想CPUライセンス（Pooled vCPU）、NetScaler VPX Check-InおよびCheck-Out (CICO)、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
管理者として、NetScaler ConsoleをPooledライセンス機能のみに構成できます。この構成では、NetScaler ConsoleはNetScalerインスタンスからライセンスデータのみを受信します。

場合によっては、NetScalerインスタンスのデータが規制区域外に出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、規制区域内にNetScaler Consoleサーバーのローカルインスタンスを展開できます。Pooledライセンス機能を使用するために同じアプローチを取る場合、さまざまなNetScaler Consoleライセンスサーバー間でPooledライセンスを分割する必要があります。このアプローチでは、グローバルに展開されたNetScalerインスタンス全体にPooledライセンスを柔軟に割り当てることはできません。

したがって、NetScaler ConsoleをPooledライセンス機能のみに構成してください。NetScaler ConsoleはすべてのNetScalerインスタンスからライセンスデータのみを受信します。これにより、規制上の義務を遵守し、グローバルに展開されたNetScalerインスタンス全体にPooled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、NetScaler Console をプールライセンス機能専用に構成する方法について説明します。

前提条件

NetScaler Console をプールライセンス機能専用に構成する前に、NetScaler Console の初回オンボーディングとセットアップを完了してください。エージェントの仕様については、システム要件を確認してください。

重要

NetScaler Console を初めてオンボーディングまたはセットアップする際は、以下を確認してください。

- カスタム展開オプションが選択されていること。
- この構成手順 のステップ 4 を完了した後に追加する NetScaler インスタンス

NetScaler Console をライセンスサーバー専用とする場合の前提条件 (/en-us/netscaler-console-service/media/preq-adm-only-license-server.png)

NetScaler Console のオンボーディングとセットアップの詳細については、はじめに を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オンボーディング手順を完了したら、NetScaler Console をプールライセンス機能専用に構成します。

NetScaler Console を Flexed または Pooled ライセンスサーバー専用として構成する方法

NetScaler Console をライセンス機能専用に構成するには、次の手順を実行します。

1. 「**設定 > グローバル設定 > システム構成 > システム展開**」に移動します。
2. 「**NetScaler Consoleの展開**」で、「**NetScaler Consoleのみをフレキシブル/プールライセンスサーバーとして**」を選択します。

   NetScaler Console をライセンスサーバー専用とする (/en-us/netscaler-console-service/media/adm-only-as-a-license-server.png)
3. 「**OK**」をクリックします。

   この操作により、プールライセンス機能のみが保持され、以下のNetScaler Console機能が無効になります。

   - NetScaler Consoleのバックアップ
   - イベント管理
   - SSL証明書管理
   - ネットワークレポート
   - ネットワーク機能
   - 構成監査

   注

   デフォルトでは、NetScaler Consoleの分析機能は無効になっています。この機能を有効にしている場合は、必ず無効にしてください。

   確認ボックスで、「**はい**」をクリックします。

   NetScaler Console GUIには、プールライセンス機能のみが表示されるようになります。残りの機能は表示されません。
4. ライセンス機能のみにNetScaler Console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NetScalerインスタンスを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

- NetScaler ConsoleおよびNetScaler Consoleサーバーにも他のNetScalerインスタンスを追加できます。このようなNetScalerインスタンスのパスワードを変更する場合は、インスタンスが検出されているすべてのNetScaler Consoleサーバーでパスワードを更新してください。この注記は、NetScaler Consoleがプールライセンス機能のみを使用するように構成されている場合に適用されます。
- ユーザーは、NetScaler Console GUIで無効になっている機能の一部操作を依然として実行できます。たとえば、イベントポーリングやNetScalerのバックアップなどです。スーパー管理者として、そのような操作を制限したい場合は、適切なアクセスポリシーを使用して他の管理者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、(/ja-jp/netscaler-console-service/setting-up/configuring-role-based-access-control.html#configure-access-policies-on-citrix-adm)を参照してください。

レガシーライセンス

レガシーライセンスオプションを使用すると、プール容量、チェックイン/チェックアウトライセンス、仮想CPUライセンスなど、以前のNetScalerライセンスモデルを管理できます。また、NetScaler®展開向けの永続ライセンスをアップグレードしたり、プール容量ライセンスの問題をトラブルシューティングしたりすることもできます。

以下のトピックは、レガシーライセンスの管理に役立ちます。

- NetScalerプール容量
- NetScaler MPXでの永続ライセンスのADCプール容量へのアップグレード
- NetScaler SDXでの永続ライセンスのADCプール容量へのアップグレード
- NetScaler VPXチェックイン/チェックアウトライセンス
- NetScaler仮想CPUライセンス
- FAQとその他のリソース
- プール容量ライセンスの問題のトラブルシューティング

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プールされたキャパシティ

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されていましたが、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体で製品アクティベーションを行う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互換の最小要件となるNetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-prem のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-prem リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console on-prem リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-prem リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負う

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
NetScalerのプールされたキャパシティは、NetScaler Consoleでホストおよび提供される共通の帯域幅とインスタンスプールで構成されるライセンスフレームワークです。この共通プールから、データセンター内の各NetScalerインスタンスは、プラットフォームやフォームファクターに関係なく、1つのインスタンスライセンスと、必要なだけの帯域幅をチェックアウトします。ライセンスファイルと帯域幅はインスタンスにバインドされません。インスタンスがこれらのリソースを必要としなくなると、それらを共通プールにチェックインし、必要とする他のインスタンスが利用できるようにします。

注

NetScaler Consoleでは、エージェントの1つがライセンスサーバーです。

このライセンスフレームワークは、インスタンスが必要以上の帯域幅を割り当てられないようにすることで、帯域幅の利用率を最大化します。NetScalerインスタンスが共通プールからライセンスと帯域幅をチェックできる機能は、インスタンスのプロビジョニングを自動化することも可能にします。

実行時にインスタンスに割り当てられた帯域幅を、トラフィックに影響を与えることなく増減できます。また、プール内のライセンスをあるインスタンスから別のインスタンスへ転送することもできます。

NetScaler MPX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:

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製品スイート全体の製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの他のすべての従来のNetScalerライセンス形式は、LASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つ可能性のあるその他の救済策に加えて、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。
永続ライセンスを持つNetScaler MPXアプライアンスは、NetScalerプール容量ライセンスにアップグレードできます。NetScalerプール容量ライセンスにアップグレードすると、ライセンスプールからNetScaler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。
NetScalerは、永続ライセンスまたはプールライセンスのいずれか1つのライセンスを一度に使用できます。お客様は、プールライセンスから永続ライセンスに切り替えることができます。永続ライセンスが有効である限り、NetScalerを再構成し、プールライセンス設定を削除できます。お客様が永続ライセンスからプールライセンスへ、またはプールライセンスから永続ライセンスへ切り替える場合、すべてのNetScalerインスタンスが再起動されます。

高可用性モードで構成されたNetScalerインスタンスに対して、NetScalerプール容量ライセンスを構成することもできます。高可用性モードのNetScaler MPXインスタンスにNetScalerプール容量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.

注

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。設定タブで、**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になります。アプライアンスはHTTPSリクエストの処理を停止します。

   アップグレード前にアプライアンスで**セキュアアクセスのみ**オプションが有効になっている場合、HTTPSを使用してNetScaler Console GUI経由でアプライアンスに接続することはできません。

8. **確認**ページで、**はい**をクリックします。

9. アプライアンスの再起動後、アプライアンスにログオンします。
10. ようこそページで、**Licenses**セクションをクリックします。

11. **License Server**セクションで、次の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **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。
b. **License Port**フィールドに、ライセンスサーバーポートを入力します。デフォルト値: 27000。
c. NetScaler Consoleを介してインスタンスのプールライセンスを管理する場合は、**Register with Licensing Server for manageability**チェックボックスをオンにし、NetScaler Consoleの資格情報を入力します。
d. **Continue**をクリックします。

12. ライセンスの割り当てウィンドウで、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、アプライアンスを再起動するために**再起動**をクリックします。
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、ライセンスされたすべての機能が一覧表示されます。

14. **システム \> プールライセンス**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NetScaler MPXアプライアンスの場合、HAペアのプライマリとセカンダリの両方のNetScalerインスタンスでNetScalerプール容量を構成する必要があります。HAペアのプライマリとセカンダリの両方のNetScalerインスタンスに同じ容量のライセンスを割り当て

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Gbpsの容量を割り当てて、HAペアのプライマリとセカンダリのNetScalerインスタンスそれぞれに1 Gbpsの容量を割り当てられるようにする必要があります。

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ペアのプライマリとセカンダリの両方のインスタンスにMPX-Zライセンスをアップロードしていることを確認してください。

HAペアのNetScaler MPXインスタンスにMPX-Zライセンスをアップロードするには：

1. Webブラウザで、アプライアンスのIPアドレス（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. 「**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。

   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. 「**再起動**」をクリックしてアプライアンスを再起動します。
8. 「**確認**」ページで、「**はい**」をクリックします。

既存のHAセットアップをNetScaler Pooled容量にアップグレードするには：

1. セカンダリNetScaler MPXインスタンスにログオンします。Webブラウザで、NetScaler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**」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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「**ようこそ**」ページで、「**ライセンス**」セクションをクリックします。

   高可用性セットアップへようこそ(/en-us/netscaler-console-service/media/upgrade-mpx-4-welcome.jpg)

4. 「**ライセンスサーバー**」セクションで、次の操作を行います。

   ライセンスサーバー(/en-us/netscaler-console-service/media/upgrade-mpx-5.jpg)

   a. 「**サーバー名/IPアドレス**」フィールドに、ライセンスサーバーの詳細を入力します。
   b. 「**ライセンスポート**」フィールドに、ライセンスサーバーポートを入力します。デフォルト値: 27000。
   c. NetScaler Console を介してインスタンスのプールライセンスを管理する場合は、「**管理のためにライセンスサーバーに登録**」チェックボックスをオンにし、NetScaler Console の資格情報を入力します。
   d. 「**続行**」をクリックします。

5. 「**ライセンスの割り当て**」ウィンドウで、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-console-service/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-console-service/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。

      セカンダリのNetScaler MPXアプライアンスが再起動すると、HAペアのプライマリNetScaler MPXアプライアンスになります。

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。次の手順を実行します。

   a. 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。
   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。
   e. **System**ページで、**Reboot**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスを再起動する(/en-us/netscaler-console-service/media/upgrade-vpx-034.png)

f. **Reboot**ページで、**Warm reboot**を選択し、**OK**をクリックします。

設定を保存して再起動する(/en-us/netscaler-console-service/media/upgrade-mpx-11.jpg)

プライマリの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。必要に応じて、HAペア内の任意のインスタンスで次のコマンドを使用して、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ペア構成に変更できます。

```
> force ha failover
```

NetScaler SDX 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: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

注: Console on-prem の LAS サポートは、リリース 14.1-51.x 以降です。ただし、ファイルベースのライセンスは、April 15 2026 をもって、Console on-prem リリース 14.1-51.x 以降および 13.1-60.x 以降では非推奨となります。Console on-prem リリース 14.1-51.x またはリリース 13.1-60.x 以降にアップグレードした場合、15th April 2026 までファイルベースのライ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

センスを引き続き使用できます。ただし、Console on-prem 13.1 は LAS をサポートしていないため、15th April 2026 までに Console on-prem リリース 14.1-51.x 以降にアップグレードし、LAS に切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来の NetScaler ライセンス形式は LAS ではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用している NetScaler インスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LAS ベースのライセンスは、法律または規制によって禁止されている地域のお客様には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 SDX 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。
NetScaler は、永続ライセンスまたはプールライセンスのいずれか、一度に1つのライセンスを使用できます。お客様は、プールライセンスから永続ライセンスに切り替えることができます。永続ライセンスが有効である限り、お客様は NetScaler を再構成し、プールライセンス設定を削除できます。お客様が永続ライセンスからプールライセンスへ、またはプールライセンスから永続ライセンスへ切り替える場合、すべての NetScaler インスタンスが再起動されます。

高可用性モードで構成された NetScaler インスタンスに対して、NetScaler Pooled capacity ライセンスを構成することもできます。

注

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。

NetScaler ConsoleでNetScalerインスタンスを追加する権限があることを確認してください。
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、SDX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**フィールドと**パスワード**フィールドに、管理者資格情報を入力します。
3. **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.

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。

   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。
7. **プールされたライセンス**セクションで、次の操作を行います。

   a. **ライセンスサーバー名またはIPアドレス**フィールドに、ライセンスサーバーの詳細を入力します。

      NetScaler Consoleサーバーをライセンスサーバーとして構成する場合は、NetScaler ConsoleサーバーのIPアドレスを指定します。

      NetScaler Console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、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. **ライセンスの取得**をクリックします。
8. **ライセンスの割り当て**ウィンドウで、必要なインスタンスと帯域幅を指定し、**割り当て**をクリックします。

   ライセンスの割り当て](/en-us/netscaler-console-service/media/allocate-licenses.png)

   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-console-service/media/license-server-configured.png)

注

永続ライセンスをプール容量にアップグレードしても、SDXアプライアンスの再起動は必要ありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX チェックインおよびチェックアウトライセンス

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれます）は、April 15, 2026にサポート終了（EOL）となります。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体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してライセンスを付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互換の最小NetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Consoleオンプレミス: 14.1-51.x

  注: ConsoleオンプレミスでのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Consoleオンプレミスリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Consoleオンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Consoleオンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsoleオンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、Perpetualなどの従来のNetScalerライセンスの他のすべての形式はLASではサポートされません。アクティブなメンテナンスのないPerpetualライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

負うことなくCitrix Maintenanceを制限または停止する場合があります。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 ConsoleからオンデマンドでNetScaler VPXライセンスをNetScaler VPXインスタンスに割り当てることができます。ライセンスはNetScaler Consoleによって保存および管理され、NetScaler Consoleには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があります。NetScaler VPXインスタンスは、プロビジョニングされるとNetScaler Consoleからライセンスをチェックアウトでき、インスタンスが削除または破棄されるとNetScaler Consoleにライセンスをチェックインできます。

NetScaler Consoleにライセンスをインストールする

NetScaler Consoleにライセンスファイルをインストールするには:

1. 「**NetScaler Licensing > License Management**」に移動します。
2. 「**License Files**」セクションで、「**Add License File**」をクリックし、次のいずれかのオプションを選択します。
   - **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ある場合は、Consoleにアップロードできます。
   - **ライセンスアクセスコードを使用する**: 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を指定します。「**Get Licenses**」をクリックし、次に「**Finish**」をクリックします。
3. 「Finish」をクリックします。 ライセンスファイルがNetScaler Consoleに追加されます。

注

ライセンスをインストールするためにライセンスアクセスコードを使用する前に、インターネットに接続していることを確認してください。

NetScaler GUIを使用してNetScaler VPXインスタンスにNetScaler VPXライセンスを割り当てる

1. NetScaler VPXインスタンスにログインし、「**System > Licenses > Manage Licenses**」に移動して、「**Add New License**」をクリックし、「**Use remote licensing**」を選択します。
2. 「**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.

注

インスタンスのNetScaler VPXライセンスをNetScaler Console経由で管理する場合は、「**Register with NetScaler MA Service**」チェックボックスをオンにし、NetScaler Consoleの資格情報を入力します。

3. 「**Continue**」をクリックします。
4. 「**Allocate licenses**」ウィンドウで、ライセンスの種類を選択します。このウィンドウには、合計および利用可能な仮想CPUと、割り当て可能なCPUが表示されます。「**Get Licenses**」をクリックします。
5. 次のページで「**Reboot**」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。

6. ライセンスの割り当てを変更または解放するには、**System > Licenses > Manage Licenses** に移動し、**Change allocation** または **Release allocation** を選択します。
7. **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NetScaler VPXライセンスをNetScaler VPXインスタンスに割り当てる

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sh licenseserverpool
```

4. NetScaler VPXインスタンスにライセンスを割り当てるには、次のコマンドを入力します。

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

NetScaler VPX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構成する

NetScaler VPXライセンスの有効期限しきい値を構成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 Console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 Consoleで期限切れになった場合も、SNMPトラップと通知が送信されます。

ライセンスの有効期限通知が送信されるとイベントが生成され、このイベントはNetScaler Consoleで表示できます。

詳細については、ライセンス管理を参照してください。

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。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console on-premリリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。
LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。
ご質問やご不明な点がある場合は、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。
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、少なくとも以下の機能が含まれている必要があります。

- ソフトウェア定義ネットワーク (SDN)
- ネットワーク機能仮想化 (NFV)
- ネットワーク仮想化 (NV)
- マイクロサービス

このような動きには、絶えず変化するビジネスニーズに対応するために、ソフトウェア要件が動的で、柔軟で、俊敏であることも必要です。ライセンスは、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も期待されています。

NetScaler VPX の仮想 CPU ライセンス

以前は、NetScaler VPX ライセンスはインスタンスによる帯域幅消費に基づいて割り当てられていました。NetScaler VPX は、バインドされているライセンスエディションに基づいて、特定の帯域幅とその他のパフォーマンスメトリックを使用するように制限されています。利用可能な帯域幅を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

増やすには、より多くの帯域幅を提供するライセンスエディションにアップグレードする必要があります。特定のシナリオでは、帯域幅の要件は少ないかもしれませんが、SSL TPS、圧縮スループットなどの他の L7 パフォーマンスの要件が高い場合があります。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 負荷の高い処理に必要なシステムリソースを解放するために、大容量の帯域幅を持つライセンスを購入する必要があるかもしれません。NetScaler Console は、仮想 CPU 要件に基づいて NetScaler インスタンスにライセンスを割り当てることをサポートするようになりました。

仮想 CPU 使用量ベースのライセンス機能では、ライセンスは特定の NetScaler VPX が使用できる CPU の数を指定します。そのため、NetScaler VPX は、ライセンスサーバーから、自身で実行されている仮想 CPU の数にのみライセンスをチェックアウトできます。NetScaler VPX は、システムで実行されている CPU の数に応じてライセンスをチェックアウトします。NetScaler VPX は、ライセンスをチェックアウトする際にアイドル状態の CPU を考慮しません。 プールされたライセンス容量と CICO ライセンス機能と同様に、NetScaler Console ライセンスサーバーは、仮想 CPU ライセンスの個別のセットを管理します。ここでも、仮想 CPU ライセンス用に管理される 3 つのエディションは、Standard、Advanced、Premium です。これらのエディションは、帯域幅ライセンスのエディションによってアンロックされる機能と同じ機能セットをアンロックします。

仮想 CPU の数に変更があった場合、またはライセンスエディションに変更があった場合があります。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. **Continue** をクリックします。

注

NetScaler VPXインスタンスは常にNetScaler Consoleに登録してください。まだ登録していない場合は、「NetScaler Consoleに登録」を有効にし、NetScaler Consoleのログイン資格情報を入力してください。

© 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。このウィンドウには、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。「**ライセンスを取得**」をクリックします。

   注

   NetScaler HAペアの場合、各ノードに仮想CPUライセンスを個別に割り当てます。

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エディションのライセンスが既に実行されている場合、そのライセンスを解放してからAdvancedエディションからチェックアウトできます。

FAQとその他のリソース

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。ライセンスアクティベーションサービス（LAS）は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。LASは、April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法となり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬よりサポート。
- NetScaler Console オンプレミス: 14.1-51.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注: Console on-premのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、Console on-premリリース14.1-51.x以降および13.1-60.x以降では、April 15 2026をもって非推奨となります。Console on-premリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console on-prem 13.1はLASをサポートしていないため、15th April 2026までにConsole on-premリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、perpetualなどの従来の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。
このセクションでは、Pooledライセンスの構成と運用に関する参照ドキュメントを一覧表示します。構成および運用に関する問題については、これらのドキュメントを参照してください。

構成

1. Pooled容量の概要と機能に関する情報はどこで確認できますか？

   回答：プールされたキャパシティの構成を参照してください。

2. 永続ライセンスをプールライセンスに、またその逆の方法で変換または移行するにはどうすればよいですか？

   回答：永続ライセンスからプールキャパシティ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。プールキャパシティライセンスを永続ライセンスに戻すことはできません。

3. NetScaler Consoleサーバーを展開するにはどうすればよいですか？

   回答：はじめにドキュメントに従ってください。

4. 既存のプールライセンスにライセンスを追加し、それを割り当てるにはどうすればよいですか？

   回答：ライセンス管理ドキュメントに従ってください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. インスタンス上でキャパシティと帯域幅を割り当て/増加するにはどうすればよいですか？

   回答：ライセンス管理ドキュメントに従ってください。

ライセンスサーバーエージェント

1. 特定のエージェントにLSAロールを割り当てるにはどうすればよいですか？

   回答：最初に展開されたエージェントにLSAロールが割り当てられます。LSAエージェントがダウンした場合、プールライセンスのためにNetScaler Consoleに接続されているすべてのNetScalerインスタンスは、1日間の猶予期間に入ります。翌日、NetScaler Consoleは新しいエージェントをLSAとして選択します。この動作はデフォルトで有効になっています。

   管理者は、LSAがダウンしてから24時間後にNetScaler Consoleサービスがエージェントを自動選択するのを待つ代わりに、24時間以内にNetScalerエージェントをLSAとして手動で選択できます。

   注：

   この移行中、NetScalerの機能には影響ありません。

2. どのエージェントがライセンスサーバーの役割をホストしているかをどのように判断できますか？

   回答: どのエージェントがLSAの役割をホストしているかを知るには、シェルで次のコマンドを実行します。

   ```
   cat /mpsconfig/.lmp/agent
   ```

   「role」の出力値が**lsa**の場合、そのエージェントがライセンスサーバーの役割をホストしています。

   LSAの役割をホストしているエージェント(/en-us/netscaler-console-service/media/adm-serviceagent-hosting-lsa.png)

   NetScaler Console GUIでは、指定されたエージェントのIPアドレスの横にLSAと表示されます。

   LSAとして指定されたエージェント(/en-us/netscaler-console-service/media/agent-designated-as-lsa.png)

3. LSAの役割をホストしているエージェントがダウンした場合、どうなりますか？

© 1997–2026 Citrix Systems, Inc. All rights reserved.

回答: LSAの役割をホストしているエージェントがオフラインの場合、プールされた容量ライセンス用に構成されたすべての展開済みNetScalerデバイスは猶予期間に入ります。猶予期間は30日間続き、NetScalerデバイスに割り当てられたリソースはこの期間中も維持されます。この状態のNetScalerインスタンスは、LSAの役割をホストしているエージェントが再びオンラインになるか、LSAの役割を持つ新しいエージェントが指定されるまで、ライセンスの割り当てを割り当てたり変更したりすることはできません。

4. LSAの役割をホストしているエージェントが長期間オフラインになった場合、再選が行われますか？

   回答: 管理者が24時間以内に新しいLSAを選択しない場合、LSAエージェントがダウンしてから24時間後に、NetScaler Consoleサービスは自動的に稼働中の次のエージェントを新しいLSAとして選択します。新しいLSAが選出されると、NetScalerデバイスの猶予期間は終了します。

一般的な問題

1. 接続障害、アップグレード、スプリットブレインなどにより、猶予モードで実行されているインスタンス。

   回答: NetScalerプール容量の構成に記載されているNetScaler Consoleライセンスサーバーの動作を参照してください。

2. インスタンスにライセンスが適用されない、または反映されない。

   回答: プールされたキャパシティライセンスの問題のトラブルシューティングを参照してください。

3. ライセンスの割り当てが「同期進行中」のままになっています。

   回答: プールされたキャパシティライセンスの問題のトラブルシューティングを参照してください。

4. ライセンスファイル上のホストIDが間違っていることによるエラー。

   回答: NetScaler Consoleサーバーを識別するには、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 Consoleのユニバーサルライセンスに表示されます。詳細については、NetScaler Consoleサーバーにホスト名を割り当てるを参照してください。

移行

1. プールまたはフレックスライセンスを使用している場合、あるConsoleテナントから別のConsoleテナントに移行する際に、SDX上のVPXの帯域幅とインスタンスの再割り当ては必要ですか？

© 1997–2026 Citrix Systems, Inc. All rights reserved.

回答: 両方のテナントでライセンスエディションが同じであり、SDXが以前に割り当てられたキャパシティを取得できる場合、SDX上のVPXの帯域幅とインスタンスの再割り当ては必要ありません。

プール容量ライセンスの問題をトラブルシューティングする

重要:

オンプレミスコンポーネントのアクティベーションに従来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製品アクティベーションを行う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互換の最小要件となるNetScaler®バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

  注: Console オンプレミス のLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console オンプレミス リリース14.1-51.x以降および13.1-60.x以降では非推奨となります。Console オンプレミス リリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console オンプレミス 13.1はLASをサポートしていないため、15th April 2026までにConsole オンプレミス リリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。

© 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。
このセクションでは、一般的なプール容量の問題を分析およびトラブルシューティングする方法について説明します。また、トラブルシューティングのシナリオは、手動で管理されるエンタイトルメント（ファイルベースのライセンス）にも適用されます。

ライセンスステータスの確認

NetScaler Consoleは、NetScalerプール容量ライセンスのライセンスサーバーとして機能します。NetScaler Console GUIを使用して、ライセンスのステータスを確認できます。**Infrastructure > Pooled Licensing > Throughput Capacity > License Usage**に移動します。

次の表に、ライセンスステータスの種類とその意味を示します。

ステータス	意味
割り当て済み	ライセンスの状態は正常です。
割り当て済み: NetScalerに適用されていません	ライセンスがNetScalerからチェックアウトまたはチェックインされた場合、NetScalerの再起動が必要になることがありますが、まだ再起動されていません。
未割り当て	ライセンスはNetScalerインスタンスに割り当てられていません。
猶予期間	NetScalerインスタンスは30日間のライセンス猶予期間中です
同期中	NetScaler Consoleは2分間隔でNetScalerから情報を取得します。NetScaler ConsoleとNetScaler間のライセンス同期には最大15分かかる場合があります。NetScaler Consoleが再起動したか、NetScaler ConsoleのHAフェイルオーバーがトリガーされた可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステータス	意味
部分的に割り当て済み	NetScalerが最大割り当てで実行されている可能性があるため、割り当てられた容量を受け入れることができません。たとえば、NetScalerは10 Gbpsのライセンスプール容量で実行されています。NetScalerが再起動すると、10 GbpsはNetScaler Consoleライセンスサーバーにチェックインされます。NetScalerがオンラインに戻ると、以前に割り当てられた10 Gbpsを自動的にチェックアウトしようとします。その間、他のNetScalerインスタンスがその帯域幅をチェックアウトしている可能性があります。ライセンスプールに完全な10 Gbps、またはこのNetScalerへの部分的な容量を割り当てるのに十分な容量がない場合、「部分的に割り当て済み」と表示されます。
管理されていません	NetScalerは管理のためにNetScaler Consoleに追加されていません。これはNetScalerのライセンスには影響しませんが、NetScaler Consoleからのライセンス監視には影響する可能性があります。
管理されていません	NetScalerは管理のためにNetScaler Consoleに追加されていません。これはNetScalerのライセンスには影響しませんが、NetScaler Consoleからのライセンス監視には影響する可能性があります。
接続が失われました	NetScalerは管理のためにNetScaler Consoleから到達できません。たとえば、ネットワーク接続の問題、NITROが機能していない、またはNetScalerのパスワードの不一致などがあります。NITROが機能していない、またはNetScalerのパスワードの不一致がある場合、これはNetScalerのライセンスには影響しません。ただし、NetScaler Consoleからのライセンス監視には影響する可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サーバーのステータスを確認する

このセクションでは、一般的なサーバーのステータス問題、考えられる原因、および修正について説明します。

問題: NetScalerがライセンスサーバーに到達できないと表示し、ライセンスステータスが猶予期間に変更されます。

- ライセンスサーバー（NetScaler Consoleまたはエージェント）への接続が15分以上切断されています。ライセンスサーバーが稼働しており、到達可能であることを確認してください。
- NetScalerは猶予モードです。

問題: NetScalerはライセンスサーバーのステータスを到達可能と表示しますが、ユーザーが割り当てを変更しようとしても効果がありません。「**割り当ての変更**」をクリックすると「0 0」が返されます。この値は、設定された容量が失われたように見える可能性があります。

- ライセンスサーバーへの接続は最近切断されましたが、NetScalerはまだ2回目のハートビートを見逃していません。したがって、まだ猶予期間ではありません。ライセンスサーバーが稼働しており、到達可能であることを確認してください。

問題: NetScalerは容量とインスタンス数を表示しますが、ライセンスサーバーは**到達可能/到達不能**です。「**割り当ての変更**」をクリックするといくつかの数値が返されますが、設定された容量は考慮されていません。

- ライセンスサーバーへの接続は復元されましたが、NetScalerはまだ2回目のハートビートを逃すか、再接続プローブを送信していません。

問題: NetScaler Consoleでプールライセンスを設定する際に、NetScalerが「ライセンスサーバーに接続できません」と表示する

- ファイアウォールルールを確認し、ポート27000と7279が開いていることを確認します。
- エージェントが登録されていません。詳細については、はじめにを参照してください。
- NetScaler Consoleにライセンスファイルがアップロードされていません。詳細については、NetScalerプール容量の構成を参照してください。
- NetScaler Consoleに誤ったライセンスファイルがあります。

ライセンスの使用状況レポートを確認する

NetScaler Console GUIの**NetScaler Licensing > Pooled Licensing > Throughput Capacity > License Usage**で、ライセンス使用状況の月間ピークを確認できます。このレポートを使用して、ライセンス使用量を増やしたり、追加ライセンスの購入を計画したりできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レポートがどのように生成され、使用できるかについての詳細は以下のとおりです。

ポーリング: ライセンスデータは、NetScalerインスタンスから15分ごとにポーリングされます。

1時間あたりのピークの維持: NetScaler Consoleは、デバイスごとに1時間あたりの最大ライセンス使用量のみを維持します。

レポート作成: 各インスタンスについて、特定の期間のGUIレポートを生成できます。

エクスポート: レポートはCSV形式またはXLS形式でエクスポートできます。

パージ: NetScaler Consoleは、毎月1日の午前12時10分にデータをパージします。パージ期間は設定可能です（デフォルト期間は2か月です）。

プール容量ライセンスのカウンターと統計

以下のカウンタ、ログ、およびコマンドは、NetScaler ConsoleとNetScalerインスタンスの両方がプールライセンスモードで動作していることを示すNetScalerプールライセンスメトリックを公開します。

- **SNMPトラップ**: NetScalerバージョン13.xx以降で利用可能です。
- **レート制限用のNSCONMSGカウンタ**: NetScalerバージョン12.1 57.xx以降で利用可能です。
- **NetScaler Consoleカウンタ** NetScaler Consoleコマンドアクションは、NetScaler Cloudサービスで利用可能です。

SNMPトラップ

以下のSNMPトラップv.13プールライセンスアラームを設定できます。

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

これらのアラームの詳細については、「NetScaler SNMP OIDリファレンス」を参照してください。

NSCONMSGカウンタ

以下の`NCCONMSG`カウンタとその意味を確認してください。

- `allnic_err_rl_cpu_pkt_drops`: CPU制限に達した後の集約（すべてのNIC）パケットドロップ
- `allnic_err_rl_pps_pkt_drops`: pps制限後のシステム全体の集約パケットドロップ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `allnic_err_rl_rate_pkt_drops`: システム全体の集約レートドロップ
- `allnic_err_rl_pkt_drops`: レート、pps、CPUによる累積レート制限ドロップ
- `rl_tot_ssl_rl_enforced`: SSL RLが適用された回数 (新規SSL接続時)
- `rl_tot_ssl_rl_data_limited`: SSLスループット制限に達した回数
- `rl_tot_ssl_rl_sess_limited`: SSL TPS制限に達した回数

NetScaler Console カウンター

「**コマンド実行アクション**」イベントアクションを選択すると、特定のフィルター条件に一致するイベントに対してNetScaler Consoleで実行できるコマンドまたはスクリプトを作成できます。また、「**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を設定できます。

パラメータ	説明
ソース	このパラメータは、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	このパラメータは、フィルターのカテゴリで定義されているトラップの種類に対応します。
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。
$failureobj	障害オブジェクトは、イベントの処理方法に影響を与え、通知されたとおりの正確な問題を反映するようにします。このパラメータを使用すると、単に生のイベントを報告するのではなく、問題を迅速に追跡し、障害の原因を特定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定

NetScaler Console の設定を使用すると、サービスの動作を設定および管理できます。ロールベースのアクセス制御、データストレージと保持、システムアラーム、可観測性統合、通知、および NetScaler® 展開のその他のグローバル設定を管理できます。

以下のトピックは、NetScaler Console の設定に役立ちます。

- Cloud Connect を使用して Console サービスに接続されたオンプレミス Console インスタンス
- オンプレミス Console テレメトリのアップロード
- 仮想サーバーでの分析の設定
- ロールベースのアクセス制御の設定
- 管理対象 NetScaler インスタンスのネットプロファイルの割り当て
- データストレージ管理
- データ保持ポリシー
- システムアラームの設定と表示
- 可観測性統合
- 分析設定の構成
- 通知の設定
- 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
- グローバル設定(/ja-jp/netscaler-console-service/settings/global-settings.html)
- アクションポリシーの構成(/ja-jp/netscaler-console-service/settings/action-policies.html)
- 監査ログメッセージ(/ja-jp/netscaler-console-service/adm-logs-syslog-messages.html)
- IPAMの構成(/ja-jp/netscaler-console-service/networks/configure-ipam.html)

Cloud Connectを使用してConsoleサービスに接続されたオンプレミスConsoleインスタンス

設定 > NetScaler Console On-Premで、Cloud Connectを介してNetScaler Consoleサービステナントに接続されているNetScaler Consoleオンプレミスインスタンスの詳細を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オンプレミスConsoleクラウド(/en-us/netscaler-console-service/media/cloud-connector-instance-details.png)

- **名前** - NetScaler ConsoleオンプレミスのIPアドレス
- **顧客名** - NetScaler Consoleサービステナントの名前
- **状態** - NetScaler ConsoleオンプレミスインスタンスとNetScaler Consoleサービス間の接続ステータス
- **バージョン** - NetScaler Consoleオンプレミスインスタンスのビルドバージョン

Console on-prem アップロード

このページは、テレメトリーデータをNetScaler Consoleサービスにアップロードするために手動モードを選択したNetScaler® on-premユーザーにのみ適用されます。NetScaler Console on-premからテレメトリーデータをダウンロード済みであることを確認してください (必要なテレメトリーデータを含むバンドル(.tgz)ファイルをダウンロードするには、**NetScaler Telemetry**ホームページから**Download Telemetry**をクリックします)。

ビルド**14.1-43.x**以降、NetScaler Consoleサービスにテレメトリーファイルをアップロードするには、NetScaler Console on-premインスタンスごとにプロファイルを作成する必要があります。グローバルに複数のNetScaler Console on-premインスタンスが展開されている場合があります。各on-premインスタンスのプロファイルを作成することで、それらのon-premインスタンスのテレメトリーファイルをアップロードし、アップロード期限を個別に監視できます。

プロファイルを作成するには：

1. **Settings > Console on-prem telemetry upload**に移動し、**Create Profile**をクリックします。
2. **Create Profile**ページで、以下を指定します。
   a. 任意のプロファイル名。
   b. NetScaler Console on-premのIPアドレス。
   c. NetScaler Console on-premの管理者名。
   d. **Next**をクリックします。

   プロファイル名が作成されました。テレメトリーファイルをアップロードして完了をクリックするか、後でアップロードすることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. すべてのNetScaler Console on-premインスタンスに対して複数のプロファイルを作成するには、この手順を繰り返します。

プロファイルを作成した後、作成されたプロファイルを表示できます。

注:

既存のNetScaler Consoleオンプレミスユーザーで、以前にテレメトリファイルをNetScaler Consoleサービスにアップロードしたことがある場合は、新しいプロファイルを作成してからテレメトリファイルをアップロードする必要があります。プロファイルを作成した後、NetScaler Consoleオンプレミスの期限とNetScaler Consoleサービスの期限との間に不一致が見られる場合があります。NetScaler Consoleオンプレミスに表示されている期日までに、テレメトリファイルをNetScaler Consoleサービスにアップロードしてください。この不一致は、新しいプロファイルを使用して1回のアップロードを完了すると解消されます。

NetScaler Consoleサービスでデータテレメトリをアップロードするには:

1. **NetScaler Console on-prem upload**ページで、作成したプロファイルから**Upload Telemetry**をクリックし、ダウンロードした(.tgz)ファイルを選択してアップロードプロセスを完了します。
2. 手動モードを選択してから30日以内に最初のアップロードを完了します。その後は同じ手順を繰り返し、90日ごとにテレメトリファイルをアップロードします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

- ファイルが有効な(.tgz)形式でない場合、または整合性チェックに合格しない場合、アップロードは失敗します。再度ダウンロードしてアップロードを再試行することをお勧めします。問題が解決しない場合は、カスタマーケアにお問い合わせください。
- NetScaler Consoleサービスは、90日以上前のアップロードされたテレメトリファイルを拒否します。再試行するには、新しいテレメトリファイルをダウンロードしてアップロードしてください。
- オプションのテレメトリデータを無効にできます。無効にするには、NetScaler Console オンプレミスで、まず**NetScaler Telemetry**ページで**Security Advisory**を無効にし、次に**Settings > Administration > Enable or disable the Console feature data sharing**に移動して、**I agree to share Console feature usage data**チェックボックスをオフにする必要があります。

プロファイルを編集または削除するには:

1. **Settings > Console on-prem telemetry upload**に移動し、編集または削除したいプロファイルを選択します。
2. 編集するには、**Edit**アイコンをクリックします。必要なフィールドを更新し、**Save**をクリックします。
3. 削除するには、**Delete**アイコンをクリックします。

仮想サーバーでアナリティクスを構成する

14.1-21.xビルド以降、検出されたすべての仮想サーバーとそれに続く仮想サーバーは自動的にライセンスされます。アナリティクスの構成に進むことができます。

アナリティクスは2つの方法で構成できます。**Settings > Analytics Configuration** に移動して、以下を表示します。

- **仮想サーバーアナリティクス概要** - 検出された仮想サーバーでアナリティクスを構成できます。
- **グローバルアナリティクス概要** - 検出された仮想サーバーとそれに続く仮想サーバーの両方でアナリティクスを構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

検出された仮想サーバーでアナリティクスを構成する

注:

アナリティクスを有効にする仮想サーバーが **UP** ステータスであることを確認してください。

1. **仮想サーバーアナリティクス概要** で、**Configure Analytics** をクリックします。

   すべての仮想サーバー ページが表示されます。次のことができます。

   - アナリティクスを有効にする
   - アナリティクスを編集する
   - アナリティクスを無効にする

   注:

   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。

2. 仮想サーバーを選択し、 をクリックします。

   注

   または、インスタンスのアナリティクスを有効にすることもできます。

   a. **> >** の順に移動し、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、 リストから を選択します。
   c. ページで、仮想サーバーを選択し、 をクリックします。

3. ウィンドウで、次の操作を行います。

   a. インサイトタイプを選択します。

      注:

      14.1-44.xビルド以降、**Web Transaction Analytics** は仮想サーバーレベルで利用可能です。有効にするには、 の下の オプションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. で、次の操作を行います。

- 転送モードとして 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 および Logstream の詳細については、Logstream の概要を参照してください。

- **HTTP X-Forwarded-For を有効にする** - HTTP プロキシまたはロードバランサーを介した、クライアントとアプリケーション間の接続の IP アドレスを識別するには、このオプションを選択します。
- **カスタムヘッダー** - X-Real-IP、X-Client-IP、またはその他のカスタムヘッダーを定義して、プロキシ IP アドレスではなく実際のクライアント IP アドレスを取得します。管理対象の NetScaler インスタンスが 14.1–38.24 以降のビルドであることを確認してください。
- **NetScaler Gateway** - NetScaler Gateway の分析を表示するには、このオプションを選択します。

c. 式はデフォルトで true です。

d. **OK** をクリックします。

注:

- 管理者パーティションでは、**Web Insight** のみがサポートされます。
- キャッシュリダイレクト、認証、GSLB などの仮想サーバーでは、分析を有効にできません。エラーメッセージが表示されます。

OK をクリックすると、NetScaler Console は選択した仮想サーバーで分析を有効にする処理を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

NetScaler Console は、Logstream には NetScaler SNIP を、IPFIX には NSIP を使用します。NetScaler エージェントと NetScaler インスタンスの間でファイアウォールが有効になっている場合は、NetScaler Console が AppFlow トラフィックを収集できるように、次のポートを開いていることを確認してください。

トランスポートモード	送信元 IP	タイプ	ポート
IPFIX	NSIP	UDP	4739
ログストリーム	SNIP	TCP	5557

アナリティクスを編集

仮想サーバーでアナリティクスを編集するには：

1. 仮想サーバーを選択します。

   注：

   または、インスタンスのアナリティクスを編集することもできます。

   a. **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、 をクリックします。

2. をクリックします。
3. ウィンドウで、適用するパラメータを編集します。
4. 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、次の手順を実行します。

1. 仮想サーバーを選択します。
2. をクリックします。

NetScaler Console は、選択した仮想サーバーの分析を無効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の表は、トランスポートモードとして IPFIX と Logstream をサポートする NetScaler Console の機能について説明しています。

機能	IPFIX	ログストリーム
ウェブインサイト	サポート対象	対応
WAFセキュリティ違反	対応	対応
ゲートウェイインサイト	対応	対応
HDXインサイト	対応	対応
SSLインサイト	非対応	対応
CRインサイト	対応	対応
IPレピュテーション	対応	対応
AppFirewall	対応	対応
クライアント側測定	対応	対応
Syslog/Auditlog	対応	対応

グローバルアナリティクスを構成する

カスタムポリシーまたはグローバルポリシーを作成することで、グローバルアナリティクスを有効にできます。

注記:

- 作成できるポリシーは最大10個です。ポリシーは、9つのカスタムポリシーと1つのグローバルポリシーの組み合わせ、または10個のカスタムポリシーのいずれかになります。
- カスタムポリシーとグローバルポリシーの両方がある場合、両方のポリシーで選択されたインサイトが仮想サーバーに適用されます。インサイトを削除したい場合は、手動で削除する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタムポリシー

カスタムポリシーを使用すると、特定のインサイトのみを必要とするインスタンスまたは仮想サーバーを制御できます。NetScaler Consoleで管理されているさまざまなNetScalerインスタンスを通じて、数百の仮想サーバーが構成されている場合があります。特定のシナリオでは、一部の仮想サーバーまたはインスタンスにのみ選択的なインサイト（たとえば、ボットセキュリティ違反やWAFセキュリティ違反など）を適用したい場合があります。そのようなシナリオでは、カスタムポリシーを構成し、特定の分析機能を選択して、関連するインスタンスと仮想サーバーに適用できます。

カスタムポリシーを構成するには:

1. **Global Analytics Summary**で、**Global Analytics Configuration**をクリックします。

2. **Policy details**で、**Custom policy**を選択し、任意のポリシー名を指定します。

   注記:

   ポリシー名は後で編集できません。

3. **Define Conditions**で、インスタンスIPのセット、特定のインスタンス、仮想サーバー名、またはその両方を選択して条件を作成します。

4. **Enable analytics**で、分析機能のタイプを選択します。

   注:

   「**後続の仮想サーバーにこの分析設定を適用する**」を有効にすると、定義された分析機能に基づいて、後続の仮想サーバーに分析が適用されます。

5. 「**保存**」をクリックします。

   注意点:

   - 既存のインサイトを削除して別のインサイトを追加することでポリシーを変更した場合、更新されたポリシーには新しいインサイトが適用されます。いずれかのインサイトを削除したい場合は、すでに構成されているインサイトを手動で削除する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX InsightとWeb Insightを含むカスタムポリシーを作成したとします。HDX Insightを削除し、ボットセキュリティ違反を追加するようにポリシーを更新した場合、仮想サーバー/インスタンスはHDX Insight、Web Insight、およびボットセキュリティ違反で更新されます。HDX Insightを削除したい場合は、分析の編集オプションを使用して手動で削除する必要があります。

- 既存のポリシーを削除し、同じインスタンスまたは仮想サーバーを追加して別のポリシーを作成した場合にも、同じロジックが適用されます。

グローバルポリシー

グローバルポリシーを使用すると、検出された仮想サーバーと後続の仮想サーバーの両方で分析を有効にできます。グローバルポリシーを作成するには:

1. 「**グローバル分析の概要**」で、「**グローバル分析構成**」をクリックします。
2. 「**ポリシーの詳細**」で、「**グローバルポリシー**」を選択します。
3. 「**分析を有効にする**」で、分析機能の種類を選択します。

> **注:**
>
> 「**後続の仮想サーバーにこの分析設定を適用する**」を有効にすると、定義されたカテゴリに基づいて、後続の仮想サーバーに分析が適用されます。

4. 「**保存**」をクリックします。

設定後、アナリティクスは検出された仮想サーバーと、その後に検出される仮想サーバーの両方で有効になります。

注意点

- 「**Web Insight**」、「**HDX™ Insight**」、「**Gateway Insight**」を選択して、グローバルポリシーを初めて構成したとします。後でアナリティクス設定を再度変更し、「**Gateway Insight**」の選択を解除しても、その変更はすでにアナリティクスが有効になっている仮想サーバーには影響しません。仮想サーバー上のGateway Insightは手動で削除する必要があります。
- 10台の仮想サーバーがあり、そのうち2台は「**アナリティクスの構成**」オプションを使用してすでにアナリティクスが有効になっているとします。このシナリオでは、グローバルポリシーを構成すると、アナリティクスは残りの8台の仮想サーバーにのみ適用されます。
- 10台の仮想サーバーがあり、そのうち2台のアナリティクスを手動で無効にしたとします。このシナリオでは、グローバルポリシーを構成すると、アナリティクスは残りの8台の仮想サー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バーにのみ適用され、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されます。

アナリティクスの移行

14.1-40.xビルド以降、仮想サーバーでアナリティクスを有効にすると、アナリティクスはプロファイルベースの構成を通じて適用されます。以前は、アナリティクスはAppFlowポリシーを通じて構成されていました。プロファイルベースの構成には、次の利点があります。

- パフォーマンスと柔軟性の向上
- 構成と管理の簡素化

「

注:

」.

アナリティクス構成に関連する機能強化は、プロファイルベースの構成を通じてのみサポートされます。アナリティクスが有効になっている既存のすべての仮想サーバーをプロファイルベースの構成に移行することをお勧めします。

1. 「**設定 > アナリティクス構成**」に移動し、「**アナリティクスの移行**」を選択します。

2. 「**アナリティクスの移行**」ページで、AppFlow®ポリシーを通じて1つ以上の仮想サーバーが構成されているインスタンスを表示できます。

   「インスタンスを選択」(/en-us/netscaler-console-service/media/select-instances-migrate-analytics.png)

   確認ウィンドウが表示されます。移行を完了するには、**はい**をクリックします。

ロールベースのアクセス制御を構成する

NetScaler Consoleは、企業内の個々のユーザーの役割に基づいてアクセス権限を付与できる、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。

NetScaler Consoleでは、すべてのユーザーがCitrix Cloudに追加されます。組織の最初のユーザーとして、まずCitrix Cloudでアカウントを作成し、Citrix Cloudの資格情報を使用してNetScaler Console GUIにログオンする必要があります。スーパー管理者ロールが付与され、デフォルトです

© 1997–2026 Citrix Systems, Inc. All rights reserved.

べてのNetScaler Consoleアクセス権限を持ちます。後で、Citrix Cloudで組織内の他のユーザーを作成できます。

後で作成され、通常のユーザーとしてNetScaler Consoleにログオンするユーザーは、委任された管理者として知られています。これらのユーザーは、デフォルトではユーザー管理権限を除くすべての権限を持っています。ただし、適切なポリシーを作成し、それらの委任されたユーザーに割り当てることで、特定のユーザー管理権限を付与できます。ユーザー管理権限は、**設定** > **ユーザーとロール**にあります。

特定の権限を割り当てる方法の詳細については、「委任された管理者ユーザーに追加の権限を割り当てる方法」を参照してください。

ポリシー、ロール、グループの作成方法、およびユーザーをグループにバインドする方法の詳細については、以下のセクションで説明します。

例:

次の例は、NetScaler ConsoleでRBACを実現する方法を示しています。

NetScalerグループの責任者であるクリスは、彼の組織におけるNetScaler Consoleのスーパー管理者です。彼は、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対して完全なアクセス権を持つ必要がありますが、システム管理操作に対しては読み取り専用アクセス権を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が必要です。
- 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。

次の図は、管理者およびその他のユーザーが持つ権限と、組織内での彼らの役割を示しています。

Chrisがユーザーにロールベースのアクセス制御を提供するには、まずCitrix Cloudでユーザーを追加する必要があり、その後でNetScaler Consoleでユーザーを確認できます。Chrisは、各ユーザーの役割に応じてアクセスポリシーを作成する必要があります。アクセスポリシーは役割に厳密に紐

© 1997–2026 Citrix Systems, Inc. All rights reserved.

付けられています。そのため、Chrisは役割も作成し、その後グループを作成する必要があります。役割は個々のユーザーではなくグループにのみ割り当てることができるためです。

アクセスとは、ファイルの表示、作成、変更、削除など、特定のタスクを実行する機能です。役割は、企業内のユーザーの権限と責任に基づいて定義されます。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かもしれませんが、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することができます。

ポリシーはユーザーの役割を決定します。ポリシーを作成した後、役割を作成し、各役割を1つ以上のポリシーにバインドし、ユーザーに役割を割り当てることができます。ユーザーのグループに役割を割り当てることもできます。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。役割とは、特定の条件に基づいて特定のグループにユーザーを追加することで、ユーザーに付与されるIDです。NetScaler Consoleでは、役割とポリシーの作成はNetScalerのRBAC機能に固有のものです。役割とポリシーは、企業ニーズの変化に応じて、個々の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。

役割は機能ベースまたはリソースベースにすることができます。たとえば、SSL/セキュリティ管理者とアプリケーション管理者を考えてみましょう。SSL/セキュリティ管理者は、SSL証明書の管理および監視機能に完全にアクセスできる必要がありますが、システム管理操作には読み取り専用アクセス権が必要です。アプリケーション管理者は、自分のスコープ内のリソースのみにアクセスできます。

したがって、スーパー管理者であるChrisとしての役割で、組織のセキュリティ管理者であるDavidのアクセスポリシー、役割、およびユーザーグループを構成するために、NetScaler Consoleで次の例のタスクを実行します。

NetScaler Consoleでユーザーを構成する

スーパー管理者として、NetScaler ConsoleではなくCitrix Cloudでアカウントを構成することで、より多くのユーザーを作成できます。新しいユーザーがNetScaler Consoleに追加された場合、適切なグループをユーザーに割り当てることによってのみ、その権限を定義できます。

Citrix Cloud™に新しいユーザーを追加するには：

1. NetScaler Console GUIで、左上のハンバーガーアイコンをクリックし、 を選択します。

2. ページで、 タブを選択します。

   このタブには、Citrix Cloudで作成されたユーザーが一覧表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. リストからIDプロバイダーを選択します。

   - **Citrix Identity**: NetScaler Consoleに追加するユーザーのメールアドレスを入力し、 をクリックします。

     注記:

     ユーザーはCitrix Cloudからメール招待を受け取ります。ユーザーは、氏名とパスワードを入力して登録プロセスを完了するために、メールに記載されているリンクをクリックする必要があります。その後、資格情報を使用してNetScaler Consoleにログオンします。

   - **Azure Active Directory (AD)**: このオプションは、Azure ADがCitrix Cloudに接続されている場合にのみ表示されます。「Azure Active DirectoryをCitrix Cloudに接続する」を参照してください。このオプションを選択してユーザーまたはグループを招待する場合、選択したユーザーまたはグループに対して**カスタムアクセス**のみを指定できます。ユーザーはAzure ADの資格情報を使用してNetScaler Consoleにログインできます。また、選択したAzure ADに属するユーザーに対してCitrix Identityを作成する必要はありません。招待されたグループにユーザーが追加された場合、新しく追加されたユーザーに招待を送信する必要はありません。このユーザーはAzure ADの資格情報を使用してNetScaler Consoleにアクセスできます。

4. 指定したユーザーまたはグループに対して**カスタムアクセス**を選択します。
5. **Application Delivery Managment**を選択します。

   このオプションには、NetScaler Consoleで作成されたユーザーグループが一覧表示されます。ユーザーを追加するグループを選択します。

   |シトリックス アイデンティティ|アジュール エーディー| |-|-| |

   |

   | |**招待を送信**をクリックします。|**管理者グループの追加**をクリックします。|

管理者は、NetScaler Consoleのユーザーリストに新しいユーザーが表示されるのは、ユーザーがNetScaler Consoleにログオンした後のみです。

NetScaler Consoleでユーザーを構成するには:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. NetScaler Console GUIで、**設定** > **ユーザーとロール** > **ユーザー** に移動します。
2. ユーザーは**ユーザー**ページに表示されます。
3. ユーザーを選択して**編集**をクリックすると、そのユーザーに付与されている権限を編集できます。また、**設定**ノードの下にある**グループ**ページでグループ権限を編集することもできます。

注:

- ユーザーはCitrix CloudからのみNetScaler Consoleに追加されます。そのため、管理者権限を持っていても、NetScaler Console GUIでユーザーを追加または削除することはできません。グループ権限のみを編集できます。ユーザーはCitrix Cloudから追加または削除できます。
- ユーザーの詳細情報は、そのユーザーがNetScaler Consoleに少なくとも一度ログインした後にのみ、サービスGUIに表示されます。

NetScaler Consoleで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、ロールを作成することで、ユーザーグループまたは複数のグループに適用できます。ポリシーはユーザーロールを決定します。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、ユーザーグループにロールを割り当てる必要があります。NetScaler Consoleには、5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。

- **admin_policy**。すべてのNetScaler Consoleノード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 Consoleコンテンツを表示でき、すべての編集操作を実行できます。つまり、ユーザーはリソースに対する追加、変更、削除の操作を実行できます。
- **adminExceptSystem_policy**。設定ノードへのアクセスを除く、NetScaler Console GUIのすべてのノードへのユーザーアクセスを許可します。
- **readonly_policy**。読み取り専用権限を付与します。ユーザーはNetScaler Consoleのすべてのコンテンツを表示できますが、いかなる操作も実行する権限はありません。
- **appadmin_policy**。NetScaler Consoleのアプリケーション機能にアクセスするための管理権限を付与します。このポリシーにバインドされたユーザーは、次のことができます。
  - カスタムアプリケーションの追加、変更、削除
  - サービス、サービスグループ、およびコンテンツスイッチングやキャッシュリダイレクションなどのさまざまな仮想サーバーの有効化または無効化

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **appreadonly_policy**。アプリケーション機能に対する読み取り専用権限を付与します。このポリシーにバインドされたユーザーはアプリケーションを表示できますが、追加、変更、削除、有効化、または無効化の操作を実行することはできません。

これらの事前定義されたポリシーを編集することはできませんが、独自の（ユーザー定義）ポリシーを作成できます。

以前は、ポリシーをロールに割り当て、ロールをユーザーグループにバインドすると、NetScaler Console GUIでノードレベルのユーザーグループに権限を付与できました。たとえば、**負荷分散**ノード全体にのみアクセス権限を付与することができました。ユーザーは、**負荷分散**下のすべてのエンティティ固有のサブノード（仮想サーバー、サービスなど）にアクセスする権限を持つか、**負荷分散**下のどのノードにもアクセスする権限を持っていませんでした。

NetScaler Console 507.xビルド以降のバージョンでは、アクセスポリシー管理が拡張され、サブノードにも権限を付与できるようになりました。仮想サーバー、サービス、サービスグループ、サーバーなど、すべてのサブノードに対してアクセスポリシー設定を構成できます。

現在、このようなきめ細かいレベルのアクセス権限は、**負荷分散**ノード下のサブノードに対してのみ、および**GSLB**ノード下のサブノードに対しても提供できます。

たとえば、管理者として、ユーザーに仮想サーバーの表示のみを許可するアクセス権限を付与したい場合がありますが、**負荷分散**ノード内のバックエンドサービス、サービスグループ、およびアプリケーションサーバーは許可しません。このようなポリシーが割り当てられたユーザーは、仮想サーバーのみにアクセスできます。

ユーザー定義のアクセスポリシーを作成するには:

1. NetScaler Console GUIで、**設定** > **ユーザーとロール** > **アクセスポリシー**に移動します。
2. **追加**をクリックします。
3. **アクセスポリシーの作成**ページで、**ポリシー名**フィールドにポリシーの名前を入力し、**ポリシーの説明**フィールドに説明を入力します。

   権限セクションには、すべてのNetScaler Console機能が一覧表示され、読み取り専用、有効化/無効化、または編集アクセスを指定するオプションがあります。

   a. (+)アイコンをクリックして、各機能グループを多くの機能に展開します。

   b. 機能名の横にある権限チェックボックスを選択して、ユーザーに権限を付与します。

      - **表示:** このオプションを使用すると、ユーザーはNetScaler Consoleで機能を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **有効化/無効化:** このオプションは、NetScaler Consoleで有効化または無効化アクションを許可する**ネットワーク機能**機能でのみ使用できます。ユーザーは機能を有効または無効にできます。ユーザーは**今すぐポーリング**アクションを実行することもできます。

  ユーザーに**有効化/無効化**権限を付与すると、**表示**権限も付与されます。このオプションの選択を解除することはできません。

- **編集:** このオプションは、ユーザーに完全なアクセス権を付与します。ユーザーは機能とその機能を変更できます。

  編集権限を付与すると、**表示**権限と**有効化/無効化**権限の両方が付与されます。自動選択されたオプションの選択を解除することはできません。

機能のチェックボックスを選択すると、その機能のすべての権限が選択されます。

注:

負荷分散と**GSLB**を展開して、その他の構成オプションを表示します。

次の画像では、負荷分散機能の構成オプションには異なる権限があります。

仮想サーバー機能に対して、ユーザーに**表示**権限が付与されます。ユーザーはNetScaler Consoleで負荷分散仮想サーバーを表示できます。仮想サーバーを表示するには、**インフラストラクチャ > ネットワーク機能 > 負荷分散**に移動し、**仮想サーバー**タブを選択します。

サービス機能に対して、ユーザーに**有効化/無効化**権限が付与されます。この権限は**表示**権限も付与します。ユーザーは負荷分散仮想サーバーにバインドされているサービスを有効または無効にできます。また、ユーザーはサービスに対して**今すぐポーリング**アクションを実行できます。サービスを有効または無効にするには、**インフラストラクチャ > ネットワーク機能 > 負荷分散**に移動し、**サービス**タブを選択します。

注:

ユーザーが**有効化/無効化**権限を持っている場合、サービスに対する有効化または無効化アクションは、次のページで制限されます。

a. **インフラストラクチャ > ネットワーク機能**に移動します。

b. 仮想サーバーを選択し、**構成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **負荷分散仮想サーバーサービスバインディング**ページを選択します。 このページで**有効化**または**無効化**を選択すると、エラーメッセージが表示されます。

サービスグループ機能に対して、ユーザーに**編集**権限が付与されます。この権限は、**表示**権限と**有効化/無効化**権限が付与される完全なアクセス権を付与します。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グループを変更できます。サービスグループを編集するには、**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、**サービスグループ**タブを選択します。

4. 「**作成**」をクリックします。

注:

「**編集**」を選択すると、権限セクションで有効として表示されない依存権限が内部的に割り当てられる場合があります。たとえば、障害管理の編集権限を有効にすると、NetScaler Console は、ユーザーがレポートをメールとして送信できるように、メールプロファイルの構成や SMTP サーバー設定の作成の権限を内部的に提供します。

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、表示権限は自動的に有効になります。

NetScaler Consoleでロールを構成する

NetScaler Consoleでは、各ロールは1つ以上のアクセスポリシーにバインドされます。ポリシーとロールの間で、1対1、1対多、多対多の関係を定義できます。1つのロールを複数のポリシーにバインドすることも、複数のロールを1つのポリシーにバインドすることもできます。

たとえば、あるロールが2つのポリシーにバインドされている場合、一方のポリシーは1つの機能に対するアクセス権限を定義し、もう一方のポリシーは別の機能に対するアクセス権限を定義する場合があります。あるポリシーはNetScaler ConsoleでNetScalerインスタンスを追加する権限を付与し、別のポリシーはStyleBookを作成および展開し、NetScalerインスタンスを構成する権限を付与する場合があります。

複数のポリシーが単一の機能に対して編集権限と読み取り専用権限を定義している場合、編集権限が読み取り専用権限よりも優先されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleには、次の5つの事前定義されたロールが用意されています。

- **admin_role**。すべてのNetScaler Console機能にアクセスできます。(このロールは `adminpolicy` にバインドされています。)
- **adminExceptSystem_role**。設定権限を除くネットスケーラー コンソール GUIにアクセスできます。(このロールはadminExceptSystem_policyにバインドされています)
- **readonly_role**。読み取り専用アクセス権があります。(このロールは `readonlypolicy` にバインドされています。)
- **appAdmin_role**。NetScaler Console のアプリケーション機能にのみ管理者アクセス権を持ちます。(このロールは appAdminPolicy にバインドされています。).
- **appReadonly_role**。アプリケーション機能への読み取り専用アクセス権を持ちます。(このロールは appReadOnlyPolicy にバインドされています。)

事前定義されたロールを編集することはできませんが、独自の (ユーザー定義の) ロールを作成できます。

ロールを作成し、ポリシーを割り当てるには:

1. NetScaler Console GUI で、**Settings** > **Users & Roles** > **Roles** の順に移動します。
2. **Add** をクリックします。
3. **Create Roles** ページで、**Role Name** フィールドにロールの名前を入力し、**Role Description** フィールドに説明を入力します (オプション)。
4. **Policies** セクションで、1 つ以上のポリシーを **Configured** リストに移動します。

   注:

   ポリシーには、すべてのテナントに固有のテナント ID (例: `maasdocfour`) がプレフィックスとして付けられます。

   注:

   New をクリックしてアクセスポリシーを作成するか、**Settings** > **Users & Roles** > **Access Policies** の順に移動してポリシーを作成できます。

5. **Create** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console でグループを構成する

NetScaler Consoleでは、グループは機能レベルとリソースレベルの両方のアクセス権を持つことができます。たとえば、あるユーザーグループは選択されたNetScalerインスタンスのみにアクセスでき、別のグループは選択された少数のアプリケーションのみにアクセスできる、といった具合です。

グループを作成する際、そのグループにロールを割り当てたり、アプリケーションレベルのアクセス権を付与したり、ユーザーを割り当てたりすることができます。そのグループ内のすべてのユーザーには、NetScaler Consoleで同じアクセス権が割り当てられます。

NetScaler Consoleでは、ネットワーク機能エンティティの個々のレベルでユーザーアクセスを管理できます。エンティティレベルでユーザーまたはグループに特定の権限を動的に割り当てることができます。

NetScaler Consoleは、仮想サーバー、サービス、サービスグループ、およびサーバーをネットワーク機能エンティティとして扱います。

- **仮想サーバー（アプリケーション）** - 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

グループを作成するには：

1. NetScaler Console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。適切な説明を提供することで、グループの役割と機能を理解しやすくなります。
5. **ロール** セクションで、1つ以上のロールを **構成済み** リストに移動します。

> **注:**
>
> 役割には、すべてのテナントで一意のテナントID (例: `maasdocfour`) がプレフィックスとして付加されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. **Available** リストで、**New** または **Edit** をクリックしてロールを作成または変更できます。

   または、**Settings > Users & Roles > Users** に移動して、ユーザーを作成または変更できます。

7. **Next** をクリックします。
8. **Authorization Settings** タブで、次のカテゴリからリソースを選択できます。

   - **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**
   - **IPAMプロバイダーとネットワーク**
   - **StyleBook**
   - **構成パック**
   - **ドメイン名**

   ユーザーがアクセスできるカテゴリから特定のリソースを選択します。

   オートスケールグループ:

   ユーザーが表示または管理できる特定のオートスケールグループを選択するには:

   a. **すべてのオートスケールグループ**チェックボックスをオフにし、**オートスケールグループの追加**をクリックします。
   b. リストから必要なオートスケールグループを選択し、**OK**をクリックします。

   インスタンス:

   ユーザーが表示または管理できる特定のインスタンスを選択するには:

   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。

   タグ:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

関連付けられたタグに基づいて、ユーザーが特定のインスタンスを表示または管理することを許可するには:

a. **すべてのインスタンス**チェックボックスをオフにし、**タグの選択**をクリックします。
b. リストから必要なタグを選択し、**OK**をクリックします。

後で、選択したタグにさらにインスタンスを関連付けると、承認されたユーザーは新しいインスタンスに自動的にアクセスできるようになります。

タグとインスタンスへのタグの関連付けの詳細については、「タグを作成してインスタンスに割り当てる方法」を参照してください。

アプリケーション:

アプリケーションの選択リストでは、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から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 Console 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、ユーザーにアクセスさせたい必要なアプリケーションを追加できます。**アプリケーションの追加**をクリックし、リストから必要なアプリケーションを選択します。
- **個々のエンティティタイプを選択:** 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。

  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を許可できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バインドされたエンティティにも適用オプションは、選択したエンティティタイプにバインドされているエンティティを承認します。たとえば、アプリケーションを選択し、**バインドされたエンティティにも適用**を選択すると、NetScaler Console は選択したアプリケーションにバインドされているすべてのエンティティを承認します。

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 Consoleに保持されます。正規表現を追加するには、次の手順を実行します。

a. **正規表現の追加**をクリックします。

b. テキストボックスに正規表現を指定します。

次の画像は、**特定のアプリケーション**オプションを選択したときに、正規表現を使用してアプリケーションを追加する方法を示しています。

次の画像は、**個々のエンティティタイプを選択**オプションを選択したときに、正規表現を使用してネットワーク機能エンティティを追加する方法を示しています。

さらに正規表現を追加する場合は、**+**アイコンをクリックします。

注：

正規表現は、**サーバー**エンティティタイプの場合、サーバー名のみに一致し、サーバーIPアドレスには一致しません。

検出されたエンティティに対して**バインドされたエンティティにも適用**オプションを選択すると、ユーザーは検出されたエンティティにバインドされているエンティティに自動的にアクセスできます。

正規表現は、承認スコープを更新するためにシステムに保存されます。新しいエンティティがそのエンティティタイプの正規表現に一致すると、NetScaler Consoleは承認スコープを新しいエンティティに更新します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成テンプレート:

ユーザーが表示または管理できる特定の構成テンプレートを選択する場合は、次の手順を実行します。

a. **すべての構成テンプレート**をクリアし、**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。

IPAMプロバイダーとネットワーク:

ユーザーが表示または管理できる特定のIPAMプロバイダーとネットワークを追加する場合は、以下を実行します。

- **プロバイダーの追加** - **すべてのプロバイダー**をクリアし、**プロバイダーの追加**をクリックします。必要なプロバイダーを選択し、**OK**をクリックできます。
- **ネットワークの追加** - **すべてのネットワーク**をクリアし、**ネットワークの追加**をクリックします。必要なネットワークを選択し、**OK**をクリックできます。

StyleBook:

ユーザーが表示または管理できる特定のStyleBookを選択する場合は、次の手順を実行します。

a. **すべてのStyleBook**チェックボックスをオフにし、**グループにStyleBookを追加**をクリックします。個々のStyleBookを選択するか、フィルタークエリを指定してStyleBookを承認できます。

個々のStyleBookを選択したい場合は、**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ます。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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名が`lb-mon`または`lb`のいずれかです。
- StyleBook namespace は `com.citrix.adc.stylebooks` です。
- StyleBook version 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` のいずれかである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。

保存されたクエリは、**Custom Filters Query** に表示されます。保存されたクエリに基づいて、NetScaler Console はそれらの StyleBook へのユーザーアクセスを提供します。

b. リストから必要な StyleBook を選択し、**OK** をクリックします。

グループを作成し、そのグループにユーザーを追加する際に、必要な StyleBook を選択できます。ユーザーが許可された StyleBook を選択すると、すべての依存 StyleBook も選択されます。

構成パック:

構成パックで、次のいずれかのオプションを選択します。

- **すべての構成**: このオプションはデフォルトで選択されています。これにより、ユーザーはADM内のすべての構成を管理できます。
- **選択したStyleBookのすべての構成**: このオプションは、選択したStyleBookのすべての構成パックを追加します。
- **特定の構成**: このオプションを使用すると、任意のStyleBookの特定の構成を追加できます。
- **ユーザーグループによって作成されたすべての構成**: このオプションを使用すると、ユーザーは同じグループのユーザーによって作成された構成のみにアクセスできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

グループを作成し、そのグループにユーザーを割り当てる際に、該当する構成パックを選択できます。

ドメイン名:

ユーザーが表示または管理できる特定のドメイン名を選択する場合は、次の手順を実行します。

a. **すべてのドメイン名**チェックボックスをオフにし、**ドメイン名の追加**をクリックします。
b. リストから必要なドメイン名を選択し、**OK**をクリックします。
c. **グループの作成**をクリックします。
d. **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、新しいユーザーを追加することもできます。

ユーザーの割り当て(/en-us/netscaler-console-service/media/ns-assign-users.png)

a. **完了**をクリックします。

承認スコープに基づいてユーザーアクセスがどのように変化するか

管理者が異なるアクセスポリシー設定を持つグループにユーザーを追加すると、そのユーザーは複数の承認スコープとアクセスポリシーにマッピングされます。

この場合、NetScaler Console は、特定の承認スコープに応じて、ユーザーにアプリケーションへのアクセスを許可します。

Policy-1 と Policy-2 の2つのポリシーを持つグループに割り当てられているユーザーを考えてみましょう。

- **Policy-1** – アプリケーションへの表示のみの権限。
- **Policy-2** – アプリケーションへの表示および編集権限。

承認スコープによるユーザーアクセスの変更(/en-us/netscaler-console-service/media/user-authorization-with-user-authorization-scopes.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーは Policy-1 で指定されたアプリケーションを表示できます。また、このユーザーは Policy-2 で指定されたアプリケーションを表示および編集できます。Group-1 アプリケーションへの編集アクセスは、Group-1 の承認スコープに含まれないため制限されます。

制限事項

以下の NetScaler Console 機能は、RBAC を完全にサポートしていません。

- **Analytics** - 分析モジュールは RBAC を完全にサポートしていません。RBAC のサポートはインスタンスレベルに限定されており、Gateway Insight、HDX™ Insight、および Security Insight の分析モジュールではアプリケーションレベルには適用されません。
  - 例 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、**HDX Insight** > **Devices** の下にそれらのインスタンスのみを表示でき、**HDX Insight** > **Applications** の下には対応する仮想サーバーのみを表示できます。これは、RBAC がインスタンスレベルでサポートされているためです。
  - 例 2: アプリケーションベースの RBAC (サポート対象外)。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、**HDX Insight** > **Applications** の下のすべての仮想サーバーを表示できますが、それらにアクセスすることはできません。これは、RBAC がアプリケーションレベルでサポートされていないためです。
- **StyleBooks** – StyleBooks では RBAC が完全にサポートされていません。
  - 多くのユーザーが単一の StyleBook にアクセスできるが、異なる NetScaler インスタンスへのアクセス権限を持っている状況を考えてみましょう。ユーザーは、自分以外のインスタンスにアクセスできないため、自分のインスタンスで構成パックを作成および更新できます。しかし、自分以外の NetScaler インスタンスで作成された構成パックやオブジェクトは引き続き表示できます。

管理対象のNetScalerインスタンスにネットプロファイルを割り当てる

NetScaler Consoleで仮想サーバーの分析またはメトリクスコレクターを有効にすると、NetScalerからのAppFlowまたはメトリクスデータは、NetScalerサブネットIPアドレス（SNIP）を介してNetScaler Consoleにエクスポートされます。シナリオによっては、ネットワーク内のファイアウォールによってSNIPがブロックされる場合があります。そのようなシナリオでは、別のIPアドレスを使用する必要がある場合があります。ネットプロファイルの詳細については、「バックエンド通信に指定されたソースIPを使用する」(/ja-jp/citrix-adc/current-release/load-balancing/load-balancing-manage-clienttraffic/use-specified-srcip.html)を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerからNetScaler ConsoleにAppFlowデータをエクスポートするために、NetScaler Consoleを介してNetScalerインスタンスにネットプロファイルを割り当てることができます。

前提条件

以下を確認してください。

- NetScalerインスタンスのバージョンが**13.0-48.4以降**であること。
- ネットプロファイルがNetScalerインスタンスで構成されていること。

NetScaler Consoleでネットプロファイルを割り当てるには：

1. **Infrastructure > Instances > NetScaler**に移動します。
2. インスタンスを選択し、**Select Action**リストから：
   - **Configure Net Profiles**をクリックして、AppFlowのネットプロファイルを割り当てます。
   - **Configure Net Profiles for Metrics Collector**をクリックして、メトリクスコレクターのネットプロファイルを割り当てます。
3. リストからネットプロファイルを選択し、**Apply**をクリックします。

注：

- AppFlowの場合、インスタンスにネットプロファイルを割り当てる前に、すべての仮想サーバーの分析を無効にしてください。
- Metrics Collectorについては、インスタンスにネットプロファイルを割り当てる前に、すべての仮想サーバーのメトリクスを無効にしてください。

データストレージ管理

NetScaler Consoleでどの機能が使用されているか、およびそれぞれの機能のデータ使用量を把握することが重要です。**データストレージ管理**ダッシュボードは、この目的のために、NetScaler Consoleデータベースに保存されている様々な機能の総データ量を理解するための視覚化ツールとして機能します。このダッシュボードは、消費されたストレージが指定された制限内にあるか、または割り当てられたストレージを超えているかどうかも示します。

管理者として、**データストレージ管理**ダッシュボードで次のタスクを実行できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 過去30日間のデータストレージ消費量を表示 - データストレージの傾向は、過去30日間、NetScaler Consoleデータベースに保存されます。これらの傾向は、グラフ形式または表形式で利用できます。これらの傾向は、NetScaler Consoleでスケジュールされたプルーニングサイクル後に、どれだけのデータが取り込まれ、どれだけのデータが保存されているかを示します。
- データ取り込みステータスの表示 - データ取り込みアクティビティは、消費されたストレージが割り当てられたストレージの制限内にある限り行われます。消費されたストレージが割り当てられたストレージを超えると、データアクティビティは一時停止されます。
- 通知の送信 - 消費されたストレージが割り当てられたストレージの75%または100%に達したときに通知が送信されるように設定でき、ユーザーがストレージを管理できるようになります。
- データストレージスペースを管理する柔軟性 - 削除または削減に適していると判断したデータをプルーニングすることで、保存されているデータ内にさらにスペースを作成できます。

データストレージダッシュボードを表示するには、**Settings > Data Storage**に移動します。

以下のセクションでは、効果的なデータストレージ管理のために**データストレージ管理**ダッシュボードを使用する方法について概説します。

- データストレージを理解する - このセクションでは、ダッシュボードを使用してデータストレージに関する情報を表示する方法を理解するのに役立ちます。
- データストレージを管理する - このセクションでは、データストレージを管理するためにダッシュボードで実行できるアクションに関する情報を提供します。

データストレージを理解する

NetScaler Consoleの**データストレージ管理**ダッシュボードを使用して、データストレージの使用状況を追跡するのに役立つデータとグラフを表示できます。

データストレージの消費量を監視するには、**設定 > データストレージ**に移動します。

データストレージ管理ダッシュボードには、次の情報が表示されます。

- データ取り込みアクティビティの状態
- 総ストレージ消費量
- データプルーニングステータス
- ストレージ消費トレンド
- 機能別ストレージ消費量

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データ取り込みアクティビティの状態

データ取り込みとは、イベント、Syslog、ネットワークレポートなどのさまざまな機能を通じて、管理対象のすべてのNetScalerインスタンスから大量の多様なデータをNetScaler Consoleストレージにインポートするプロセスを指します。

データ取り込みステータスは、NetScaler ConsoleがNetScalerインスタンスから統計情報を収集しているかどうかを示します。データ取り込みアクティビティは、消費されたストレージが許可されたストレージ内にある限り継続されます。消費量が許可されたストレージを超えると、データ取り込みは一時停止されます。

データ取り込みタイルを表示して、データ取り込みの現在の状態を把握します。このタイルには、次のいずれかの状態が表示されます。

- **アクティブ** - データ取り込みアクティビティが進行中です。

- **一時停止** - 消費されたストレージが許容ストレージを超過したため、データ取り込みアクティビティが一時停止されています。

一時停止されたデータ取り込みを再開する方法

データ取り込みアクティビティを再開するには、次のいずれかの操作を実行できます。

- データストレージを追加する。
- データプルーニングを実行する。

総ストレージ消費量

データストレージの概要を素早く確認するには、**ストレージ消費量**タイルを表示します。

ストレージ消費量タイルには、デプロイ内のすべての機能で使用されている総ストレージが表示されます。

ドーナツグラフにカーソルを合わせると、以下が表示されます。

許容ストレージ

許容ストレージとは、ライセンスに基づいて使用できるストレージの合計です。Expressライセンスをお持ちの場合、500 MBの許容ストレージが提供されます。Advancedライセンスをお持ちの場合、購入したVIPごとに500 MBのストレージと、VIPを購入せずに直接購入した追加ストレージの合計が提供されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次のシナリオを考慮してください。

- 20個のVIPを購入しました。各VIPにつき500 MBの無料ストレージが提供されます。お客様の利用可能なストレージは20*500 = 10 GBです。
- 20個のVIPと5 GBの追加ストレージを購入しました。各VIPにつき500 MBの無料ストレージが提供されます。お客様の利用可能なストレージは20*500 + 5 = 15 GBです。

消費済みストレージ

消費済みストレージとは、展開内のすべての機能で使用されるストレージの合計です。以下の色分け基準は、機能によって使用されるストレージの量を指定します。

- **緑** - 消費済みストレージが利用可能なストレージの75%未満です。
- **琥珀色** - 消費済みストレージが利用可能なストレージの75%から99%の間です。
- **赤** - 消費済みストレージの制限に達したか、現在の利用可能なストレージを超えています。

データプルーニングのステータス

プルーニングとは、データを手動で削除してストレージスペースを解放するプロセスです。毎月10回のデータプルーニングが許可されています。たとえば、7月1日から7月31日までの間にデータを10回削除できます。

使用済みのデータプルーニングの回数と残りの回数を知るには、**データプルーニング**タイルを表示します。

注:

選択された機能の数に関係なく、各プルーニングアクティビティは1回のデータプルーニングとしてカウントされます。

ストレージ消費の傾向

過去30日間のデータ消費状況を知るには、**ストレージ消費傾向**セクションを表示します。

ストレージ消費傾向は、どの機能が一定期間に最も多くのストレージを使用しているか、または最も少ないストレージを使用しているかについての洞察を提供し、データストレージの使用量を効果的に管理するのに役立ちます。

ストレージデータの傾向は、以下のいずれかの形式で表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **グラフィカルビュー** – データストレージがさまざまなNetScaler Console機能にどのように分散されているかを表示します。タイムラインにマウスを合わせると、その月の任意の日付のデータストレージ情報を表示できます。

  注:

  グラフィカルビューがデフォルトのビューです。

- **表形式ビュー** – 「**表形式ビュー**」をクリックすると、データストレージ情報が表形式で表示されます。

  注:

  表形式ビューでは、検索フィールドを使用してデータをフィルタリングできます。

次の表は、「**ストレージ消費傾向**」セクションに表示されるフィールドについて説明しています。

機能	説明
構成	インスタンス、構成ジョブ、構成監査などに関する、すべての構成可能なデータが含まれます。
HDX インサイト	NetScalerを通過するICAトラフィックに対してエンドツーエンドの可視性を提供します。
ネットワーク レポーティング	すべてのNetScalerインスタンスのネットワークパフォーマンスを表示します。
Web インサイト	エンタープライズWebアプリケーションへの可視性を提供し、アプリケーションの統合されたリアルタイム監視を可能にします。
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ステータスを評価し、アプリケーションを保護するための修正措置を講じるのに役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能	説明
ゲートウェイ インサイト	NetScaler Gatewayへのログオン時に、アクセスモードに関係なく、すべてのユーザーが遭遇した障害に対する可視性を提供します。
イベント	NetScalerインスタンス上のイベントまたはエラーの発生を監視および管理します。
アプリ ダッシュボード	アプリケーションの表示および管理を可能にします。
ボット インサイト	ボット違反とその違反に対して取られたアクションを可視化します。
システムログ	デバイスがすべてのsyslogメッセージをNetScaler Consoleにリダイレクトするように構成されている場合、NetScalerインスタンスで生成されたsyslogイベントを監視します。
ビデオインサイト	NetScalerインスタンスで使用されるビデオ最適化技術のメトリックを監視します。
詳細トランザクション	Webトランザクションを可視化し、クライアント、NetScaler、サーバーに分割された応答時間メトリックを視覚的に表示します。

機能別のストレージ消費量

データストレージがさまざまな機能にどのように分散されているかについて詳しく知るには、「**Storage Consumption by features as on *dd mmm***」セクションを参照してください。

「**Storage Consumption by features as on *dd mmm***」は、以下の理解に役立ちます。

- NetScaler Consoleのすべての異なる機能で使用されるストレージスペース
- 特定の日に機能が消費するスペースの割合

機能と説明の図(/en-us/netscaler-console-service/media/data-storage-distribution.png)

テーブルのエントリをソートしたい場合は、テーブルのヘッダーを使用します。NetScaler Consoleは、選択した列のデータに基づいて、テーブルを上から下へ英数字順にソートします。テーブルを逆順にソートするには、列見出しをもう一度クリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データのプルーニング、プルーニング履歴、およびストレージイベントログの詳細については、「データのストレージを管理する」を参照してください。

ストレージスペースを管理する

データストレージ管理ダッシュボードを使用して、データストレージの使用状況を監視し、データストレージがライセンス制限を超過した場合にスペースを解放したりストレージを増やしたりするために必要なアクションを実行できます。

アクション(/en-us/netscaler-console-service/media/data-storage-actions.png)

アクションタイルには、ストレージ容量を管理するために実行できる推奨手順のリストが表示されます。

- データ保持ポリシーを確認する
- データプルーニングを実行する
- ストレージ制限超過時に通知する

消費されたストレージがライセンスされたストレージの100%に達すると、データ取り込みアクティビティは一時停止され、データはNetScaler Consoleに保存されなくなります。

データプルーニングを実行する

ストレージリソースを最適化し、より多くのストレージスペースを確保するためにデータをプルーニングします。スペースを解放するだけでなく、データプルーニングはデータ品質を向上させ、処理時間を短縮します。不要なデータを定期的に確認し、パージすることをお勧めします。このプロセスにより、リソースが適切に使用され、NetScaler Consoleが俊敏で応答性が高くなります。

データをプルーニングするには：

1. **データストレージ管理**ページで、***yyyy-mm-dd時点の機能別ストレージ消費量***セクションまでスクロールします。
2. 1つ以上の機能を選択し、**プルーニング**をクリックします。**Config**はすべてのシステム構成を含むため、選択できません。

   ポップアップウィンドウが表示され、選択した機能のすべてのデータを削除するかどうかを確認します。**はい、プルーニング**をクリックします。

   機能と説明(/en-us/netscaler-console-service/media/prune-data-message.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

ポップアップウィンドウには、現在のプルーニング試行に関する情報も表示されます。

プルーン履歴の表示

をクリックすると、NetScaler Console で実行したすべてのプルーンアクティビティの詳細が表示されます。

タスクログ(/en-us/netscaler-console-service/media/view-prune-history-tasks.png)

ページには、すべてのプルーンタスクのリストと、それぞれのステータス、開始時刻、終了時刻が表示されます。

各プルーン操作でどの機能が削除されたかを理解するには、タスクを選択し、 をクリックします。

機能ログ(/en-us/netscaler-console-service/media/view-prune-history-feature.png)

ストレージイベントログの表示

をクリックすると、データがライセンス制限の 75% を超えた、または達したすべての時点に関するインサイトが得られます。

機能ログ(/en-us/netscaler-console-service/media/data-ingestion-history.png)

データ保持ポリシーの確認

データ保持ポリシーとは、NetScaler Console が履歴データを時間の経過とともに管理および維持する方法を決定する一連のルールと構成を指します。このポリシーは、データが自動的に削除されるまでにデータが保存される期間を概説します。

すべての異なる機能で使用されるストレージスペースを削減したい場合は、NetScaler Console でデータを保持する期間を変更できます。

ページを使用して、次のデータストレージ設定を編集します。

- イベントメッセージ
- Syslogメッセージ
- ネットワークレポートデータ

データストレージ設定の詳細については、「データ保持ポリシー」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ストレージ制限超過時の通知

NetScaler Consoleで、データストレージ容量が指定された制限を超過した場合にアラートを送信する通知を設定できます。

システム通知を表示および設定するには：

1. **アクション**タイルで、**ストレージ制限超過時の通知**をクリックします。
2. **システム通知の設定**ページで、**システムイベントカテゴリ**の下にある**DataStorageExceeded**カテゴリが通知を受信するように選択されていることを確認します。

通知がいつ、どのようにあなたや他のユーザーに送信されるかに関連するさまざまなパラメータを指定できます。優先する通信方法（例：メール、Slack、PagerDuty、ServiceNow通知）を選択し、通知の受信者を定義します。

プロファイルの設定方法と通知の送信方法の詳細については、「通知の設定」を参照してください。

データ保持ポリシー

NetScaler Consoleでは、システムイベント、syslogメッセージ、およびネットワークレポートデータを特定の期間アクセスできます。

1. データ保持を設定するには、 **> >** の順に移動します。
2. 編集ボタンをクリックします。
3. 以下の各オプションについて、NetScaler Consoleでデータを保持する日数を入力します。

オプション	説明
イベント	NetScaler Consoleに保存されるイベントメッセージを最大40日間に制限できます。保持ポリシーの有効期限が切れると、イベントはNetScaler Consoleから削除されます。クリアされたイベントは1日後に削除されます。
シスログ	データベースに保存されるsyslogデータの量を最大180日間に制限できます。
ネットワークレポート	NetScaler Consoleに保存されるネットワークレポートデータを最大30日間に制限できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

Expressアカウントでは、データ保持ポリシーを編集できません。

アカウントがExpressアカウントに変換されると、NetScaler Consoleはストレージデータを500 MBまたは1日分のデータのいずれか少ない方を保持します。詳細については、Expressアカウントを使用したNetScaler Consoleリソースの管理を参照してください。

システムアラームの設定と表示

NetScaler Consoleサーバーの健全性を監視するために、一連のアラームを有効にして設定できます。重要な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設定する必要があります。

例えば、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と思うかもしれません。cpuUsageHighやmemoryUsageHighなどの一部のアラームカテゴリでは、しきい値を設定し、それぞれの重大度（CriticalやMajorなど）を定義できます。inventoryFailedやloginFailureなどの一部のカテゴリでは、重大度のみを定義できます。アラームカテゴリのしきい値が破られた場合（例：memoryUsageHigh）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）には、メッセージがシステムに記録され、そのメッセージをsyslogメッセージとして表示できます。さらに、アラーム設定に応じて電子メールまたはSMS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るか変更できます。割り当て可能な重大度レベルは、Critical、Major、Minor、Warning、およびInformationalです。

アラームを設定する

バックアップの失敗を監視したいシナリオを考えてみましょう。backupFailedアラームを有効にし、Majorなどの重大度を割り当てることができます。NetScaler Consoleがシステムファイルのバックアップを試行し、その試行が失敗すると、アラームがトリガーされます。NetScaler Consoleのログメッセージページでメッセージを表示したり、電子メールまたはSMSで通知を受け取ったりできます。

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。アラームはデフォルトで有効になっています。

NetScaler Consoleを使用してシステムアラームを設定および表示するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Settings > SNMP**に移動します。右上隅にある**Alarms**をクリックします。

   アラーム(/en-us/netscaler-console-service/media/snmp-alarms-settings.png)

2. 設定したいアラーム（例：cpuUsageHigh）を選択し、**Edit**をクリックして設定を変更します。

   アラームの編集(/en-us/netscaler-console-service/media/snmp-alarms-edit.png)

3. **Configure Alarm**ページで、アラートを作成するために**Enable Alarm**を選択し、次の項目を指定します。

   - **時間**。アラームをトリガーしたい時間（分単位）を入力します。
   - **重大度**。重大度レベルを選択します。
   - **アラームしきい値**。アラームがトリガーされ、アラートが送信される値を入力します。

   OK をクリックします。

注:

一部のアラーム（例: backupFailed）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。

アラームによって生成されたイベント（例: backupFailed）を表示するには:

1. **設定** > **監査ログメッセージ** に移動します。
2. 検索フィールドで、アラームの種類を選択します。この例では、**イベント**、**=** (特定の値に等しい)、そして **BACKUPFAILED** を選択します。

   バックアップ失敗アラーム(/en-us/netscaler-console-service/media/snmp-alarms-select.png)

   バックアップ失敗のために生成されたイベントが表示されます。

   バックアップ失敗アラーム(/en-us/netscaler-console-service/media/backup-failure-message.png)

   アラームがトリガーされたときに、メールまたはSMS（ショートメッセージサービス）テキストを受信する通知を設定することもできます。

ディスク使用率アラームにしきい値制限を追加する

ディスク使用率アラームは、NetScaler Consoleサーバーで使用されているディスク容量が事前定義されたしきい値を超えたときにトリガーされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理者として、アラートを受信した際に、不要なデータを削除するか、追加のストレージリソースを割り当てて、サービスの中断やパフォーマンスの低下を防ぐことができます。

リリース14.1ビルド25x以降、ディスク使用率アラームに下位レベルのしきい値を追加することもできます。このしきい値を使用すると、上位のしきい値制限が侵害される前にアラートを受信する下位レベルの制限を設定できます。

下位レベルのしきい値を設定するには：

1. **Settings > SNMP > Alarms** に移動し、検索フィールドに diskUtilizationHigh と入力して、ディスク使用率アラームを表示します。
2. アラームを選択し、**Edit** をクリックします。
3. **Configure Alarm** ページで、**Configure a lower-level threshold** を選択します。下位レベルのしきい値制限を入力します。

例えば、ディスク使用率の下位しきい値を60、上位しきい値を80に設定した場合、ディスク使用量がディスク容量の60%を超えるとアラートを受信します。この設定により、ディスク使用率が80%に達する前に是正措置を講じることができます。

可観測性統合

現代のアプリケーションの複雑さが増しているため、管理者は次の課題に直面しています。

- アプリケーションの監視とトラブルシューティング。
- インフラストラクチャとアプリケーションの動作の可視化。

可観測性は、インフラストラクチャ全体にこれらの洞察を提供することで、このギャップを埋めます。NetScaler Console の可観測性統合機能を使用すると、次のことができます。

- NetScaler Console を Splunk と統合する。
- NetScaler Console を New Relic と統合する。
- NetScaler Console を Microsoft Sentinel と統合する
- デフォルトスキーマを使用して、洞察を Prometheus にエクスポートするように NetScaler インスタンスを構成する。

Splunkとの統合

NetScaler ConsoleをSplunkと統合して、以下の分析を表示できるようになりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WAF違反
- ボット違反
- SSL証明書のインサイト
- ゲートウェイのインサイト
- NetScaler® Console監査ログ

Splunkアドオンを使用すると、次のことが可能になります。

- 他のすべての外部データソースを結合します。
- 分析の可視性を一元的に高めます。

NetScaler Consoleは、ボット、WAF、SSL、ゲートウェイ、監査ログのイベントを収集し、定期的にSplunkに送信します。Splunk Common Information Model (CIM) アドオンは、これらのイベントを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 ConsoleからデータをSplunkを構成する
- NetScaler ConsoleからSplunkにデータをエクスポートするように構成する
- Splunkでダッシュボードを表示する

SplunkがNetScaler Consoleからデータを受信するように構成する

Splunkでは、次の操作を行う必要があります。

1. Splunk HTTPイベントコレクターエンドポイントを設定し、トークンを生成する
2. Splunk Common Information Model (CIM) アドオンをインストールする
3. CIMノーマライザーをインストールする（WAFおよびボットインサイトにのみ適用）
4. Splunkでサンプルダッシュボードを準備する

Splunk HTTPイベントコレクターエンドポイントを設定し、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、NetScaler ConsoleとSplunk間の統合が可能になり、WAFまたはボットデータを送信できます。次に、Splunkでトークンを生成して、次の操作を行います。

- NetScaler ConsoleとSplunk間の認証を有効にします。
- イベントコレクターエンドポイントを介してデータを受信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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「なし」として選択されています。

    e. **インデクサーの確認を有効にする**: NetScaler Consoleはこのオプションをサポートしていません。このオプションを選択しないことをお勧めします。

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. エントリを確認するために**レビュー**をクリックし、**送信**をクリックします。

    トークンが生成されます。NetScaler Consoleで詳細を追加する際に、このトークンを使用する必要があります。

Splunk共通情報モデルをインストールする

Splunkでは、Splunk CIMアドオンをインストールする必要があります。このアドオンは、NetScaler Consoleから受信したデータを取り込み、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、取り込まれたデータを正規化し、共通の標準に一致させることを保証します。

注:

Splunk CIMアドオンをすでにインストールしている場合は、この手順を無視できます。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 検索バーに「**CIM**」と入力し、**Enter**キーを押して「**Splunk Common Information Model (CIM)**」アドオンを取得し、「**Install**」をクリックします。

CIMノーマライザーをインストールする

CIMノーマライザーは、SplunkでWAFとボットのインサイトを表示するためにインストールする必要がある追加のプラグインです。

1. Splunkポータルで、**Apps > Find More Apps**に移動します。

2. 検索バーに**ADMサービスイベント/データ用のCIM正規化**と入力し、**Enter**キーを押してアドオンを取得し、**インストール**をクリックします。

Splunkでサンプルダッシュボードを準備する

Splunk CIMをインストールしたら、WAFとボット、およびSSL証明書インサイト用のテンプレートを使用してサンプルダッシュボードを準備する必要があります。ダッシュボードテンプレート(`.tgz`) ファイルをダウンロードし、任意のテキストエディター (例: メモ帳) を使用してその内容をコピーし、Splunkにデータを貼り付けてダッシュボードを作成できます。

注:

サンプルダッシュボードを作成するための以下の手順は、WAFとボット、およびSSL証明書インサイトの両方に適用されます。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、可観測性統合で利用可能な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。

注記:

抽出後、2つの`json`ファイルが得られます。
`adm_splunk_security_violations.json`を使用してWAFおよびBotのサンプルダッシュボードを作成し、`adm_splunk_ssl_certificate.json`を使用してSSL証明書インサイトのサンプルダッシュボードを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Splunkポータルで、**Search & Reporting > Dashboards**に移動し、次に**Create New Dashboard**をクリックします。

4. **Create New Dashboard**ページで、次のパラメータを指定します。

   a. **ダッシュボードのタイトル** - 任意のタイトルを指定します。

   b. **説明** - 必要に応じて、参照用に説明を指定できます。

   c. **権限** - 要件に基づいて、**Private**または**Shared in App**を選択します。

   d. **Dashboard Studio**を選択します。

   e. いずれかのレイアウト（**Absolute**または**Grid**）を選択し、**Create**をクリックします。

      Createをクリックした後、レイアウトから**Source**アイコンを選択します。

5. 既存のデータを削除し、ステップ2でコピーしたデータを貼り付け、**Back**をクリックします。
6. **Save**をクリックします。

   Splunkで以下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-console-service/media/splunk-sample-dashboard.png)

NetScaler Consoleを構成してSplunkにデータをエクスポートする

Splunkでの準備はすべて整いました。最後のステップは、サブスクリプションを作成し、トークンを追加してNetScaler Consoleを構成することです。

以下の手順が完了すると、NetScaler Consoleで現在利用可能な更新されたダッシュボードをSplunkで表示できます。

1. NetScaler Consoleにログオンします。
2. **Settings > Observability Integration** に移動します。
3. **Integrations** ページで、**Add** をクリックします。
4. **Create Subscription** ページで、以下の詳細を指定します。

   a. **Subscription Name** フィールドに任意の名前を指定します。

   b. **Source** として **NetScaler Console** を選択し、**Next** をクリックします。

   c. **Splunk** を選択し、**Configure** をクリックします。**Configure Endpoint** ページで、:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. **End Point URL** – Splunk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://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用に設定された有効なIPアドレス。
- **SPLUNK_HEC_PORT** – HTTPイベントエンドポイント設定時に指定したポート番号を示します。デフォルトのポート番号は8088です。
- **Services/collector/event** – HECアプリケーションのパスを示します。

ii. **認証トークン** – Splunkから認証トークンをコピーして貼り付けます。

iii. **Submit**をクリックします。

d. **Next**をクリックします。

e. **Add Insights**をクリックし、**Select Feature**タブで、エクスポートしたい機能を選択して**Add Selected**をクリックします。

> **注:**
>
> **NetScaler Console Audit Logs**を選択した場合、監査ログをSplunkにエクスポートする頻度として**Daily**または**Hourly**を選択できます。

f. **Next**をクリックします。

g. **Select Instance**タブで、**Select All Instances**または**Custom select**のいずれかを選択し、**Next**をクリックします。

- **Select All Instances** - すべてのNetScalerインスタンスからSplunkにデータをエクスポートします。
- **Custom select** - リストからNetScalerインスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択されたNetScalerインスタンスからのみSplunkにエクスポートされます。

h. **Submit**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注:**
>
> 選択したインサイトのデータは、NetScaler Consoleで違反が検出されるとすぐに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 Console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。

- [ ] 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。

- [ ] ダッシュボードとは別に、サブスクリプションを作成した後、Splunkでデータを表示することもできます。

1. Splunkで、**Search & Reporting**をクリックします。
2. 検索バーで:

   - `sourcetype="bot"`または`sourcetype="waf"`と入力し、リストから期間を選択して、ボット/WAFデータを表示します。
   - `sourcetype="ssl"`と入力し、リストから期間を選択して、SSL証明書インサイトデータを表示します。
   - `sourcetype="gateway_insights"`と入力し、リストから期間を選択して、Gatewayインサイトデータを表示します。
   - `sourcetype= "audit_logs"`と入力し、リストから期間を選択して、監査ログデータを表示します。

New Relicとの統合

NetScaler ConsoleをNew Relicと統合できるようになり、New RelicダッシュボードでWAF、Bot、SSL、Gateway Insights、およびNetScaler Consoleの監査ログの分析を表示できます。この統合により、次のことが可能になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- New Relicダッシュボードで他のすべての外部データソースを結合する。
- 一元化された場所で分析の可視性を得る。

NetScaler Consoleは、Bot、WAF、SSL、Gateway Insights、およびNetScaler Consoleの監査ログイベントを収集し、それらをNew Relicに即座に送信します。管理者として、これらのイベントをNew Relicダッシュボードで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する:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  イベントエンドポイントの構成の詳細については、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 Consoleでキーの詳細を追加する

NetScaler Consoleでキーの詳細を追加する

トークンを生成したら、New Relicと統合するためにNetScaler Consoleで詳細を追加する必要があります。

1. NetScaler Consoleにログオンします。
2. **Settings > Observability Integration**に移動します。
3. **Integrations**ページで、**Add**をクリックします。
4. **Create Subscription**ページで、次の詳細を指定します。
   a. **Subscription Name**フィールドに任意の名前を指定します。
   b. **Source**として**NetScaler® Console**を選択し、**Next**をクリックします。
   c. **New Relic**を選択し、**Configure**をクリックします。**Configure Endpoint**ページで、次のようにします。
      i. **End Point URL** – 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

セキュリティ上の理由から、HTTPSを使用することをお勧めします。

d. **Authentication token** – New Relicから認証トークンをコピーして貼り付けます。

   i. **Submit**をクリックします。

e. **Next**をクリックします。

f. **Add Insights**をクリックし、**Select Feature**タブで、エクスポートする機能を選択して**Add Selected**をクリックします。

注:

「**NetScaler Console Audit Logs**」を選択した場合、New Relic に監査ログをエクスポートする頻度として「**Daily**」または「**Hourly**」を選択できます。

g. 「**Next**」をクリックします。

h. 「**Select Instance**」タブで、「**Select All Instances**」または「**Custom select**」を選択し、「**Next**」をクリックします。

- **Select All Instances** - すべてのNetScalerインスタンスからNew Relicにデータをエクスポートします。
- **Custom select** - リストからNetScalerインスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択したNetScalerインスタンスからのみNew Relicにエクスポートされます。

i. 「**Submit**」をクリックします。

注:

- 選択したインサイトのデータは、NetScaler Console で違反が検出されるとすぐに New Relic にプッシュされます。

設定が完了しました。「**Subscriptions**」ページで詳細を表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、「**Metrics & events**」の下で、以下のJSON形式でイベントの詳細を表示できます。

`<subsription_name>_adm_<event name>` ここで、イベント名はBot、WAFなどになります。

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、取り込まれたデータに基づいてクエリを構築することで、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。

ダッシュボードの例(/en-us/netscaler-console-service/media/new-relic-example-dashboard.png)

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ユニークな攻撃の総数

  `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: ユニークなボットタイプの総数およびそのカウント

  `SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago`

- ウィジェット 4: ボット違反を検出しているユニークなアプリ名の総数

  `SELECT uniques(appname) from <event_name> since 30 days ago`

Microsoft Sentinelとの統合

NetScaler ConsoleからMicrosoft Sentinelに以下の分析データをエクスポートするために、NetScaler ConsoleをMicrosoft Sentinelと統合できます。

- WAF違反
- ボット違反

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSL証明書のインサイト
- ゲートウェイインサイト
- NetScaler® Console監査ログ

Microsoft Sentinelは、アプリケーションやサーバーなど、さまざまなソースからデータを収集する一元化されたデータ収集機能を提供します。管理者として、インサイトや違反がMicrosoft Sentinelで報告された後、データを表示し、意思決定を行うことができます。

統合を成功させるには、アクティブなAzureサブスクリプションがあることを確認し、各セクションの手順に従ってください。

Log Analyticsワークスペースを構成する

収集されたデータを保存および分析するには、Log Analyticsワークスペースが必要です。

1. Azureにログインします。
2. **リソースの作成**をクリックします。

3. 検索バーに「log analytics workspace」と入力し、**Log Analytics Workspace**の下にある**作成**をクリックします。

4. **Log Analytics Workspace** のメインページで、**Create** をクリックします。

5. **Log Analytics ワークスペースの作成**で:

   a. アクティブなサブスクリプションとリソースグループを選択します。

   > **注:**
   >
   > 権限がある場合は、**新規作成**をクリックしてリソースグループを追加することもできます。

   b. 任意の名前を指定します。

   c. リストから地域を選択します。

   d. **確認 + 作成**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. 検証成功メッセージが表示されます。**作成**をクリックしてワークスペースをデプロイします。

f. デプロイの進行状況メッセージが表示されます。デプロイ完了メッセージが表示されたら、**リソースに移動**をクリックします。

ワークスペースが正常に作成されました。

Microsoft Entra アプリケーションを作成する

Log Analytics Workspace の代わりに通信するには、Azure サブスクリプションに関連付けられた Entra アプリケーションを作成する必要があります。アプリケーションを作成したら、**Microsoft Sentinel Contributor** ロールでアクセス許可を付与する必要もあります。アプリケーションは、**クライアント ID**、**テナント ID**、**クライアント シークレット**などの詳細も提供します。これらの詳細をメモしておくことをお勧めします。これらの詳細は、統合プロセスを完了するために NetScaler Console でサブスクリプションを作成する際に必要になります。

1. Azure ポータルで、検索バーにキーワードを入力します。
2. **Microsoft Entra ID** をクリックします。

3. **追加**をクリックし、**アプリの登録**を選択します。

4. アプリの名前を指定し、**サポートされているアカウントの種類**の下にあるデフォルトのオプションを選択し、**登録**をクリックします。

5. アプリケーションを登録したら:

a. **クライアント ID** と **テナント ID** をメモします。

b. アプリケーションのシークレット ID を作成します。**証明書とシークレット**をクリックし、**クライアント シークレット**の下にある**新しいクライアント シークレット**をクリックします。説明と有効期間を指定し、**追加**をクリックしてアプリケーションのシークレット ID を作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. アプリケーションの詳細が表示されます。シークレット作成後すぐに、**Value**の下に表示されるIDをメモしておいてください。他のGUIオプションに移動すると、この値は非表示になります。

値のID(/en-us/netscaler-console-service/media/sentinel-client-value-id.png)

Microsoft Entra IDデータコネクタを使用してMicrosoft Sentinelにデータを送信する

Microsoft Entra IDログは、Entraテナントにアクセスするユーザー、アプリケーション、およびネットワークに関する包括的な情報を提供します。詳細については、Microsoft Entra IDデータコネクタを使用してMicrosoft Sentinelにデータを送信するを参照してください。

データ収集エンドポイントを構成する

エンドポイントURLを取得するには、データ収集エンドポイントを作成する必要があります。これは、NetScaler Consoleでサブスクリプションを作成する際に必要です。

1. Azureポータルで、**Azureサービス**の下にある**データ収集エンドポイント**を選択するか、検索バーにキーワードを入力します。

   DCRの選択(/en-us/netscaler-console-service/media/sentinel-dcr-select.png)

2. **データ収集エンドポイント**ページで**作成**をクリックします。

   DCRの作成(/en-us/netscaler-console-service/media/sentinel-dcr-create.png)

3. **データ収集エンドポイントの作成**で:

   a. 任意のデータ収集エンドポイント名を指定します
   b. **サブスクリプション**、**リソースグループ**、および**リージョン**を選択します。
   c. **確認 + 作成**をクリックします。
   d. 検証成功のメッセージが表示されたら、**作成**をクリックします。

エンドポイントURLをメモする必要があります。**データ収集エンドポイント**のメインページで、作成したエンドポイントを選択し、**JSONビュー**をクリックして、エンドポイントIDをメモします。

DCR ID(/en-us/netscaler-console-service/media/sentinel-dcr-id.png)

データエクスポート用のテーブルを作成する

NetScaler ConsoleからMicrosoft Sentinelにエクスポートする各インサイトについて、テーブルを作成し、JSON情報を提供する必要があります。各インサイトのテーブル要件については、以下の詳細を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	必要なテーブルの総数
SSLインサイト	3
WAF	1
Bot	1
Gatewayインサイト	5

各ワークスペースにつき、最大10個のテーブルを作成できます。10個を超えるテーブルを作成する場合は、別のワークスペースを作成する必要があります。

1. Azureポータルでワークスペースに移動し、**設定**の下にある**テーブル**をクリックします。
2. **作成**をクリックし、**新しいカスタムログ (DCRベース)**を選択します。

3. **カスタムログの作成**で:
   a. テーブル名を指定します。テーブル名は**console_insightname**の形式である必要があります。例: **console_ns_sslvserver**、**console_ns_ssl_certkey**。各インサイトに適用されるテーブル名を取得するには、ステップ4を参照してください。
   b. テーブル名に関する詳細情報を追加するための説明を入力します。これはオプションです。
   c. 新しいデータ収集ルールを作成し、追加します。
   d. リストからデータ収集エンドポイントを選択します。

   e. **次へ**をクリックします。
4. **スキーマと変換**タブで、エクスポートするインサイトのJSONサンプルログをアップロードする必要があります。各インサイトについて以下のサンプルJSONを使用し、アップロードするJSONファイルを作成できます。

インサイト	JSON	使用するテーブル名
SSL (1)	`{"id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141",`	console_ns_sslvserver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	"name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite": "DISABLED", "skipclientcertpolicycheck": "", "tls13sessionticketsperauthcontext": 1,	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	"cipherredirect": "DISABLED", "dropreqwithnohostheader": "NO", "sessionticketlifetime": -1, "maxage": 0, "pushenctrigger": "Always", "strictsigdigestcheck": "f", "sslredirect": "DISABLED", "sessionkeylifetime": -1, "alpnprotocol": "", "clientauthuseboundcachain": "", "sesstimeout": 120, "clientcert": "", "snihttphostmatch": "CERT", "preload": "NO", "prevsessionkeylifetime": -1, "sessionticketkeydata": "", "encrypttriggerpktcount": 45, "cleartextport": "", "ssliocspcheck": "", "hsts": "f", "sslinterception": "", "commonname": "", "sslireneg": "", "ocspstapling": "DISABLED", "quantumsize": 8192, "insertionencoding": "Unicode", "sslimaxsessperserver": -1, "cipherurl": "", "pushflag": 0, "zerorttearlydata":	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	"DISABLED", "allowextendedmastersecret": "", "dhekeyexchangewithpsk": "NO", "clientauth": "DISABLED", "denysslreneg": "NONSECURE", "sendclosenotify": "YES", "dhcount": 0, "snienable": "DISABLED", "table_name": "ns_sslvserver"}	
SSL (2)	{"id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number":	console_ns_ssl_certkey

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	"7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "no_of_bound_entities": 0, "partition_name": "", "display_name": "10.106.186.141", "hostname": "athulsadc", "key_name": "", "subjaltname": "", "managed_by": "", "certificate_dn": "", "linkcertkeyname": "", "table_name": "ns_ssl_certkey"}	
SSL (3)	{"id": "2baffd1a-7ed6-4035-91e8-ad3a3125bff4", "certkeypair_name": "cert1", "ns_ip_address": "10.106.186.127", "poll_time":	console_ns_sslcertkey_binding

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	1715671567, "partition_name": "", "display_name": "10.106.186.127", "hostname": "", "entity_name": "secure_gateway", "entity_type": "sslvserver", "table_name": "ns_sslcertkey_binding" }	
WAF	[{"ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address":	console_af_threat_exporter_data_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "violation_threat_index": 5, "app_threat_index": 5, "http_method": 0, "violation_action": 3, "violation_action_desc": "Blocked", "severity_type": 2, "severity_type_desc": "Medium", "iprep_score": 0, "iprep_category": 0, "counter_value": 0, "appname": "vserver_1_10.106.185.156_lb", "violation_category": 12, "violation_category_desc": "Start URL", "source_ipv6_address": "", "true_client_ip": "\\N", "backend_vserver": "",	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	"backend_appname": "", "transactionId": "0", "table_name": "af_threat_exporter_data_l2"}]	
Bot	{"ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216",	console_af_bot_attack_details_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	`"table_name": "af_bot_attack_details_l2"}`	
ゲートウェイインサイト (1)	`{"adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}`	console_af_vpn_error_details
ゲートウェイ インサイト (2)	`{"adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}`	console_ns_vpnvserver
ゲートウェイ インサイト (3)	`{"adc_ip_address": "10.106.186.141",`	console_af_vpn_session_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	"gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1}	
ゲートウェイ インサイト (4)	{"active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}	console_af_vpn_active_session_1
ゲートウェイ インサイト (5)	{"adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports"}	console_af_vpn_error_reports
監査ログ	{"system_gmt_time":1721868291, "source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage",	console_syslog_messages

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイト	JSON	使用するテーブル名
	`"instance_ip":"X.X.X.X", "app_name":""}`	

JSONをアップロードした後、以下の詳細を表示できます。

Transformation editorをクリックし、適切なインサイトに適用される以下のクエリを入力し、**Run**をクリックしてNetScaler Consoleでのポーリング時間からデータを承認します。

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time) | project-rename sslvserver_id = id`
- **WAF** および **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **ゲートウェイインサイト** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

5. **Next**をクリックし、**Create**をクリックして完了します。
6. **Data collection rules**に移動し、作成したDCRをクリックします。
7. **Configuration**の下にある**Data sources**をクリックして、作成されたテーブルを表示します。

DCR (Data collection rule) には、**Monitoring Metrics Publisher**ロールへのアクセスが必要です。

a. AzureポータルのRecentsからアクセスできるDCRに移動します。
b. DCRページから**Access control (IAM)**をクリックし、**Add role assignment**をクリックします。

役割の割り当て(/en-us/netscaler-console-service/media/sentinel-dcr-role-assign.png)

c. 検索バーに「monitor」と入力して**Monitoring Metrics Publisher**を選択し、**Next**をクリックします。
d. **Members**タブで、**Select Members**をクリックし、作成したEntraアプリを選択します。
e. **Review + assign**をクリックします。

データ収集ルールIDをメモする必要があります。データ収集ルールページに移動し、DCRを選択してJSONビューをクリックし、IDをメモします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DCR ID(/en-us/netscaler-console-service/media/sentinel-dcr-value.png)

NetScaler Consoleでサブスクリプションを作成する

これで準備が整いました。最後のステップは、サブスクリプションを作成し、必要な詳細を追加してNetScaler Consoleを構成することです。NetScaler Consoleでサブスクリプションを作成するには、メモした以下の詳細が必要です。

- エンドポイントURL
- データ収集ルールID
- テナントID
- クライアントID
- クライアントシークレット

1. NetScaler Consoleにログインします。
2. **設定 > 可観測性統合**に移動します。
3. **統合**ページで、**追加**をクリックします。
4. **サブスクリプションの作成**ページで、次の詳細を指定します。
    a. サブスクリプション名フィールドに任意の名前を指定します。
    b. **ソース**として**NetScaler Console**を選択し、**次へ**をクリックします。
    c. **Microsoft Sentinel**を選択し、**構成**をクリックします。**エンドポイントの構成**ページで、すべての詳細を入力し、**送信**をクリックします。
    d. **次へ**をクリックします。
5. **インサイトの追加**をクリックし、**機能の選択**タブで、Microsoft Azureに追加したテーブルに応じて、エクスポートする機能を選択し、**選択を追加**をクリックして、**次へ**をクリックします。
6. **インスタンスの選択**タブで、**すべてのインスタンスを選択**または**カスタム選択**のいずれかを選択し、**次へ**をクリックします。
    - **すべてのインスタンスを選択** - すべてのNetScalerインスタンスからMicrosoft Sentinelにデータをエクスポートします。
    - **カスタム選択** - リストからNetScalerインスタンスを選択できます。リストから特定のインスタンスを選択した場合、データは選択されたNetScalerインスタンスからのみMicrosoft Sentinelにエクスポートされます。
7. **送信**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Azureでログを表示する

すべてを構成した後、Microsoft Azureで詳細を表示するには30分待つことをお勧めします。

1. Azureポータルで、**Log Analyticsワークスペース**に移動します。
2. 「**ログ**」をクリックし、テーブル名を入力し、「**実行**」をクリックして結果を表示します。

デフォルトスキーマを使用して、Prometheusへのインサイトのエクスポートのためにの構成する

NetScalerは、メトリクスをPrometheusに直接エクスポートすることをサポートしています。NetScalerインスタンスによって提供される豊富なメトリクスセットを使用して、NetScalerの健全性とアプリケーションの健全性を監視できます。たとえば、CPUとメモリ使用量に関するメトリクスを収集して、NetScalerの健全性を把握できます。同様に、1秒あたりのHTTPリクエスト数やアクティブクライアント数などのメトリクスを使用して、アプリケーションの健全性を監視できます。

メトリクスをPrometheusにエクスポートするには、タイプを時系列として分析プロファイルを構成する必要があります。詳細については、「Prometheusを使用したNetScaler、アプリケーション、およびアプリケーションセキュリティの監視」を参照してください。

NetScaler Consoleのオブザーバビリティ統合機能を使用すると、デフォルトスキーマを使用してPrometheusへのインサイトのエクスポートを構成できます。

1. **設定 > オブザーバビリティ統合**に移動します。
2. **統合**ページで、**追加**をクリックします。
3. **サブスクリプションの作成**ページで、次の詳細を指定します。
    a. **サブスクリプション名**フィールドに任意の名前を指定します。
    b. **ソース**として**NetScaler**を選択し、**次へ**をクリックします。
    c. 宛先として**Prometheus**を選択します。
    d. エクスポートするデフォルトのインサイトとして**デフォルト**を選択します。
    e. **インスタンスの追加**をクリックし、Prometheusにインサイトをエクスポートするインスタンスを選択します。
    f. **送信**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

失敗した構成のログを表示

サブスクリプションを作成した後、**設定 > オブザーバビリティ統合**で作成されたサブスクリプションのステータスを表示できます。ステータスが**失敗**と表示されている場合は、クリックして詳細を表示します。

- [ ] 「**構成ジョブの詳細**」の下にある「**詳細を表示**」をクリックします。
- [ ] 問題の詳細を表示するには、「**ログを表示**」をクリックします。
- [ ]

NetScaler® のメトリクスと監査ログの Splunk へのエクスポートを構成する

NetScaler は、メトリクスを JSON 形式で Splunk に直接エクスポートすることをサポートしています。NetScaler は、アプリケーションの健全性とアプリケーションセキュリティの健全性を監視するための豊富なメトリクスを提供します。NetScaler が提供するメトリクスを Splunk にエクスポートすることで、メトリクスを視覚化し、意味のあるインサイトを得ることができます。

監査ロギングを使用すると、NetScaler のさまざまなモジュールによって収集された NetScaler の状態とステータス情報をログに記録できます。ログを確認することで、問題やエラーをトラブルシューティングして修正できます。

詳細については、以下を参照してください。

- NetScaler から Splunk に監査ログを直接エクスポートする
- NetScaler から Splunk にメトリクスを直接エクスポートする

NetScaler Console を介してメトリクスと監査ログの Splunk へのエクスポートを構成するには：

1. **>** に移動します。
2. ページで、 をクリックします。
3. ページで、次の詳細を指定します。
    a. フィールドに任意の名前を指定します。
    b. として を選択し、 をクリックします。
    c. として を選択し、 をクリックします。 で：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- - 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。
- - Splunk から認証トークンをコピーして貼り付けます。
- 「**Submit**」をクリックします。

d. 「**Next**」をクリックします。

e. 「**Add Insights**」をクリックし、「**NetScaler Metrics**」と「**NetScaler Audit Logs**」を選択してから、「**Add Selected**」をクリックします。

f. 「**Next**」をクリックします。

g. 「**Add Instances**」をクリックし、インスタンスを選択します。

h. 「**Submit**」をクリックします。

失敗した構成のログを表示する

サブスクリプションを作成した後、「**Settings > Observability Integration**」で作成したサブスクリプションのステータスを表示できます。ステータスが「**Failed**」と表示されている場合は、クリックして詳細を表示します。

「**Config job details**」の下にある「**View details**」をクリックします。

問題の詳細を表示するには、「**View logs**」をクリックします。

アナリティクス設定の構成

NetScaler Consoleでアナリティクス機能の使用を開始してインスタンスおよびアプリケーションデータの可視性を得る前に、この機能で最適なエクスペリエンスを確保するために、いくつかのアナリティクス設定を構成することをお勧めします。

アナリティクス用のしきい値とアラートの作成

検出されたインスタンスで構成された管理対象仮想サーバーのアナリティクスのメトリックを監視するために、しきい値とアラートを設定できます。メトリックの値がしきい値を超えると、NetScaler Consoleはしきい値違反を示すイベントを生成します。

設定された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、GUIへのアラート表示、構成済みの電子メールの送信が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、ユーザーのICA RTT値が1秒を超えた場合に、HDX™ Insightのイベントを生成するしきい値を設定できます。また、生成されたイベントのアラートを有効にし、しきい値違反情報を構成済みの電子メールリストに送信することもできます。

アナリティクス用のしきい値とアラートを作成するには：

1. **設定** > **分析設定** > **しきい値** に移動します。
2. **Thresholds**画面で、**Add**をクリックして新しいしきい値を追加し、設定されたしきい値のアラートを構成します。
3. **Create Thresholds and Alerts**ページで、次の詳細を指定します。
   - **名前** – しきい値を構成するための名前。
   - **トラフィックタイプ** – しきい値を構成するアナリティクストラフィックのタイプ。例：HDX Insight、Security Insight。
   - **エンティティ** – しきい値を構成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** - しきい値を構成する間隔。
4. メール通知を設定するには、設定されたしきい値のチェックボックスを選択します。
5. **ルール**セクションで、以下を指定します。
   - **メトリック** – しきい値を設定するための、選択したトラフィックタイプのメトリック。
   - **比較演算子** – 選択したメトリックに対する比較演算子 (例: \<, \>=)。
   - **値** – しきい値を設定し、アラートを呼び出すためのメトリックの値。
6. **作成**をクリックします。

通知を構成する

以下の機能について通知を受け取るための通知タイプを選択できます。

- **イベント** – NetScalerインスタンス用に生成されるイベントのリスト。詳細については、「イベントルールアクションの追加」を参照してください。
- **ライセンス** – 現在アクティブなライセンス、期限切れ間近のライセンスなどのリスト。詳細については、「NetScaler Consoleライセンスの有効期限」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SSL証明書** – NetScalerインスタンスに追加されたSSL証明書のリスト。詳細については、「SSL証明書の有効期限」を参照してください。

NetScaler Consoleは、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、NetScaler Console GUIには構成済みの配布リストまたはプロファイルが表示されます。NetScaler Consoleは、選択された配布リストまたはプロファイルに通知を送信します。

メール配布リストを作成する

NetScaler Console機能のメール通知を受信するには、メールサーバーと配布リストを追加する必要があります。

メール配布リストを作成するには、以下の手順を実行します。

1. 「**Settings > Notifications**」に移動します。
2. 「**Email**」で、「**Add**」をクリックします。
3. 「**Create Email Distribution List**」で、次の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **宛先** - NetScaler Consoleがメッセージを送信するメールアドレスを指定します。
   - **Cc** - NetScaler Consoleがメッセージのコピーを送信するメールアドレスを指定します。
   - **Bcc** - NetScaler Consoleがアドレスを表示せずにメッセージのコピーを送信するメールアドレスを指定します。

   メールを追加(/en-us/netscaler-console-service/media/config-jobs-maintenance-6.png)
4. 「**Create**」をクリックします。

複数のメール配信リストを作成するには、この手順を繰り返します。「**Email**」タブには、NetScaler Consoleに存在するすべてのメール配信リストが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SMS配信リストを作成する

NetScaler Console機能のSMS通知を受信するには、SMSサーバーと電話番号を追加する必要があります。

SMS通知設定を構成するには、次の手順を実行します。

1. 「**Settings > Notifications**」に移動します。
2. 「**SMS**」で、「**Add**」をクリックします。
3. 「**SMS配信リストの作成**」で、以下の詳細を指定します。
   - **名前** - 配信リスト名を指定します。
   - **SMSサーバー** - SMS通知を送信するSMSサーバーを選択します。
   - **宛先** - NetScaler Consoleがメッセージを送信する電話番号を指定します。
4. **作成**をクリックします。

複数のSMS配信リストを作成するには、この手順を繰り返します。**SMS**タブには、NetScaler Consoleに存在するすべてのSMS配信リストが表示されます。

Slackプロファイルの作成

NetScaler Console機能のSlack通知を受信するには、Slackプロファイルを作成する必要があります。

Slackプロファイルを作成するには、次の手順を実行します。

1. **設定 > 通知**に移動します。
2. **Slack**で、**追加**をクリックします。
3. 「**Slackプロファイルの作成**」で、以下の詳細を指定します。
   - **プロファイル名** - プロファイル名を指定します。この名前はSlackプロファイルリストに表示されます。
   - **チャネル名** - NetScaler Consoleが通知を送信するSlackチャネル名を指定します。
   - **Webhook URL** - チャネルのWebhook URLを指定します。受信Webhookは、外部ソースからSlackにメッセージを投稿する簡単な方法です。URLはチャネル名に内部的にリンクされています。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>`

Slackチャネルを追加(/en-us/netscaler-console-service/media/upgrade-slack.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**作成**」をクリックします。

複数のSlackプロファイルを作成するには、この手順を繰り返します。**Slack**タブには、NetScaler Consoleに存在するすべてのSlackプロファイルが表示されます。

PagerDutyプロファイルの作成

PagerDutyの設定に基づいてインシデント通知を監視するために、PagerDutyプロファイルを追加できます。PagerDutyを使用すると、登録された番号に電子メール、SMS、プッシュ通知、電話で通知を設定できます。

NetScaler ConsoleでPagerDutyプロファイルを追加する前に、PagerDutyで必要な設定を完了していることを確認してください。PagerDutyの使用を開始するには、PagerDutyドキュメントを参照してください。

PagerDutyプロファイルを作成するには、次の手順を実行します。

1. **設定 > 通知**に移動します。
2. **PagerDuty**で、**追加**をクリックします。
3. **PagerDutyプロファイルの作成**で、次の詳細を指定します。
   - **プロファイル名** - 任意のプロファイル名を指定します。
   - **統合キー** - 統合キーを指定します。このキーはPagerDutyポータルから取得できます。
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、NetScaler Consoleに存在するすべてのPagerDutyプロファイルが表示されます。

ServiceNow プロファイルを確認する

NetScaler イベントおよび NetScaler Console イベントの ServiceNow 通知を有効にする場合は、ITSM コネクタを使用して NetScaler Console を ServiceNow と統合する必要があります。詳細については、「NetScaler Console と ServiceNow インスタンスを統合する」(/ja-jp/netscaler-console-service/setting-up/integrate-itsm-adapter-citrix-adm-servicenow.html)を参照してください。

ServiceNow プロファイルを表示および確認するには、次の手順を実行します。

1. **設定 > 通知**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Console GUI で ServiceNow チケットを表示する場合は、**ServiceNow チケット**を選択します。

レポートのエクスポートまたはエクスポートレポートのスケジュール設定

NetScaler Consoleでは、選択したNetScaler Console機能の包括的なレポートをエクスポートできます。このレポートは、インスタンス、パーティション、および対応する詳細間のマッピングの概要を提供します。

NetScaler Consoleは、個々のNetScaler Console機能の下に機能固有のスケジュールされたエクスポートレポートを表示します。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、**Infrastructure > Instances > NetScaler**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。

レポートのエクスポートでは、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

レポートをエクスポートする

NetScaler Consoleからローカルコンピューターにレポートをエクスポートするには、次の手順を実行します。

1. ページの右上隅にあるエクスポートアイコンをクリックします。
2. **今すぐエクスポート**を選択します。
3. 次のエクスポートオプションのいずれかを選択します。

   - **スナップショット** - このオプションは、NetScaler Consoleレポートをスナップショットとしてエクスポートします。
   - **表形式** - このオプションは、NetScaler Consoleレポートを表形式でエクスポートします。また、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleレポートのエクスポート(/en-us/netscaler-console-service/media/export-snapshot.png)

4. レポートをローカルコンピューターに保存するファイル形式を選択します。
5. **エクスポート**をクリックします。

エクスポートレポート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 Consoleは、エクスポートされたレポートを設定済みのメールまたはSlackプロファイルに送信します。

1. ページ右上のエクスポートアイコンをクリックします。
2. **エクスポートのスケジュール**を選択し、以下を指定します。

   - **件名** - デフォルトでは、このフィールドには選択した機能名が自動入力されます。ただし、意味のあるタイトルに書き換えることができます。
   - **エクスポートオプション** - NetScaler Consoleレポートをスナップショット形式または表形式でエクスポートします。表形式でエクスポートするデータレコードの数を選択することもできます。
   - **形式** - 設定済みのメールまたはSlackプロファイルでレポートを受信するファイル形式を選択します。
   - **繰り返し** - リストから**毎日**、**毎週**、または**毎月**を選択します。
   - **説明** - レポートに意味のある説明を指定します。
   - **エクスポート時刻** - レポートをエクスポートする時刻を指定します。
   - **メール** - チェックボックスを選択し、リストボックスからプロファイルを選択します。プロファイルを追加する場合は、**追加**をクリックします。
   - **Slack** - チェックボックスを選択し、リストボックスからプロファイルを選択します。プロファイルを追加する場合は、**追加**をクリックします。

3. **スケジュール**をクリックします。

NetScaler Consoleレポートのエクスポートをスケジュール(/en-us/netscaler-console-service/media/schedule-export-adm-reports.png)

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ページの右上隅にあるエクスポートアイコンをクリックします。

   エクスポートレポートページには、すべての機能固有のエクスポートレポートが表示されます。

2. 編集するレポートを選択し、**編集**をクリックします。

グローバル設定

NetScaler Consoleの**グローバル設定**では、管理対象のNetScalerインスタンス全体に適用されるシステム全体にわたるオプションを構成できます。これらの設定を使用して、インスタンス設定、システム構成、メール購読を管理したり、NetScaler Consoleの機能を有効または無効にしたりできます。

次のグローバル設定を構成できます。

- インスタンス設定
- システム構成
- メール購読
- NetScaler Consoleの機能を有効または無効にする

インスタンス設定

NetScaler Consoleで検出されたインスタンスを管理し、インスタンスのバックアップ設定を構成できます。

インスタンス構成の管理

設定 > グローバル設定 > インスタンス設定 > インスタンス管理で、次のインスタンス構成を変更できます。

- **インスタンスとの通信** - NetScaler Consoleと検出されたインスタンスの間で、HTTPまたはHTTPS通信チャネルを選択できます。
- **証明書のダウンロードを有効にする** - 検出されたインスタンスからSSL証明書をダウンロードできます。
- **インスタンスログインの資格情報を要求する** - NetScaler Console GUIを介してインスタンスにアクセスすると、インスタンスログインページが表示されます。インスタンスにアクセスするには、ログイン資格情報を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インスタンスバックアップ設定の構成

設定 > グローバル設定 > インスタンス設定 > インスタンスバックアップで、NetScaler Consoleで検出されたNetScalerインスタンスのバックアップ設定を構成できます。

インスタンスバックアップ設定の構成で、**インスタンスバックアップを有効にする**を選択します。

- **保持するバックアップファイルの数**: NetScaler Consoleで保持するバックアップファイルの数を指定します。NetScalerインスタンスごとに最大3つのバックアップファイルを保持できます。デフォルトは1つのバックアップファイルです。
- **バックアップスケジューリング設定** - インスタンスバックアップは2つの方法でスケジュールできます。
  - **間隔ベース** - 指定された間隔が経過すると、NetScaler Consoleにバックアップファイルが作成されます。デフォルトのバックアップ間隔は12時間です。
  - **時間ベース** - NetScaler Consoleがインスタンスバックアップを実行する時間を `hours:minutes` 形式で指定します。
- **NetScaler設定** - このオプションを使用すると、トラップに基づいてバックアップを開始し、GeoDBファイルをバックアップに含めることができます。この設定は、MPX、VPX、CPX、およびBLXインスタンスに適用されます。
  - **NetScalerConfigSaveトラップ受信時にインスタンスバックアップを実行** - デフォルトでは、NetScaler Consoleは「NetScalerConfigSave」トラップを受信してもバックアップファイルを作成しません。ただし、NetScalerインスタンスがNetScaler Consoleに `NetScalerConfigSave` トラップを送信するたびにバックアップファイルを作成するオプションを有効にできます。

    NetScalerインスタンスは、インスタンスの構成が保存されるたびに `NetScalerConfigSave` を送信します。

    トラップ遅延時のバックアップを分単位で指定します。受信した `NetScalerConfigSave` トラップがNetScaler Consoleで指定された分数間継続する場合、NetScaler Consoleはインスタンスをバックアップします。
  - **GeoDBファイルを含める** - デフォルトでは、NetScaler ConsoleはGeoDatabase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も作成するオプションを有効にできます。
- **NetScaler SDX設定** - SDXインスタンスをバックアップするには、**バックアップタイムアウト**を分単位で指定します。SDXインスタンスのバックアップ中、NetScaler ConsoleとSDX間の接続は指定された期間維持されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

大規模なSDXバックアップファイルの場合、バックアップが完了するように、NetScaler ConsoleとSDXインスタンス間の接続をより長い期間維持してください。

重要:

接続がタイムアウトすると、バックアップは失敗します。

- **外部転送** - NetScaler Consoleでは、NetScalerインスタンスのバックアップファイルを外部の場所に転送できます。

  a. 場所のIPアドレスを指定します。
  b. バックアップファイルを転送する外部サーバーのユーザー名とパスワードを指定します。
  c. 転送プロトコルとポート番号を指定します。
  d. ファイルを保存するディレクトリパスを指定します。
  e. ファイルを外部サーバーに転送した後でバックアップファイルを削除する場合は、**転送後にApplication Delivery Managementからファイルを削除**を選択します。

管理対象デバイスの通知を無効にする

管理者は、メンテナンスおよびトラブルシューティング期間中に、特定の管理対象デバイスの通知を一時的に無効にできます。通知を無効にすることで、これらの期間中にデバイス固有の問題やステータス更新に関する不要なアラートや通知を受け取らないようにすることができます。

管理者は、プライマリ、セカンダリ、または特定のクラスターノードを含む個々のデバイスを選択できます。VPXインスタンスがSDX上にある場合、VPXとSDXは通知設定のために別々のエンティティとして扱われます。デバイスに対して通知無効化ウィンドウが設定されている場合、その設定はデバイスパーティションにも適用されます。

これらの期間中、イベントは処理されますが、選択されたデバイスに関する通知（メール、Slack、PagerDuty）は管理者に送信されません。この動作は、デバイス固有のイベント（構成変更、エンティティダウンアラートなど）と、コンソール生成イベント（ステータス調査、しきい値違反など）の両方に適用されます。

特定の管理対象デバイスの通知を無効にするには、次の手順を実行します。

1. **Settings > Administration > Instance Settings** に移動し、**Notification Disable Windows** をクリックします。
2. **Notification Disable Windows** で、**Add** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **Add Notification Disable Windows** で、**Add Instances** をクリックし、必要なインスタンスを選択します。**Ok** をクリックします。
4. **Start Date**、**Start Time**、**End Date**、および **End Time** の日付と時刻を選択します。
5. コメント（オプション）を追加し、**Create** をクリックします。通知無効化ウィンドウが **Notification Disable Windows** ページに表示されます。

これらの通知無効化ウィンドウを編集または削除することもできます。また、**History** をクリックして、通知無効化ウィンドウの履歴の詳細を表示することもできます。

システム構成

NetScaler Consoleエージェントのキープアライブ間隔とNetScaler Consoleサーバーのタイムゾーンを変更できます。

エージェントのキープアライブ間隔を設定する

NetScaler Consoleサーバーとエージェントは、指定されたキープアライブ間隔で同じTCP接続を維持します。エージェントは、この接続を使用して管理対象インスタンスのデータをNetScaler Consoleサーバーに送信します。

1. **Settings > Global Settings** に移動します。
2. **System Configurations** の下にある **Agent and Timezone** を選択します。
3. **Agent** 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。

NetScaler Consoleのタイムゾーンを設定する

NetScaler ConsoleのWebページ、通知、レポートに時間を表示するタイムゾーンを選択できます。

1. **Settings > Global Settings** に移動します。
2. **System Configurations** の下にある **Agent and Timezone** を選択します。
3. **Time zone** で、NetScaler Consoleに時間を表示するためにローカルまたはGMTタイムゾーンを選択します。
4. **Save** をクリックします。

メール購読

NetScaler Console は、すべてのアクティブでないユーザーと新規ユーザーにメール通知を送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクティブでない顧客は、次の場合にメール通知を受け取ります。

- NetScaler インスタンスが構成されていない
- テナントライセンスの有効期限が30日未満である

注:

デフォルトでは、そのようなすべてのアクティブでない顧客はメール通知を受け取ります。

新規顧客は、NetScaler Console からメールを受け取ります。このメールでは、NetScaler インスタンスを NetScaler Console サービスにオンボードするよう招待されており、そこで NetScaler インスタンスの重要なイベントを管理および監視したり、トラブルシューティングを行ったり、NetScaler の構成などのタスクを自動化したりできます。

購読メール(/en-us/netscaler-console-service/media/subscription-email.png)

メール通知の購読解除

NetScaler Console サービスから受信するメール通知を購読または購読解除できます。**メール通知の購読を解除**するには:

1. NetScaler Console で、**設定 > グローバル設定 > システム構成**に移動し、**メール購読**をクリックします。**メール通知の購読解除**ウィンドウが表示されます。

   メール通知の購読解除(/en-us/netscaler-console-service/media/unsubscribe-email-notifications.png)

   注:

   デフォルトでは、メール通知をオフにするトグルボタンはオフの位置にあり、すべての非アクティブユーザーに対してメール通知が有効になっています。

2. 「**メール通知の登録解除**」ウィンドウで、トグルボタンをオンにします。「**OK**」をクリックします。

メール通知の登録を解除しました。これで、オンボードのNetScalerインスタンスへのメールは届かなくなります。

機能の有効化または無効化

管理者は、 **> >** ページで次の機能を有効または無効にできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **エージェントフェイルオーバー** - エージェントフェイルオーバーは、2つ以上のアクティブなエージェントを持つサイトで発生する可能性があります。サイトでエージェントが非アクティブ（DOWN状態）になると、NetScaler Consoleは非アクティブなエージェントのNetScalerインスタンスを他のアクティブなエージェントに再配布します。詳細については、「マルチサイト展開用のNetScalerエージェントの構成」を参照してください。
- **エンティティポーリングネットワーク機能** - エンティティとは、NetScalerインスタンスにアタッチされたポリシー、仮想サーバー、サービス、またはアクションのいずれかです。デフォルトでは、NetScaler Consoleは構成されたネットワーク機能エンティティを60分ごとに自動的にポーリングします。詳細については、「ポーリングの概要」を参照してください。
- **インスタンスバックアップ** - NetScalerインスタンスの現在の状態をバックアップし、後でバックアップファイルを使用してNetScalerインスタンスを同じ状態に復元します。詳細については、「NetScalerインスタンスのバックアップと復元」を参照してください。
- **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 Consoleで受信したイベントは、 ページ（ **>** ）に表示されます。すべてのアクティブなイベントは、 ページ（ **> >** ）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 Console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** - デバイスを構成してすべてのsyslogメッセージをNetScaler Consoleにリダイレクトしている場合、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。詳細については、「インスタンスでのsyslogの構成」を参照してください。

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. をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。

アプリケーションイベント通知を受信するためのアクションポリシーを構成する

アプリケーションイベントの既存のアナリティクスビューとは別に、Slack、Email、PagerDuty、またはServiceNowを介してアプリケーションイベント通知を取得するようにアクションポリシーを構成できます。アプリケーションイベントには、パフォーマンスの問題、ボットおよびWAF違反、サービスグラフ違反が含まれます。管理者として、アクションポリシーを使用すると、リアルタイムでイベント通知を受け取ることができます。

アクションポリシーを使用すると、次のことができます。

- アプリケーションイベントの特定の条件を事前定義する。
- Slack、Email、PagerDuty、およびServiceNowを介して、以下のイベントの通知を受け取る：

イベントカテゴリ	イベントサブカテゴリ	イベント
セキュリティ違反	すべてのセキュリティ違反	すべてのボット違反（ボット違反のリストの詳細については、違反カテゴリを参照してください）。
		すべてのWAF違反（WAF SQL違反、WAF XSS違反、WAF Infer XML違反）
	クライアントごとのすべてのセキュリティ違反	クライアントごとのボット違反
		クライアントごとのWAF違反
		注: WAF違反通知を受信するには、最小違反トランザクションが20%である必要があります。たとえば、100トランザクションのうち、最低20は違反トランザク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イベントカテゴリ	イベントサブカテゴリ	イベント
		ションである必要があります。
アプリケーションパフォーマンス		アプリスコア違反
		クライアントネットワーク遅延
		サーバーネットワーク遅延
		サーバー処理時間
		応答時間
		リクエスト
		帯域幅
		サービスグラフ違反
アプリケーション使用状況		1秒あたりのリクエスト数
		スループット
		データ量

アクションポリシーを構成する

1. 「**Settings > Action > Action Policies**」に移動します。
2. 「**Add**」をクリックします。
3. 「**Create Action Policy**」ページで、次の操作を行います。
   a. **ポリシー名** – 任意のポリシー名を入力します。
   b. **有効** – このオプションはデフォルトで選択されています。
   c. **次のイベントが発生した場合** – リストからイベントを選択します。
   d. **次の条件が満たされた場合** – リストから、通知を受けたい条件を定義するために選択します。**+** をクリックして条件を追加できます。条件を削除するには、**–** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の演算子を使用してアクションポリシーを設定できます。演算子は、選択した条件に基づいて表示されます。

演算子	説明
等しい	定義された値と等しい
等しくない	定義された値と等しくない
より大きい	定義された値より大きい
以上	定義された値以上
未満	定義された値より小さい
以下	定義された値以下
含む	定義された用語または値を含む
で始まる	定義された用語または値で始まる
で終わる	定義された用語または値で終わる
IN	複数の値を選択できます

e. **次に以下を実行** – 「**通知**」を選択します。「**通知**」を選択すると、「通知タイプ」オプションが表示されます。

f. **通知タイプ** – 通知タイプとして、Email、Slack、PagerDuty、またはServiceNowを選択します。選択した通知タイプに応じて、対応するオプション（配布リスト、Slackプロファイル、PagerDutyプロファイル、またはServiceNowプロファイル）が表示されます。リストからプロファイルを選択します。

新しいプロファイルを作成する場合は、「**追加**」をクリックします。

g. 「**ポリシーの作成**」をクリックします。

ポリシーが設定されました。設定されたポリシーの詳細を表示できます。

ポリシーを設定した後、ポリシーを選択して、以下をクリックできます。

- **編集** – アクションポリシーを更新または変更します。更新後、「ポリシーの更新」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **削除** – アクションポリシーを削除します。複数のポリシーを選択し、「**削除**」をクリックして削除できます。
- **アクション履歴** – 時間、実行されたアクション、ポリシー名、アラートタイプ、アラートメッセージなどの詳細を表示します。

次の表に、アクションポリシー設定の詳細を示します。

違反名	条件	説明
すべてのセキュリティ違反	インスタンスIP	NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。
	違反数	通知を受け取りたい違反数。たとえば、違反数を10以下に設定した場合、ボット違反トランザクションが10以下で受信されると通知されます。
	違反率	この値は、特定のトランザクションからの合計違反数を示し、値は0から1の間である必要があります。たとえば、100件のトランザクションのうち20件が違反であり、そのようなシナリオで通知を受け取りたい場合は、0.2を入力する必要があります。
すべてのボット違反	ボットプロファイル	NetScalerインスタンスでボット管理を設定するために使用されるボットプロファイル名。
	インスタンスIP	NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。
	違反数	通知を受け取りたい違反数。たとえば、違反数を10以下に設定した場合、ボット違反ト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
		ランザクションが10以下で受信されると通知されます。
	違反率	この値は、特定のトランザクションからの合計違反数を示し、値は0から1の間である必要があります。たとえば、100件のトランザクションのうち20件が違反であり、そのようなシナリオで通知を受け取りたい場合は、0.2を入力する必要があります。
すべてのWAF違反、WAF SQL違反、WAF XSS違反、WAF XML推論違反	WAFプロファイル	NetScalerインスタンスでWAFセキュリティ設定を構成するために使用されるWAFプロファイル名。
	インスタンスIP	NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。
	違反数	通知を受け取りたい違反数。WAF違反が通知されるための最小要件は20%です。
	違反率	この値は、特定のトランザクションからの合計違反数を示し、値は0から1の間である必要があります。たとえば、100件のトランザクションのうち20件がWAF SQL違反トランザクションであり、そのようなシナリオで通知を受け取りたい場合は、0.2と入力する必要があります。
クライアントごとのすべてのセキュリティ違反	アプリケーション名	カスタムアプリケーション名。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのす

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
		べてのアプリケーションが考慮されます。
	インスタンスIP	NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。
	クライアントIP	Botの発生元。IPアドレスを指定します。
	総攻撃数	通知を受け取りたい総攻撃数。
	リクエストURL	ブロックするように構成したいURL。URLを指定します。
	仮想サーバー名	カスタムアプリケーション用に構成された関連アプリケーション。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。
クライアントごとのBot違反	アプリケーション名	カスタムアプリケーション名。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。
	インスタンスIP	NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。
	クライアントIP	Botの発生元。IPアドレスを指定します。
	総攻撃数	通知を受け取りたい攻撃の合計数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
	違反タイプ	リストからボット違反を選択します。
	リクエストURL	ブロックするように設定したいURL。URLを指定します。
	仮想サーバー名	カスタムアプリケーション用に設定された関連アプリケーション。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。
クライアントごとのWAF違反	アプリケーション名	カスタムアプリケーション名。リストからアプリケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。
	インスタンスIP	NetScalerインスタンスのIPアドレス。リストからIPアドレスを選択します。
	クライアントIP	ボットの発生元。IPアドレスを指定します。
	総攻撃数	通知を受け取りたい攻撃の総数。
	違反タイプ	リストからWAF違反を選択します。
	リクエストURL	ブロックするように構成したいURL。URLを指定します。
	仮想サーバー名	カスタムアプリケーション用に構成された関連アプリケーション。リストからアプリ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
		ケーションを選択します。この条件を追加しない場合、NetScalerインスタンスのすべてのアプリケーションが考慮されます。
アプリスコア違反	パフォーマンスインジケーター	アプリスコアコンポーネントとそのしきい値。リストからアプリスコアコンポーネントを選択します。詳細については、「アプリスコアコンポーネントを選択してしきい値を設定する」を参照してください。
	違反回数	通知を受け取りたい違反回数。たとえば、応答時間の違反回数を5に設定した場合、応答時間のしきい値が5回違反したときに通知が届きます。
	アプリケーション名	**アプリケーションの選択**をクリックして、違反通知を受け取りたいアプリケーションを選択します。
クライアントネットワーク遅延	クライアントネットワーク平均遅延	通知を受けたいクライアント遅延（クライアントからNetScalerまで）の値をミリ秒単位で指定します。
	クライアントネットワーク遅延の異常	通知を受けたいネットワーク遅延の異常数を指定します。
	アプリケーション名	違反の通知を受けたいアプリケーションを選択するには、**[アプリケーションの選択]** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
サーバーネットワーク遅延	サーバーネットワーク平均遅延	通知を受けたいサーバー遅延（サーバーからNetScalerまで）の値をミリ秒単位で指定します。
	サーバーネットワーク遅延の異常	通知を受けたいネットワーク遅延の異常数を指定します。
	アプリケーション名	違反の通知を受けたいアプリケーションを選択するには、**[アプリケーションの選択]** をクリックします。
応答時間	応答平均時間	通知を受け取りたい値（ミリ秒単位）を指定します。
	応答平均時間の異常	通知を受け取りたい異常の数を指定します。
	アプリケーション名	通知を受け取りたいアプリケーションを選択するには、**Select Applications** をクリックします。アプリケーションを選択しない場合、すべてのアプリケーションに適用されます。
リクエスト	合計リクエスト数	通知を受け取りたい合計リクエスト数を指定します。
	アプリケーション名	通知を受け取りたいアプリケーションを選択するには、**Select Applications** をクリックします。アプリケーションを選択しない場合、すべてのアプリケーションに適用されます。
帯域幅	合計帯域幅	通知を受け取りたい帯域幅（MB）を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
	アプリケーション名	通知を受け取りたいアプリケーションを選択するには、**Select Applications** をクリックします。アプリケーションを選択しない場合、すべてのアプリケーションに適用されます。
サーバー処理時間	サーバー処理平均時間	通知を受け取りたいサーバー処理（サーバーからNetScalerへ）の値をミリ秒単位で指定します。
	サーバー処理時間の異常	通知を受け取りたいサーバー処理時間の異常数を指定します。
	アプリケーション名	**アプリケーションの選択**をクリックして、違反の通知を受け取りたいアプリケーションを選択します。
サービスグラフ違反		設定されたしきい値を超えるマイクロサービス。詳細については、「サービスグラフでしきい値を設定する」を参照してください。
1秒あたりのリクエスト数	1秒あたりのリクエスト数平均	アプリケーションが1秒あたりに受信するリクエスト数。通知を受け取る平均値を指定します。
	1秒あたりのリクエスト数平均の異常	通知を受け取りたい平均異常数を指定します。
		注: このイベントにAND条件を使用している場合、1秒あたりのリクエスト数平均とアプリケーション名、または1秒あたりのリクエスト数異常

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
		平均とアプリケーション名のいずれかを設定できます。
	アプリケーション名	違反通知を受け取りたいアプリケーションを選択するには、「**アプリケーションの選択**」をクリックします。
スループット	スループット平均	特定の期間に送信されたデータの合計。通知を受け取る平均値（MB単位）を指定します。
	スループット平均異常	通知を受け取りたい平均異常数を指定します。
		注: このイベントにAND条件を使用している場合、スループット平均とアプリケーション名、またはスループット平均異常とアプリケーション名のいずれかを構成できます。
	アプリケーション名	違反通知を受け取りたいアプリケーションを選択するには、「**アプリケーションの選択**」をクリックします。
データ量	総データ量	特定の期間に転送されるデータの合計。通知を受け取る値（MB単位）を指定します。
	データ量異常	通知を受け取りたい異常数を指定します。
		注: このイベントにAND条件を使用している場合、合計データ量とアプリケーション名、またはデータ量異常とアプリケーション名のいずれかを構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

違反名	条件	説明
	アプリケーション名	**「アプリケーションの選択」**をクリックして、違反通知を受け取りたいアプリケーションを選択します。

検索バーを使用する

検索バーを使用すると、結果をフィルタリングできます。検索バーをクリックすると、検索候補のリストが表示されます。コンポーネントを選択し、要件に基づいて結果をフィルタリングできます。

アクションポリシー検索バー(/en-us/netscaler-console-service/media/awp-search.png)

監査ログオプションを使用する

「監査ログ」をクリックし、リストから期間を選択して、選択した期間に作成、変更、削除されたアクションポリシーを表示し、**「検索」**をクリックします。

注

データストレージポリシーは、今後のリリースで変更される予定です。これらの変更により、ストレージ制限を超過した履歴データを保存することはできません。現時点では、ストレージを追加するか、ライセンスエンタイトルメントの制限内でストレージを維持することをお勧めします。

監査ログを使用してインフラストラクチャを管理および監視する

NetScaler Console を使用して、NetScaler Console 上のすべてのイベントと、NetScaler インスタンスで生成された syslog イベントを追跡できます。これらのメッセージは、インフラストラクチャの管理と監視に役立ちます。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ます。NetScaler Console 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、NetScaler Console の syslog および監査ログメッセージを検索できます。フィルタは、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方法をガイドします。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レポートのエクスポートを、指定されたメールアドレスにさまざまな間隔でスケジュールできます。

NetScaler Console GUI から、次の種類のログメッセージを確認できます。

- NetScaler インスタンス関連の監査ログ
- NetScaler Console 関連の監査ログ
- アプリケーション監査ログ

NetScaler インスタンス関連の監査ログ

NetScaler Console から NetScaler インスタンス関連の syslog メッセージを表示する前に、NetScaler Console を NetScaler インスタンスの syslog サーバーとして構成します。構成が完了すると、すべての syslog メッセージはインスタンスから NetScaler Console にリダイレクトされます。

NetScaler Console を syslog サーバーとして構成する

NetScaler Console を syslog サーバーとして構成するには、次の手順に従います。

1. NetScaler Console GUI から、**Infrastructure > Instances** に移動します。
2. syslog メッセージを収集して NetScaler Console に表示する NetScaler インスタンスを選択します。
3. **Select Action** リストで、**Configure Syslog** を選択します。
4. **Enable** をクリックします。
5. 「**Facility**」ドロップダウンリストで、ローカルまたはユーザーレベルのファシリティを選択します。
6. syslog メッセージに必要なログレベルを選択します。
7. 「**OK**」をクリックします。

NetScaler Console での Syslog の構成 (/en-us/netscaler-console-service/media/configure-syslog-adm.png)

これらの手順により、NetScaler インスタンス内のすべての syslog コマンドが構成され、NetScaler Console は syslog メッセージの受信を開始します。メッセージを表示するには、**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console の Syslog メッセージ (/en-us/netscaler-console-service/media/adm-syslog-messages.png)

ログメッセージをエクスポートするには、右上隅の矢印アイコンをクリックします。

次に、「**Export Now**」または「**Schedule Export**」をクリックします。詳細については、「Syslog メッセージのエクスポート」を参照してください。

NetScaler Console 関連の監査ログ

事前設定されたルールに基づいて、NetScaler Console は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。NetScaler Console に存在するすべての監査ログメッセージを表示するには、**Settings->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、右上隅の矢印アイコンをクリックします。

アプリケーション関連の監査ログ

すべての NetScaler Console アプリケーション、または特定のアプリケーションの監査ログメッセージを表示できます。

- NetScaler Console に存在するすべてのアプリケーションのすべての監査ログメッセージを表示するには、**Infrastructure > Network Functions > Auditing** に移動します。
- NetScaler Console 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 > 仮想サーバーをダブルクリック > Audit Log** に移動します。

注

> NetScaler Consoleの監査ログメッセージを外部サーバーに転送できます。詳細については、監査情報の表示を参照してください。

IPアドレス管理 (IPAM) の設定

NetScaler Console IPAMを使用すると、NetScaler Consoleで管理される構成でIPアドレスを自動割り当ておよび解放できます。IPは、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範囲から割り当てることができます。

- NetScaler Consoleの組み込みIPAMプロバイダー。
- Infoblox IPAMソリューション。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console IPAMは、次の用途で使用できます。

- **StyleBooks**: 構成を作成するときに、仮想サーバーにIPを自動割り当てします。
- **APIゲートウェイ**: APIプロキシにIPアドレスを自動割り当てします。

NetScaler Consoleによって管理されている各ネットワークまたはIP範囲のIPアドレスを追跡することもできます。

外部IPAMプロバイダーを追加する際に次のエラーが発生した場合、NetScaler Consoleが外部IPAMプロバイダーのSSL証明書を検証できないことを示しています。これは、不足しているか認識されない認証局 (CA) 証明書が原因で発生します。

```
certificate verify failed: unable to get local issuer certificate
```

この問題を解決するには、外部IPAMプロバイダーへのアクセスに使用されるNetScaler Consoleエージェントに、必要なCA証明書を手動で追加できます。必要なCA証明書を追加することで、外部IPAMプロバイダーへのセキュアな接続が適切に検証されるようになります。

外部IPAMプロバイダーへのアクセスに使用されるNetScaler Consoleエージェントにログインし、CA証明書を信頼された証明書バンドル`/var/mps/ca_certs/cacert.pem`に追加します。

外部IPアドレスプロバイダーを追加する

NetScaler Consoleには、IPとIP範囲を管理するための組み込みIPAMプロバイダーがあります。NetScaler Consoleに外部IPアドレスプロバイダーを使用することもできます。

重要:

始める前に、外部IPアドレスプロバイダーで以下の権限が有効になっていることを確認してください。

- プロバイダーに存在するネットワークをクエリする機能。
- ネットワーク内のIPアドレスを予約する。
- ネットワークからIPアドレスを解放する。
- ネットワークから使用済みIPアドレスを取得する。
- ネットワークから利用可能なIPアドレスを取得する。

NetScaler Consoleに外部IPAMプロバイダーソリューションを追加するには、以下の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **設定 > 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. IPAMプロバイダーを追加するために、以下の詳細を指定します。

   - **名前** - NetScaler Consoleで使用するIPプロバイダー名を指定します。
   - **ベンダー** - リストからIPAMベンダーを選択します。
   - **URL** - NetScaler Console環境でIPアドレスを割り当てるIPAMソリューションのURLを指定します。URLは以下の形式で指定してください。

     ```
     https://<host name>
     ```

     例: `https://myinfoblox.example.com`
   - **プライベートエンドポイントですか？** - Infoblox DDIがプライベートホストされている場合、このチェックボックスを選択し、**エージェント** を選択します。
   - **ユーザー名** - IPAMソリューションにログインするためのユーザー名を指定します。
   - **パスワード** - IPAMソリューションにログインするためのパスワードを指定します。

4. **追加**をクリックします。

外部プロバイダーとしてのInfoblox DDI

現在、NetScaler ConsoleはInfoblox DDIを外部プロバイダーとしてサポートしています。Infoblox DDIは、公開アクセス可能であるか、または企業の内部ネットワーク内でのみアクセス可能なプライベートホストであるかのいずれかです。プライベートホストされたInfoblox DDIの場合、設定プロセス中にNetScalerエージェントを選択する必要があります。NetScalerエージェントは、企業のイントラネット内にあるプロバイダーにアクセスするためのプロキシとして機能します。

InfobloxプロバイダーとNetScaler Console IPAMを使用して、次のアクションを実行できます。

- IPAMネットワークを一覧表示する
- IPAMネットワークを作成、更新、および削除する
- IPAMネットワークからIPアドレスを予約および解放する

IPAMネットワークを作成する

Infobloxプロバイダーを使用してNetScaler Console IPAMネットワークを作成するには、Infoblox上に同じCIDR IP範囲を持つネットワークが存在している必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console内でIPAMネットワークを作成する場合、NetScaler Console内でInfobloxネットワークの使用を登録しているだけです。その後、NetScaler ConsoleはInfobloxと連携して、ネットワークから割り当てられたIPアドレスを管理します。Infobloxネットワークは、NetScaler Consoleの外部で引き続き使用できます。

同様に、NetScaler Console IPAMネットワークを削除すると、NetScaler ConsoleはInfobloxネットワークの登録を解除します。これは、NetScaler Consoleがそのネットワークでの IPアドレス管理のためにInfobloxと連携しなくなることを意味します。

インフォブロックス DDI API

NetScaler Console IPAMは、次のInfoblox APIを使用してそれぞれのアクションを実行します。

- 利用可能なすべてのInfobloxネットワークを一覧表示します
- 特定のInfobloxネットワークの詳細を取得します
- Infobloxネットワーク上のすべてのIPを一覧表示します
- 特定のIPアドレスの詳細を取得します
- Infobloxネットワーク上のIPを予約および解放します

注:

- NetScaler ConsoleサービスがInfobloxサーバーに到達して接続できるように、Infoblox DNS、DHCP、およびIPアドレス管理 (DDI) サーバーのIPとポートはパブリックネットワークからアクセス可能である必要があります。
- NetScaler Consoleで構成されたInfobloxユーザーアカウントには、Infoblox APIを使用するために必要な権限が必要です。

Infoblox APIの詳細については、Infoblox DDIで入手できるInfoblox REST APIリファレンスガイドを参照してください。

ネットワークを追加

NetScaler Consoleで管理される構成でIPAMを使用するためにネットワークを追加します。

1. **Settings > IPAM** に移動します。
2. **Networks** で、**Add** をクリックします。
3. 次の詳細を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Network Name** - NetScaler Consoleでネットワークを識別するためのネットワーク名を指定します。
- **プロバイダー** - リストからプロバイダーを選択します。

  このリストには、NetScaler Console に追加されたプロバイダーが表示されます。
- **ネットワークタイプ** - 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。
- **ネットワーク値** - ネットワーク値を指定します。

  注:

  NetScaler Console IPAM は IPv4 アドレスのみをサポートしています。

  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。

割り当てられたIPアドレスを表示

IPAMネットワークから割り当てられたIPアドレスの詳細を表示するには、次の手順を実行します。

1. **設定 > IPAM** に移動します。
2. **ネットワーク**タブで、**すべての割り当て済みIPを表示**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このペインには、IPアドレス、プロバイダー名、プロバイダーベンダー、および説明が表示されます。また、このIPアドレスを予約したリソースの詳細も表示されます。

- **モジュール**: IPアドレスを予約したNetScaler Consoleモジュールが表示されます。たとえば、StyleBooksがIPアドレスを予約した場合、この列にはモジュールとしてStyleBooksが表示されます。
- **リソースタイプ**: そのモジュール内のリソースタイプが表示されます。StyleBooksモジュールの場合、構成リソースタイプのみがIPAMネットワークを使用します。そのため、この列には「構成」と表示されます。
- **リソースID**: リンク付きの正確なリソースIDが表示されます。このリンクをクリックすると、IPアドレスを使用しているリソースにアクセスできます。構成リソースタイプの場合、構成パックIDがリソースIDとして表示されます。

注:

IPアドレスを解放したい場合は、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.

ハウツー記事

NetScaler Consoleの「ハウツー記事」は、サービスで利用可能な機能に関する、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、構成管理、イベント管理、アプリケーション管理、StyleBooks、証明書管理など、NetScaler Consoleの一般的な機能に関する情報が含まれています。

次の表の機能名をクリックして、その機能のハウツー記事のリストを表示します。

トピック		
インスタンス管理	構成管理	証明書管理
StyleBooks	イベント管理	

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者パーティションを管理する方法

NetScaler Consoleにインスタンスを追加する方法

NetScaler Consoleでインスタンスグループを作成する方法

NetScaler ConsoleでNetScalerインスタンスとエンティティをポーリングする方法

NetScaler ConsoleでGeomapsのサイトを構成する方法

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

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 MPXまたはVPXのrootパスワードを変更する方法

NetScaler SDXのrootパスワードを変更する方法

構成管理

構成ジョブでSCP (put) コマンドを使用する方法

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleを使用してNetScaler SDXインスタンスをアップグレードする方法

NetScaler Consoleの組み込みテンプレートを使用して作成されたジョブをスケジュールする方法

NetScaler Consoleの組み込みテンプレートを使用して構成されたジョブを再スケジュールする方法

実行構成ジョブを再利用する

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

NetScaler Consoleで構成ジョブを作成する方法

NetScaler Consoleの構成ジョブで変数を使用する方法

NetScaler Consoleで構成テンプレートを使用して監査テンプレートを作成する方法

NetScaler Consoleで修正コマンドから構成ジョブを作成する方法(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-create-jobs-from-corrective-commands.html)

NetScaler Consoleで、実行中および保存済みの構成コマンドをあるNetScalerインスタンスから別のインスタンスにレプリケートする方法(/ja-jp/netscaler-console-service/networks/configuration-jobs/replicate-running-saved-configuration-from-one-adc-to-another.html)

構成ジョブを使用して、1つの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-console-service/networks/configuration-jobs/replicate-configuration.html)

NetScaler Consoleでマスター構成テンプレートを使用する方法(/ja-jp/netscaler-console-service/networks/configuration-jobs/use-master-configuration-template.html)

証明書管理

NetScaler Consoleでエンタープライズポリシーを構成する方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-configure-enterprise-policy.html)

NetScaler ConsoleからNetScalerインスタンスにSSL証明書をインストールする方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-install-ssl-certificates-on-instance.html)

NetScaler Consoleからインストール済みの証明書を更新する方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-update-an-installed-certificate.html)

NetScaler Consoleを使用してSSL証明書をリンクおよびリンク解除する方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-link-and-unlink-ssl-certificates.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Consoleを使用して証明書署名要求 (CSR) を作成する方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-create-csr.html)

NetScaler ConsoleからSSL証明書の有効期限切れに関する通知を設定する方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-set-up-notificationsfor-ssl-certificate-expiry.html)

NetScaler ConsoleでSSLダッシュボードを使用する方法(/ja-jp/netscaler-console-service/networks/ssl-certificate-dashboard/how-to-use-ssl-dashboard.html)

StyleBooks

NetScaler ConsoleでデフォルトのStyleBooksを使用する方法(/ja-jp/netscaler-console-service/stylebooks/how-to-use-default-stylebooks.html)

独自のStyleBooksを作成する方法(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks.html)

NetScaler Consoleでユーザー定義のStyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/how-to-use-default-stylebooks.html)

APIを使用してStyleBookから構成を作成する方法(/ja-jp/netscaler-console-service/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-console-service/stylebooks/how-to-create-custom-stylebooks/how-to-enable-analytics-on-virtual-server-defined-in-stylebooks.html)

NetScaler ConsoleにSSL証明書と証明書キーファイルをアップロードするためのStyleBookを作成する方法(/ja-jp/netscaler-console-service/stylebooks/how-to-create-custom-stylebooks/how-to-create-stylebook-to-upload-ssl-certificate-and-key-files.html)

企業でMicrosoft Skype for Business StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/microsoft-skype-business-stylebook.html)

企業でMicrosoft Exchange StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/microsoft-exchange-stylebook.html)

企業でMicrosoft SharePoint StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/microsoft-sharepoint-stylebook.html)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft ADFS Proxy StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/microsoft-adfs-proxy-stylebook.html)

Oracle E-business StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/oracle-e-business-stylebook.html)

SSO Office 365 StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/sso-office-365-stylebook.html)

SSO Google Apps StyleBookを使用する方法(/ja-jp/netscaler-console-service/stylebooks/business-application-stylebooks/how-to-use-sso-google-apps-stylebook.html)

イベント管理

NetScaler Consoleでイベントの保存期間を設定する方法(/ja-jp/netscaler-console-service/networks/events/create-event-rules.html#step-2---configure-event-age)

NetScaler Consoleを使用してイベントフィルターをスケジュールする方法(/ja-jp/netscaler-console-service/networks/events/how-to-schedule-event-filter.html)

NetScaler Consoleからのイベントの繰り返しメール通知を設定する方法(/ja-jp/netscaler-console-service/networks/events/create-event-rules.html#send-email-action)

NetScaler Console 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 Console でイベントルールを作成する方法

NetScaler インスタンスで発生するイベントの報告された重大度を変更する方法

NetScaler Console でイベントの概要を表示する方法

NetScaler Console で SNMP トラップのイベントの重大度とスキューを表示する方法

NetScaler Console を使用して Syslog メッセージをエクスポートする方法

NetScaler Console で Syslog メッセージを抑制する方法

© 1997–2026 Citrix Systems, Inc. All rights reserved.

よくある質問

いくつのエージェントをインストールする必要がありますか?

エージェントの数は、データセンター内の管理対象インスタンスの数と合計スループットによって異なります。Citrixでは、データセンターごとに少なくとも1つのエージェントをインストールすることをお勧めします。

複数のエージェントをインストールするにはどうすればよいですか?

サービスに初めてログオンするときは、1つのエージェントのみをインストールできます。複数のエージェントを追加するには、まず初期設定を完了し、次に **Settings** > **Setup Agents** に移動します。

NetScalerエージェントはAMDプロセッサをサポートしていますか?

はい。

組み込みエージェントから外部エージェントに移行できますか?

はい、できます。詳細については、「組み込みエージェントから外部エージェントへの移行」を参照してください。

アクティベーションコードを紛失した場合、新しいコードを取得するにはどうすればよいですか?

初めてオンボーディングする場合は、サービスGUIにアクセスし、**Set Up Agent** 画面に移動して、**Generate Activation Code** をクリックします。

2番目のエージェントをインストールしようとしているときに、新しいアクティベーションコードを生成するには、**Infrastructure > Instances > Agents > Generate Activation Code** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

エージェントVMにログオンするにはどうすればよいですかデフォルトの資格情報は何ですか?

エージェントがハイパーバイザーまたはMicrosoft Azureクラウドにインストールされている場合、エージェントのデフォルトのログオン資格情報は `nsrecover/nsroot` で、これによりエージェントのシェルプロンプトが開きます。

エージェントがAWSにインストールされている場合、エージェントにログオンするためのデフォルトの資格情報は `nsrecover/instance id` です。

オンプレミスのハイパーバイザーにエージェントをインストールするためのリソース要件は何ですか?

32 GB RAM、8 仮想 CPU、500 GB ストレージ、1 仮想ネットワークインターフェイス、1 Gbps スループット

プロビジョニング中にエージェントに追加のディスクを割り当てる必要がありますか?

いいえ、追加のディスクを追加する必要はありません。エージェントは、NetScaler Console とエンタープライズデータセンターまたはクラウド内のインスタンスとの間の仲介役としてのみ使用されます。追加のディスクを必要とするインベントリデータや分析データは保存しません。

複数のエージェントでアクティベーションコードを再利用できますか?

いいえ、できません。

誤った値を入力した場合、ネットワーク設定を再実行するにはどうすればよいですか?

ハイパーバイザーでエージェントコンソールにアクセスし、資格情報 nsrecover/nsroot を使用してシェルプロンプトにログオンし、コマンド `networkconfig` を実行します。

エージェントの登録が失敗した場合はどうすればよいですか?

以下を確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- エージェントがインターネットにアクセスできること（DNS を構成）。
- アクティベーションコードを正しくコピーしたこと。
- サービス URL を正しく入力したこと。
- 必要なポートが開いていること。

登録は成功しましたが、エージェントが正常に動作しているかどうかはどうすればわかりますか?

エージェントが正常に登録されたら、NetScaler Console にアクセスし、**Set Up Agent** 画面に移動します。検出されたエージェントが画面に表示されます。エージェントが正常に実行されている場合は緑色のアイコンが表示され、実行されていない場合は赤色のアイコンが表示されます。

プロキシサーバーを使用してエージェントをNetScaler Consoleに接続するにはどうすればよいですか?

プロキシサーバーを使用してエージェントをNetScaler Consoleに接続できます。スクリプトはエージェントの`/mps`フォルダーにあります。エージェントはすべてのデータをプロキシサーバーに転送し、プロキシサーバーはインターネット経由でNetScaler Consoleにデータを送信します。

プロキシサーバーを使用してデータを転送するには、次のスクリプトを使用してエージェントにプロキシサーバーの詳細を入力します: `proxy_input.py`。スクリプトの指示に従って、さらに情報を入力してください。エージェントは、プロキシサーバーを使用してNetScaler Consoleに接続する際に、この情報を取得します。

ユーザー名とパスワード情報を提供することで、プロキシサーバーを認証できます。エージェントがデータを送信すると、プロキシサーバーはNetScaler Consoleに転送する前にユーザー資格情報を認証します。

詳細については、「NetScaler ConsoleをAPIプロキシサーバーとして使用する」を参照してください。

注

NetScaler Consoleは、基本認証が有効になっているプロキシサーバーをサポートしています。NetScaler Consoleは、認証が無効になっているプロキシサーバーもサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アナリティクスレポートが表示されません

アナリティクスレポートを表示するには、仮想サーバーでインサイトを有効にします。詳細については、「アナリティクスの有効化」を参照してください。

NetScaler ConsoleでサポートされているNetScalerインスタンスのバージョンは何ですか?

管理および監視機能については、NetScaler 10.5以降のインスタンスがサポートされています。一部の機能は特定のNetScalerバージョンでのみサポートされています。詳細については、「システム要件」を参照してください。

NetScaler Consoleでダッシュボードレポートをエクスポートするにはどうすればよいですか?

NetScaler Consoleの任意のダッシュボードのレポートをエクスポートするには、このページの右上にある**エクスポート**アイコンをクリックします。**エクスポート**ページで、次のいずれかを実行できます。

1. **今すぐエクスポート**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。 レポートはシステムにダウンロードされます。
2. レポートを定期的に生成およびエクスポートするためのスケジュールを設定するには、**レポートのスケジュール**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。

   a. **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。

   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必ず選択してください。
   - **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必ず入力してください。

   b. **繰り返し時間** - 時刻を24時間形式で`Hour: Minute`入力します。

   c. **メール** - チェックボックスを選択し、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、**追加**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.

d. **Slack** - チェックボックスを選択し、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、**追加**をクリックしてメールプロファイルを作成します。

スケジュールの有効化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。**スケジュールの有効化**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。

クライアント側測定を有効にするとどうなりますか?

クライアント側測定を有効にすると、NetScaler ConsoleはHTMLインジェクションを通じてHTMLページの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。

エージェントからNetScaler Consoleサービスへの SSLトラフィックはSSLインスペクションを通過しますか?

エージェントからNetScaler ConsoleサービスへのSSLトラフィックについては、SSLインスペクションをバイパスすることをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- ダッシュボード
- WAFインサイト
- 学習プロファイルを構成する
- ネットワーク違反の詳細
- WAF学習アクションの概要を表示
- 緩和ルール、アイドルルール、および拒否ルールを表示する
- SSLインサイト
- Webトランザクションの分析を表示する
- デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順
- サービスメッシュトポロジをセットアップするための詳細な手順
- シングルティアまたは統合イングレストポロジを設定するための詳細な手順
- NetScaler® テレメトリプログラムのデータガバナンス
- NetScaler MPXおよびVPXのrootパスワードを変更する方法
- 以前のリリース

ダッシュボード

NetScaler Consoleは、**アウトバウンドトラフィックダッシュボード**と**ユーザーダッシュボード**の2つのダッシュボードを提供します。これらのダッシュボードには、エンタープライズ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。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の数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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トラフィックが使用するプロトコル、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、**Security > Users & Endpoints > Outbound Traffic Dashboard**に移動します。

ネットワークからのアウトバウンドトラフィックを表示する

アウトバウンドトラフィックダッシュボードには、**アウトバウンドトラフィック概要**ペインが含まれています。**アウトバウンドトラフィック概要**ペインでは、NetScaler ConsoleはアクセスされたURLまたはドメインを、ショッピング、ニュース、ソーシャルネットワーキングなどのカテゴリにグループ化します。**アウトバウンドトラフィック概要**ペインには、ネットワークからアクセスされたURLまたはドメインがURLカテゴリ内のノードとして表示されます。ノードのサイズは、URLまたはドメインへのアクセスによって消費されたデータ量に応じて決定されます。ノードの色は、URLまたはドメインへのアクセス中に発生したトランザクションの数を示します。

カテゴリをクリックすると、指定した期間のカテゴリに関連する詳細を表示するようにグラフをフィルタリングできます。

ユーザーダッシュボード

ユーザーダッシュボードには、企業内のユーザーが実行したアクティビティの概要が表示されます。これを使用して、次の主要なメトリックを判断できます。

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、ユーザーが生成した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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

上位ユーザーペインでユーザーをクリックすると、指定した期間に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。

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。選択した期間が1時間の場合、各凡例は1分間隔で集計され、選択した期間が1日の場合、1時間間隔で集計されます。

これらの凡例は集約され、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。期間リストから時間を選択することで、グラフの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

© 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すべてのメトリックが表示されます。このパネルでは、メトリックを選択または選択解除することで、「**トランザクション詳細**」ペイン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。
バイト出力	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 Consoleで、企業内のユーザーに関連するリスクを判断するために使用されるスコアリングシステムです。NetScaler Consoleは、ネットワーク内のユーザーがアクセスする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。次の表に、NetScaler Consoleによって割り当てられるリスクスコアを示します。

リスクスコア	説明
1	ユーザーのWebアクティビティに脅威は認識されず、異常もありません。
2	ユーザーのWebアクティビティに脅威は認識されず、異常もありませんが、ユーザーはURLレ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リスクスコア	説明
	ピュテーションスコアを持たない「不明なサイト」にアクセスしています。
3	ユーザーのWebアクティビティで脅威は検出されませんが、ユーザーは潜在的に脆弱なサイト、または潜在的に脆弱なサイトに関連するサイトへのアクセスを試みました。
4	侵害の可能性のあるユーザー。
5	ユーザーのWebアクティビティが異常であり、既知の悪意のあるサイトにアクセスしています。

WAFインサイト

インターネットに公開されているWebおよびWebサービスアプリケーションは、攻撃に対してますます脆弱になっています。アプリケーションを攻撃から保護するには、過去、現在、および差し迫った脅威の性質と範囲、攻撃に関するリアルタイムで実用的なデータ、および対策に関する推奨事項を可視化する必要があります。WAFインサイトは、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。

注

WAFインサイトは、バージョン11.0ビルド65.31以降で実行されているすべてのNetScalerアプライアンスでNetScaler Consoleでサポートされています。

WAFインサイトの仕組み

WAFインサイトは、アプリケーションに関連する脅威環境を完全に可視化する、直感的なダッシュボードベースのセキュリティ分析ソリューションです。セキュリティインサイトはNetScaler Consoleに含まれており、アプリケーションファイアウォールとNetScalerシステムセキュリティ構成に基づいて定期的にレポートを生成します。レポートには、各アプリケーションに関する次の情報が含まれます。

- **脅威インデックス。** アプリケーションがNetScalerアプライアンスによって保護されているかどうかにかかわらず、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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。値は1から7の範囲です。

脅威インデックスは攻撃情報に基づいています。違反の種類、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インサイトを提供します。違反情報がNetScaler Consoleに送信されるのは、違反または攻撃が発生した場合のみです。多くの侵害と脆弱性は、高い脅威インデックス値につながります。

- **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たかを示す1桁の評価システムです。アプリケーションのセキュリティリスクが低いほど、安全インデックスは高くなります。値は1から7の範囲です。

  安全インデックスは、アプリケーションファイアウォール構成とNetScalerシステムセキュリティ構成の両方を考慮します。高い安全インデックス値を得るには、両方の構成が強力である必要があります。たとえば、厳格なアプリケーションファイアウォールチェックが実施されていても、`nsroot`ユーザーの強力なパスワードなどのNetScalerシステムセキュリティ対策が採用されていない場合、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。
- **実用的な情報。** 脅威インデックスを下げ、安全インデックスを上げるために必要な情報であり、これによりアプリケーションのセキュリティが大幅に向上します。たとえば、違反、アプリケーションファイアウォールやその他のセキュリティ機能の既存および不足しているセキュリティ構成、アプリケーションが攻撃されている速度に関する情報を確認できます。

WAFインサイトの構成

注:

統合セキュリティダッシュボードから保護の構成を開始できます。詳細については、「統合セキュリティダッシュボード」を参照してください。

1. **インフラストラクチャ > インスタンス > NetScaler**に移動し、インスタンスタイプを選択します。たとえば、VPXなどです。
2. インスタンスを選択し、 (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. (仮想サーバーでの分析の構成) ウィンドウで、次の操作を行います。

   a. セキュリティインサイトを有効にする仮想サーバーを選択し、 (セキュリティと分析を有効にする) をクリックします。

   (セキュリティと分析を有効にする) ウィンドウが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. (WAFセキュリティ違反) を選択します。

c. (詳細オプション) で、トランスポートモードとして または 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。

d. 式はデフォルトで true です。

e. をクリックします。

注

- Flexed ライセンスを使用しておらず、ライセンスのない仮想サーバーを選択した場合、NetScaler Console はまずそれらの仮想サーバーにライセンスを付与し、その後分析を有効にします。

をクリックすると、NetScaler Console は選択した仮想サーバーで分析を有効にする処理を開始します。

注

グループを作成すると、そのグループにロールを割り当てたり、アプリケーションレベルのアクセス権を付与したり、ユーザーを割り当てたりできます。NetScaler Consoleアナリティクスは、仮想IPアドレスベースの認証をサポートするようになりました。ユーザーは、権限が付与されているアプリケーション（仮想サーバー）のみについて、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。グループおよびグループへのユーザーの割り当ての詳細については、「NetScaler Consoleでのグループの構成」を参照してください。

セキュリティインサイトレポートの地理的位置を構成する

NetScaler Consoleで地理的位置を構成すると、WAF Insightレポートには、クライアント要求の発信元となる正確な地理的位置が含まれます。地理的位置を有効にするには、組織内の各地理的位

© 1997–2026 Citrix Systems, Inc. All rights reserved.

置に対してプライベートIPブロックまたはIPアドレス範囲を指定します。その情報を、都市/州/国名、および各位置の緯度と経度座標とともに、Geoデータベースファイルに追加します。Geoデータベースファイルを入手するには、NetScalerの担当者にお問い合わせください。その後、そのファイルをNetScalerインスタンスにアップロードします。

地理的位置を構成するには：

1. Geoデータベースファイル Citrix_Netscaler_InBuilt_GeoIP_DB.csv を、NetScalerアプライアンス上の任意の場所にコピーします。
2. viエディターなどのテキストエディターでGeoデータベースファイルを開き、組織内の各場所のエントリを追加します。

   エントリは次の形式である必要があります。

   ```
   <start IP\>,<end IP\>,,<country\>,<state\>,,<city\>,,longitude,latitude
   ```

   例：

   ```
   4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
   ```
3. 地理的位置ロギングとCEF形式でのロギングを有効にするには、次のコマンドを実行します。
   - **add locationFile** <DBファイルを含む完全なパス\>
   - **set appfw 設定** -地理位置情報ロギング 有効
   - **set appfw 設定** -CEFロギング 有効

IPレピュテーションの監視

IPレピュテーション機能は、悪意のあるIPアドレスに関する攻撃関連の情報を提供します。たとえば、IPレピュテーションスコア、IPレピュテーションカテゴリ、IPレピュテーション攻撃時間、デバイスIP、およびクライアントIPアドレスに関する詳細を報告します。

IPレピュテーションスコアは、IPアドレスに関連するリスクを示します。スコアには以下の範囲があります。

IPレピュテーションスコア	危険度
1〜20	高リスク
21〜40	不審
41〜60	中リスク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IPレピュテーションスコア	危険度
61〜80	低リスク
81〜100	信頼できる

IPレピュテーションを監視するには：

1. **Security > Security Violations** に移動し、**WAF** の下で監視したいアプリケーションを選択します。
2. **Threat Index** と **Safety Index** のスコアが表示されます。**View Details** をクリックします。
3. Application Firewall Configuration の下で、IPレピュテーションの安全指数スコアを表示できます。

しきい値

WAF Insight で、アプリケーションの安全指数と脅威指数のしきい値を設定および表示できます。

しきい値を設定するには：

1. **Settings > Analytics Settings > Thresholds** に移動し、**Add** を選択します。
2. Traffic Type フィールドでトラフィックタイプを **Security** として選択し、Name、Duration、entity などの他の適切なフィールドに必要情報を入力します。
3. **Rule** セクションで、Metric、Comparator、および Value フィールドを使用してしきい値を設定します。

   例えば、"Threat Index" ">" "5"
4. **Create** をクリックします。

WAF Insight のユースケース

以下のユースケースでは、セキュリティインサイトを使用してアプリケーションの脅威エクスポージャーを評価し、セキュリティ対策を改善する方法について説明します。

脅威環境の概要を把握する

このユースケースでは、攻撃にさらされている一連のアプリケーションがあり、脅威環境を監視するようにNetScaler Consoleを設定しています。最初に重要なアプリケーションに焦点を当てるために、脅威インデックス、安全性インデックス、およびアプリケーションが経験した可能性のある攻撃の種類と重大度を確認する必要があります。セキュリティインサイトダッシュボードは、選択した期間および選択したNetScalerデバイスについて、アプリケーションが経験した脅威の概

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要を提供します。これには、アプリケーションのリスト、それらの脅威インデックスと安全性インデックス、および選択した期間の攻撃の総数が表示されます。

脅威環境の概要を取得するには、NetScaler Consoleにログオンし、**Security > Security Violation** に移動します。**WAF** の下に、影響を受けた違反の合計数に基づいて上位5つのアプリケーションが表示されます。すべてのアプリケーションを表示するには、**View All** をクリックします。

アプリケーションの既存および不足しているセキュリティ構成を特定する

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適用されており、どのような構成が不足しているかを判断したいと考えるでしょう。この情報は、アプリケーションの概要をドリルダウンすることで取得できます。

概要には、以下のセキュリティ構成の有効性に関する情報が表示されます。

- **アプリケーションファイアウォール構成。** 設定されていないシグネチャとセキュリティエンティティの数を示します。
- **NetScaler Consoleシステムセキュリティ。** 設定されていないシステムセキュリティ設定の数を示します。

Application Firewall Configuration ノードで、セキュリティチェックとセキュリティ違反の情報を確認します。

NetScaler Console System Security ノードをクリックし、システムセキュリティ設定と、アプリケーションの安全性インデックスを向上させるためのCitrixの推奨事項を確認します。

即座に注意が必要なアプリケーションを特定する

即座に注意が必要なアプリケーションとは、脅威インデックスが高く、安全性インデックスが低いアプリケーションです。

特定の時間における攻撃数を特定する

特定の時点であるアプリケーションで発生した攻撃の数を知りたい場合や、特定の期間の攻撃率を調べたい場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAFの下で、任意のアプリケーションをクリックすると、選択した期間に検出されたWAF違反の合計が表示されます。

期間を選択(/en-us/netscaler-console-service/media/analytics-security-insight-attacks-1.png)

ログをクリックすると、重大度と実行されたアクションに基づいて攻撃の詳細が表示されます。ログページには次の詳細が示されます。

- 攻撃時刻
- 攻撃が発生したクライアントのIPアドレス
- 重大度
- 違反カテゴリ
- 攻撃元URL、およびその他の詳細。

学習プロファイルを構成する

NetScaler Consoleで学習プロファイルを構成し、緩和ルールリストを生成するために**NetScaler プロファイル**を選択する必要があります。トラフィックに応じて、NetScalerインスタンスでプロファイルを構成し、NetScaler Consoleで学習プロファイルを構成できます。

注

現在、25個のプロファイルのみを構成できます。

選択した項目に対して緩和ルールリストを生成するように学習プロファイルを構成できます。

- **Webアプリケーション** – 緩和ルールを作成するアプリケーションを選択できます。
- **プロファイル名** – 緩和ルールを作成するWAFプロファイルを選択できます。

学習プロファイルを作成した後、構成されたセキュリティチェックに対してNetScalerが受信トラフィックを受け取らない場合、NetScaler Consoleから緩和ルールを削除するように構成することもできます。

学習プロファイルを構成するには:

1. **Security** > **WAF Learning** > **Learn Profiles** に移動します
2. **Add** をクリックします。

3. **Add Profile Configuration** ページで、次のパラメータを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **学習プロファイル名** – 任意の名前を指定します。

Enable オプションを選択します。デフォルトでは、このオプションは選択されています。このオプションを無効にすると、プロファイルはアクティブになりません。

b. **学習動作** – ルールを生成、ルールを削除、またはその両方を行う学習動作を選択します。

i. **ルールを学習** – 例外ルールを生成し、管理者が展開またはスキップできるようにします。

ii. **アイドルルールを削除** – 設定されたアイドル時間がしきい値を超えたときに、例外ルールを削除します。

iii. **ルールを学習してアイドルルールを削除** – 例外ルールを生成し、受信トラフィックがない場合に削除します。

> **注**
>
> - ルール削除オプションは、**Start URL**、**Deny URL**、**HTML Cross-Site Scripting**、および **HTML SQL Injection** セキュリティチェックでのみサポートされています。
> - **ルールを削除**オプションを選択すると、サポートされているセキュリティチェックオプションが表示されます。

c. **学習グループ** – **プロファイルベース**または**アプリケーションベース**のいずれかを選択します。

d. **WAFプロファイルの選択** – このオプションは、**プロファイルベース**を選択した場合に表示されます。アプリケーションまたはプロファイル名に基づいて、必要なWAFプロファイルを選択します。

WAFプロファイル(/en-us/netscaler-console-service/media/waf-learning-profile.png)

e. **アプリケーションの選択** - このオプションは、**アプリケーションベース**を選択した場合に表示されます。リストからアプリケーションを選択して追加します。

f. **セキュリティチェック**で、NetScaler Consoleで報告された違反に対してアクションを実行したいセキュリティチェックオプションを選択します。オプションを選択すると、次の情報を提供する必要があります。

i. **最小セッション数** – セッションを指定します。NetScaler Consoleは、指定されたセッションがNetScalerインスタンスで発生したことを監視し、緩和リストに報告します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ii. **自動展開** - このオプションにより、管理者はアクション（展開またはスキップ）を実行できます。NetScaler Consoleがこれらの違反を緩和ルールリストに保持する猶予期間（日、時間、分の形式）を指定する必要があります。

指定できる猶予期間の最大値は30日です。

セキュリティチェックパラメータ(/en-us/netscaler-console-service/media/waf-security-check.png)

iii. 「**ルールを削除**」オプションを選択した場合は、「**アイドル時間 (日)**」を日数と時間で指定します。この期間が経過した後、NetScalerがこのセキュリティチェックに対して受信トラフィックを受け取らない場合、ルールは自動的に削除されます。

デフォルトでは、アイドル時間は7日間ですが、この時間は23時間以上に設定できます。

g. 「**通知設定**」で、違反の通知を受け取るための通知オプションを選択します。利用可能な通知オプションは、メール、SMS、Slack、およびServiceNowです。

通知オプションを選択した後、既存の分散プロファイルから選択するか、プロファイルを作成できます。

WAF通知(/en-us/netscaler-console-service/media/waf-enable.png)

h. 「**作成**」をクリックします。

ネットワーク違反の詳細

HTTP スローロリス

スローロリスは、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長い時間がかかります。このプロセスはアプリケーションサーバーのリソースを使い果たし、**HTTP Slow Loris**攻撃につながる可能性があります。

HTTP Slow Lorisインジケーターを使用すると、**HTTP Slow Loris**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**：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 不完全ヘッダー遅延 (incompHdrDelay) 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、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総数を**スローロリス**攻撃として示す検出メッセージ

DNS スローロリス

DNS Slow Lorisインジケーターは、NetScalerが複数のパケットにまたがる多数のDNSリクエストを受信したときに検出します。このプロセスはDNSサーバーのリソースを使い果たし、**DNS Slow Loris**攻撃につながる可能性があります。デフォルトでは、NetScalerインスタンスはこれらの**DNS スローロリス**リクエストを破棄し、この問題をトラブルシューティングするためのさらなるアクションは必要ありません。

「**イベントの詳細**」で、以下を表示できます。

- 影響を受けるアプリケーション。2つ以上のアプリケーションが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
- 総DNS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

HTTP スローポスト

Slow Post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もあります。

このプロセスは、アプリケーションサーバーのリソースを使い果たし、**HTTP Slow Post**攻撃につながる可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HTTP Slow Post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。

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**攻撃として検出されたことを示す検出メッセージ

NXDOMAINフラッド攻撃

NXDOMAINフラッド攻撃は、DNSサーバーまたはNetScalerインスタンス（DNSプロキシサーバーとして構成されている場合）を標的とし、大量の存在しないリクエストまたは無効なリクエストを送信する分散型サービス拒否（DDoS）攻撃です。この攻撃は、DNSサーバーまたはNetScalerインスタンスに影響を与え、速度低下やリクエストへの応答がない状態を引き起こす可能性があります。

NXDOMAINフラッド攻撃インジケーターを使用して、リクエストがNXDOMAIN攻撃につながったかどうかを分析できます。

NXDOMAIN(/en-us/netscaler-console-service/media/nxdomain.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**：

- DNSサーバーとDNSプロキシサーバーの両方で、異常に高いリソース消費がないか確認します。
- NetScalerインスタンスでリクエストレートの制限を適用します。
- 不審なクライアントIPアドレスを特定し、ブロックします。
- ほとんどの名前がNXDOMAINになる場合、識別可能なパターンに従い、そのようなリクエストを破棄するようにDNSポリシーを構成します。
- 正当なDNSレコードのメモリを節約するために、NetScalerインスタンスでネガティブレコードの制限を構成します。詳細については、DNS DDoS攻撃の軽減を参照してください。

© 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デシンク攻撃では、単一のHTTPリクエストが次のように解釈されます。

- フロントエンドサーバー（仮想サーバー）への単一のリクエスト
- バックエンドサーバーへの2つのリクエスト

このシナリオでは、バックエンドサーバーは2番目のリクエストが別のクライアントからのものと解釈します。仮想サーバーとバックエンドサーバー間の接続は、異なるリクエストに対して再利用されます。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インスタンスが以下の存在によって発生したHTTPデシンク攻撃を受けてい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

  HTTPデシンク攻撃の図](/en-us/netscaler-console-service/media/http-desync-attack.png)

推奨されるアクションでは、無効なHTTPトランザクションを破棄することを検討するよう提案しています。

イベントの詳細では、以下を表示できます。

- 影響を受けるアプリケーション。この違反によって2つ以上のアプリケーションが影響を受けている場合は、リストからアプリケーションを選択することもできます。
- 違反の詳細を示すグラフ。棒グラフにマウスポインターを合わせると、無効なリクエスト/レスポンスの合計を表示できます。
- 違反の検出メッセージ。合計リクエスト/レスポンスを示します。
  - 異なる値を持つ複数のコンテンツ長ヘッダーを含む
  - コンテンツ長と転送エンコーディングの両方のヘッダーを含む

© 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化時に正しいパディング形式を持っているかどうかを検出します。

Bleichenbacher攻撃インジケーターを使用して、NetScalerインスタンスが誤った暗号化データを含むSSL/TLSハンドシェイク接続を受信しているかどうかを分析できます。

推奨されるアクションは、NetScalerインスタンスがハンドシェイク接続を終了し、この攻撃を軽減するため、それ以上の操作は不要であることを示しています。

イベントの詳細では、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。
- 違反の検出メッセージ。誤った暗号化データを持つ仮想サーバー上のハンドシェイク接続の合計数を示します。

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して、NetScalerインスタンスが設定されたキュー制限よりも多くの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。

「**イベントの詳細**」では、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.

SYNフラッド攻撃

SYNフラッド攻撃は、偽装されたIPアドレスを使用して数千の接続要求を送信することで、ターゲットマシンに影響を与える可能性のあるサービス拒否（DoS）攻撃です。NetScalerインスタンスが**SYNフラッド**攻撃を受けている場合、インスタンスは悪意のある各要求に対して接続を開こうとし、その後、決して届かない確認応答パケットを待ちます。

TCPプロファイルの**SYNCOOKIE**は、NetScalerアプライアンスへのSYN攻撃を防ぎます。デフォルトでは、NetScalerインスタンスの**SYNCOOKIE**は有効になっています。NetScalerインスタンスがSYNフラッド攻撃を受ける可能性が高いのは、`SYNCOOKIE`が無効になっている場合のみです。詳細については、「レイヤー3〜4 SYNサービス拒否保護」を参照してください。

SYNフラッド攻撃インジケーターを使用して、NetScalerインスタンスがSYN攻撃を受けているかどうかを分析できます。

管理者として、「**推奨されるアクション**」では、TCPプロファイルで`SYN COOKIE`を有効にすることをお勧めします。

「**イベントの詳細**」では、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。
- 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アタック

スモールウィンドウアタックは、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。ターゲットマシンに同様の接続をできるだけ多く送信することで、ターゲットマシンのメモリが最大限に利用され、応答しなくなります。

スモールウィンドウアタックインジケーターを使用して、NetScalerインスタンスがソックスストレス攻撃を受けているかどうかを分析できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デフォルトでは、NetScalerインスタンスは、そのようなすべてのTCPスモールウィンドウパケットを破棄することで、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します。
- 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。

WAF学習アクションの概要を表示

WAF学習の**アクションの概要**ページでは、デプロイされたすべてのルールを表示できます。

ダッシュボード(/en-us/netscaler-console-service/media/waf-dashboard.png)

1 – ダッシュボードで詳細を表示するには、リストから**学習済みルール**または**アイドルルール**を選択します。

2 – 提案と演算子に基づいて結果を表示できる高度な検索バー。

3 – 結果を表示したい期間のリスト

4 – 結果をフィルタリングするためにグラフをドラッグして選択できるグラフ形式の結果

5 – デプロイ済みまたは削除されたルールの詳細

詳細を表示するには、**>**をクリックします。

失敗したルールを表示

デプロイされた学習ルールが失敗した場合、その失敗理由を表示できます。

失敗したルール(/en-us/netscaler-console-service/media/failed-rule.png)

高度な検索

高度な検索バーを使用すると、要件に応じて結果を表示できます。検索ボックスをクリックすると、検索ボックスに検索候補のリストが表示されます。検索クエリで演算子を使用して、検索の焦点を絞ることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

検索ボックスにマウスポインターを置くと、次の候補が表示されます。

- **Learn-Profile-Name** – 設定した学習プロファイル名を示します。
- **Rule-Type** – ルールタイプ（拒否または許可）を示します。
- **Violation-Name** – Start URL、クロスサイトスクリプトなどの違反名を示します。
- **URL** – WebアプリケーションのURLを示します。
- **Status** – 展開されたルールのステータスを示します。
- **Field-Name** – フォームフィールドセキュリティチェックのためにWebフォームで更新されたフィールド名を示します。
- **Violation-String** – 違反が発生した可能性のある文字列を示します。
- **Value-Type** – セキュリティチェックで使用されるデータ型を示します。例：キーワード。

結果をフィルタリング

アクションの概要から、以下のオプションを選択して結果をフィルタリングできます。

- **学習プロファイル名** - 学習プロファイル名に基づいてフィルタリングします。
- **違反名** - Start URL、HTMLクロスサイトスクリプティング、コンテンツタイプなどの違反名に基づいてフィルタリングします。
- **ステータス** - 展開済みまたはアイドル状態のルールのステータスに基づいてフィルタリングします。
- **実行者** - ユーザーに基づいてフィルタリングします。

  アクションサマリー(/en-us/netscaler-console-service/media/waf-action-summary.png)

緩和ルール、アイドルルール、および拒否ルールを表示する

学習プロファイルを構成すると、NetScaler Console は緩和ルール、アイドルルール、および拒否ルールのリストの取得を開始します。

1. **Security** > **WAF Learning** > **Learn Profiles** の順に移動します。

   Learn Profiles ページには、WAF 学習プロファイル名、関連付けられている NetScaler インスタンスの合計数、インスタンスで作成された WAF プロファイルの合計数、学習済みルールの合計数、展開済みルールの合計数、およびステータスが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. プロファイル名を選択し、**Manage Relaxation Rules** をクリックします。

   選択したプロファイルの合計ルール数、学習済みルール数、展開済みルール数、アイドルルール数を表示できます。

   - **Learned Rules** タブで、緩和されたルールを表示できます。ルールを選択し、検証して、**Add & Deploy**、**Deploy**、**Edit & Deploy**、**Delete**、または **Deploy as Deny** をクリックします。
     - **Add & Deploy** - セキュリティチェックオプションを使用して新しいルールを作成できます。ルールを作成したら、**Deploy** をクリックします。
     - **Deploy** - 緩和されたルールを展開できます。
     - **Edit & Deploy** - 展開する前にルールを編集できます。SQL セキュリティチェックの場合、ルールを編集して **Rule Type** を **Deny** に変更してから展開できます。

       詳細については、「HTML SQL インジェクション攻撃を処理するための緩和ルールと拒否ルール」を参照してください。
     - **Delete** - 何もアクションを実行せずにルールを削除できます。
     - **Deploy as Deny**」 - SQLセキュリティチェックの場合、このオプションを使用してリクエストを拒否できます。
   - 「**Deployed Rules**」タブをクリックして、デプロイされたルールを表示します。ルールを選択し、そのルールを削除、有効化、または無効化します。
   - 「**Idle Rules**」タブをクリックして、トラフィックのないアイドルルールを表示します。ルールを削除する場合は、「**Delete**」をクリックします。

   注

   違反リストは、設定された猶予期間が終了するまで利用可能です。猶予期間が終了すると、NetScaler Consoleは利用可能な違反を自動的にデプロイします。

   設定された学習済みプロファイルごとに、最大100万個の学習済みルールを表示できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

拒否ルールを管理する

リラクゼーション（許可）モードに加えて、HTML SQLインジェクション攻撃セキュリティチェックを処理するための拒否ルールも構成して使用できます。HTML SQLインジェクションセキュリティチェックを拒否モードで構成すると、検出された違反はブロックされます。

「**Manage Deny Rules**」タブで、HTML SQLインジェクションチェックの拒否されたルールを表示できます。ルールを選択し、検証して、「**Add & Deploy**」、「**Deploy**」、「**Edit & Deploy**」、「**Delete**」、または「**Deploy as Relaxation**」をクリックします。

- 「**Add & Deploy**」 - セキュリティチェックオプションを使用して新しいルールを作成できます。ルールを作成したら、「**Deploy**」をクリックします。
- 「**Deploy**」 - 拒否されたルールをデプロイできます。
- 「**Edit & Deploy**」 - デプロイする前にルールを編集できます。
- 「**Delete**」 - 何もアクションを実行せずにルールを削除できます。
- 「**Deploy as Relaxation**」 - トラフィックを許可します。

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、統合されたリアルタイムおよび履歴のセキュアなWebトランザクション監視を提供することで、IT管理者がNetScalerによって提供されるすべてのセキュアなWebアプリケーションを監視できるようにします。この可視性により、管理者は以下を評価できます。

- **構成変更が顧客の使用状況に与える影響を判断する**。管理者は、SSLv3をオフにしたり、RC4-MD5のような暗号を削除したりするなどの構成変更がクライアントに与える影響を理解できます。これは、このプロトコルと暗号に関する履歴トランザクションデータを評価することで実行できます。
- **クライアントのパフォーマンスを定量化する**。管理者は、使用されているSSL暗号/プロトコルまたはネゴシエートされた証明書に基づいて、アプリケーション応答時間への影響を理解できます。
- **アプリケーションのセキュリティ**。いずれかのアプリケーションが、セキュリティの低いプロトコル、暗号、または弱い鍵強度でトランザクションを実行しているかどうかを評価します。

NetScalerインスタンスでSSL Analyticsが有効になっている場合、すべてのSSLトランザクションについてSSL統計が記録およびログに記録されます。統計にはSSLフローの詳細が表示されます。また、すべての成功した接続はNetScaler Consoleによってログに記録され、表示されます。

SSL Insightは、NetScaler Console Analyticsによって表示される以下の重要な情報を提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ネゴシエートされたSSLプロトコルバージョン
- ネゴシエートされた暗号と暗号強度
- 使用された証明書の署名ハッシュアルゴリズム
- 証明書の種類とサイズ
- SSLフロントエンドおよびバックエンドエラー

注

成功した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。SSL Insightのトランスポートタイプとして**Logstream**を有効にするには、11.1 51.21を実行しているNetScalerインスタンスで次のコマンドを実行します。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the NetScaler Console>`

   バージョン12.0以降を実行しているNetScalerインスタンスの場合、NetScaler ConsoleからAppFlowを有効にする際に、トランスポートタイプとして**Logstream**を選択します。

- NetScaler Consoleのバージョンとビルドは、NetScalerのバージョンとビルドと同じかそれ以上である必要があります。たとえば、NetScaler Console 11.1ビルド61.7をインストールしている場合、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を構成する

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パラメータを有効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インサイトを有効にする

注

AppFlow機能は、NetScaler Consoleから、または各NetScalerインスタンスから有効にできます。

NetScaler ConsoleからAppFlow機能を有効にする

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. 「**Select Action**」リストから、「**Configure Analytics**」を選択します。
3. 「**Configure Analytics on Virtual Servers**」ページで、次の操作を行います。

   a. Web Insight を有効にする仮想サーバーを選択し、「**Enable Security & Analytics**」をクリックします。

   「**Enable Security & Analytics**」ウィンドウが表示されます。

   b. 「**Web Insight**」を選択します。

   c. 「**Advanced Options**」で、トランスポートモードとして「**Logstream**」または「**IPFIX**」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。

   d. 式はデフォルトで true です。

   e. 「**OK**」をクリックします。

注

仮想サーバーの稼働状態が UP 以外の場合、その仮想サーバーでデータ収集を有効にすることはできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler GUI を使用して AppFlow 機能を有効にする

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。

ULFDモードを有効にする

仮想サーバーが構成されているNetScalerインスタンスでULFDモードを有効にすると、ULFDサーバーはNetScalerインスタンスからNetScaler Consoleに分析データをストリーミングします。

SSL Insightパラメーターを有効にする

各NetScalerインスタンスで、NetScaler ConsoleにSSL Insightレコードを表示するために、いくつかのHTTPパラメーター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パラメーターを有効にする

1. **Configuration** > **System** > **AppFlow** に移動し、**Change AppFlowSettings** をクリックします。
2. 次のチェックボックスを選択します: **HTTP Domain**、**HTTP Host**、**HTTP Method**、**HTTP URL**、**HTTP User-Agent**、**HTTP Content-Type**。
3. **OK** をクリックします。

SSL Insightメトリックを表示する

NetScaler ConsoleのSSL Insightメトリックは、NetScalerインスタンスによって提供される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メトリックを表示できます。これらのメトリックを利用して、NetScaler HTTPS設定とSSL証明書設定を分析および最適化し、パフォーマンスの問題を追跡できます。

注

グループを作成する際、グループにロールを割り当て、グループにアプリケーションレベルのアクセスを提供し、グループにユーザーを割り当てることができます。NetScaler Consoleアナリティクスは、仮想IPアドレスベースの認証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のレポートを見ることができます。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、「NetScaler Consoleでのグループの構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ConsoleでSSL Insightメトリックを監視する

管理者として、以下のSSLメトリックを表示できます。

- アプリケーション。**Applications > Dashboard** に移動し、アプリケーションをクリックして、**Web Insight** タブを選択すると、詳細なメトリックが表示されます。詳細については、「アプリケーション使用状況分析」を参照してください。
- すべてのアプリケーション。**Applications > Web Insight** に移動し、**Applications** タブと **Clients** タブをクリックすると、SSLメトリックが表示されます。

ユースケース: SSLトランザクションの概要を取得する

次のユースケースでは、SSL Insight を使用してさまざまな SSL パラメータの使用状況を評価し、セキュリティ対策を改善する方法について説明します。

通信に SSL トランザクション (HTTPS) を使用する一連のアプリケーションがあり、SSL コンポーネントを監視するように NetScaler Console を構成しているとします。最も注意が必要なアプリケーションに最初に焦点を当てられるように、アプリケーションを頻繁に確認する必要があるかもしれません。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 Errors** および **SSL Usage** の下に、次の SSL パラメータの概要が表示されます。

- SSL証明書
- SSLプロトコル
- SSL暗号
- SSLキー強度
- SSL障害 – フロントエンド
- 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: クライアントの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して、選択したクライアントのSSLメトリックを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSLクライアントメトリック(/en-us/netscaler-console-service/media/ssl-client.png)

Webトランザクションの分析を表示する

Webトランザクション分析により、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トランザクションは、いくつかのサンプルのみ表示できます。

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。

1. **Settings > Analytics Settings > Enable Features for Analytics** に移動し、次のいずれかを選択します。
   - **なし** - データは表示されません。
   - **すべて** - すべてのHTTPトランザクションを表示します。このオプションを選択すると、NetScaler Consoleはより多くのストレージを消費します。このオプションは、重要なアプリケーションにのみ使用してください。
   - **異常** - 5xxエラーおよび応答時間 > 500ミリ秒のトランザクションを表示します。

2. 仮想サーバーのanalyticsを有効にするときに、**Web Insight** の下にある **Detailed Web Transactions** を選択します。

   注記:

   14.1-44.xビルド以降、**Webトランザクション分析**は仮想サーバーレベルで利用可能です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細なWebトランザクション

この機能は、詳細なトランザクションを調査できるだけでなく、クライアント、NetScaler、およびサーバーにわたって視覚的に分割されたメトリック (クライアントRTT、サーバー応答時間、SSLメトリックなど) も理解できます。

注記:

一部のシナリオでは、NetScalerが一部のトランザクションのRTT値を計算できない場合があります。そのようなトランザクションの場合、NetScaler ConsoleはRTT値を次のように表示します。

- **NA** – NetScalerインスタンスがRTTを計算できない場合に表示されます。
- **< 1ms** – NetScalerインスタンスが0ミリ秒から1ミリ秒の間の小数でRTTを計算する場合に表示されます。例: 0.22ミリ秒。

詳細なトランザクションは以下で表示できます。

- **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アプリケーション** – **アプリケーション** > **サービスグラフ**に移動します。サービスをクリックし、**トランザクションログ**を選択します。

  注記:

  エラーを表示するには、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します。

  「問題数」(/en-us/netscaler-console-service/media/web-transaction-issue.png)

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**を含む詳細なトランザクションが表示されます。

「トランザクションサマリー」(/en-us/netscaler-console-service/media/transactions.png)

アプリ応答にマウスポインターを合わせると、NetScaler インスタンスおよびサーバーからの RTT や処理時間などの詳細が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の例は、問題がサーバーに起因してい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。

「トランザクションサマリー」(/en-us/netscaler-console-service/media/transactionsummary3.png)

ドラッグして選択することで、特定の期間のトランザクションを表示することもできます。

「選択されたトランザクション」(/en-us/netscaler-console-service/media/select-transaction.png)

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。

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-console-service/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る詳細を確認できます。

「詳細なトランザクション」(/en-us/netscaler-console-service/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-console-service/media/ssl-detailed-metrics.png)

Transaction SummaryパネルからSSLフロントエンドおよびSSLバックエンドメトリックをクリックして、結果をフィルタリングすることもできます。

結果をフィルタリングするには、**Transaction Summary**の下で利用可能なオプションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トランザクションサマリー(/en-us/netscaler-console-service/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。
- **リクエストタイプ**: トランザクションリクエストのタイプ。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でなければなりません。
- **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に基づく暗号強度（高、中、低など）。
- **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に基づく暗号強度（高、中、低など）。
- **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タイプ。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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高度な検索

トランザクションサマリーには、検索テキストボックスと期間リストもあり、要件に応じてイベントを表示できます。検索ボックスにカーソルを置くと、検索ボックスに検索候補のリストが表示されます。検索クエリで演算子を使用して、検索の焦点を絞り込むこともできます。

検索クエリに使用できる演算子は次のとおりです。

演算子	説明	例	出力
=	ある値と等しい	仮想サーバー = test	名前が「test」の仮想サーバーのイベントを表示します。
>	ある値より大きい	アプリケーション応答時間 > 500	アプリケーション応答時間が500ミリ秒を超えるアプリケーションのイベントを表示します。
<	ある値より小さい	App-Response-Time が 300 未満	アプリケーション応答時間が300ミリ秒未満のアプリケーションのイベントを表示します。
>=	ある値以上	Total-Bytes が 1024 以上	1KB以上のトランザクションのイベントを表示します。
<=	ある値以下	合計バイト数 <= 1024	1KB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。
~	何らかの値を含む	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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、合計バイト数が300バイト未満のイベントを生成したいシナリオを考えてみましょう。検索クエリは次のように指定します。

1. 検索ボックスに必要な単語を入力して、関連する候補を取得します。

2. **Total-Bytes**を選択し、検索テキストボックスをもう一度クリックして、**\<**を選択します。

3. 値「300」を入力します。

4. 期間を選択し、**Search**をクリックして、検索クエリに基づいた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

候補と演算子を使用した後に、検索クエリを保存できます。これにより、候補と演算子を再度使用する代わりに、後でリストから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から、**保存**をクリックします。

  検索を保存(/en-us/netscaler-console-service/media/save-searches.png)

- リストから検索クエリを使用するには、アイコンをクリックし、リストから検索クエリを選択して結果を表示します。

  保存された検索(/en-us/netscaler-console-service/media/search-list.png)

- 検索クエリを削除するには、アイコンをクリックし、保存された検索クエリにマウスポインターを合わせ、**削除**をクリックします。

  削除(/en-us/netscaler-console-service/media/web-remove.png)

  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。

  削除(/en-us/netscaler-console-service/media/remove-bookmark.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データのエクスポート

エクスポートアイコンをクリックして、選択した期間のWebトランザクション分析データをエクスポートできます。PDF、PNG、JPEG、CSV形式でエクスポートできます。**エクスポート**オプションを使用すると、次のいずれかを実行できます。

- **今すぐエクスポート**を選択して、レポートをPDF、JPEG、PNG、またはCSV形式で表示およびエクスポートします。
- **エクスポートのスケジュール**タブを選択して、レポートを毎日、毎週、または毎月スケジュールし、電子メールまたはSlackメッセージでレポートを送信します。

デュアルティアまたはサービスメッシュライトトポロジを設定するための詳細な手順

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デプロイ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エージェントを構成する

KubernetesクラスターとNetScaler Console間の通信を有効にするには、エージェントをインストールして構成する必要があります。エージェントは、ハイパーバイザー、パブリッククラウドサービス（Microsoft Azure、AWSなど）、またはNetScalerインスタンスで利用可能な組み込みエージェント（HA展開に最適）を使用して構成できます。

エージェントを構成するには、手順に従ってください。

注

- 既存のエージェントを使用することもできます。
- エージェントは、デフォルトでNetScaler Consoleの最新ビルドに自動的にアップグレードされます。エージェントの詳細は、**Infrastructure > Instances > Agents**ページで確認できます。エージェントのアップグレードが行われる時間を指定することもできます。詳細については、エージェントアップグレード設定の構成を参照してください。

エージェント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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ConsoleからKubernetesクラスターへの通信を有効にするには、エージェントで静的ルーティングを構成する必要があります。

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。

例のコマンド(/en-us/netscaler-console-service/media/static-routing-example.png)

エージェントの構成が正常に完了したら、次の手順を実行します。

1. SSHクライアントを使用してエージェントにログオンします。
2. `shell`と入力し、**Enter**キーを押して`bash`に切り替えます。
3. コマンド`route add -net <public IP address range> <Kubernetes IP address>`を使用して静的ルーティングを構成します。

   例：

   ```
   route add -net 192.168.0.0/24 101.xx.xx.112
   ```

   ```
   route add -net 192.168.1.0/24 101.xx.xx.111
   ```

   ```
   route add -net 192.168.2.0/24 101.xx.xx.110
   ```
4. `netstat -rn`を使用して構成を確認します。

   静的ルーティング(/en-us/netscaler-console-service/media/static-routing.png)
5. 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エージェントで、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例: `route add -net 192.168.0.0/24 101.xx.xx.112`.

GitHub からサンプルデプロイファイルをダウンロードする

1. マスターノードで Git Hub リポジトリをクローンするには、コマンド **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git` を使用します。
2. YAML にアクセスするには:

```
cd citrix-k8s-ingress-controller/example/servicegraph-demo/
```

CPX YAML ファイルにパラメータを追加する

注

CPX 58.x 以降を使用している場合は、エージェントに登録する際に非 nsroot 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 Console への CPX 登録を確実にするには、`cpx.yaml` ファイルに次のパラメータを含める必要があります。

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"

  value: "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"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – エージェントの IP アドレスを示します
- **NS_MGMT_FINGER_PRINT** – エージェント内の CPX の認証を示します。フィンガープリントを取得するには:

  a. NetScaler Console で、**Infrastructure > Instances > Agents** に移動します

  b. エージェントを選択し、 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** – エージェントのIPアドレスを示します。CPXからNetScaler Consoleにログデータを転送するには、**Logstream** プロトコルを有効にする必要があります

NetScaler ConsoleでVPX、SDX、MPX、またはBLXインスタンスを追加する

サービスグラフでティア1 NetScalerインスタンスの分析を取得するには、NetScaler ConsoleにVPX/SDX/MPX/BLXインスタンスを追加し、**Web Insight** を有効にする必要があります。NetScaler ConsoleがVPX/SDX/MPX/BLXインスタンスからのWebトランザクションの詳細を表示するには、**Web Insight** を有効にする必要があります。

1. **> >** の順に移動します
2. オプションをクリックしてインスタンスを追加します。詳細については、「NetScaler Consoleでインスタンスを追加する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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、「ライセンスを管理し、仮想サーバーで分析を有効にする」を参照してください。

NetScaler ConsoleでKubernetesクラスターを追加する

Kubernetesクラスターを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. 「**Infrastructure > 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。

   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 Console間の通信アクセスを検証するために必要です。認証トークンを生成するには：

      Kubernetesマスターノードで：

      i. 以下の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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サービスアカウントが作成されます。

iii. クラスターロールをサービスアカウントにバインドするために `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` を実行します。

サービスアカウントはクラスター全体のアクセス権を持つようになりました。

サービスアカウントの作成中にトークンが自動的に生成されます。

iv. トークンを表示するには、`kubectl describe sa <name>` を実行します。

v. シークレット文字列を取得するには、`kubectl describe secret <token-name>` を実行します。

d. リストからエージェントを選択します。

注

CPX YAML に追加したのと同じエージェントを選択していることを確認してください。

e. **作成** をクリックします。

サンプルのマイクロサービスアプリケーションを展開する

マスターノードで:

1. 名前空間を作成するには、`kubectl create -f namespace.yaml` を実行します。
2. 次のコマンドを使用して、`hotdrink` マイクロサービス、イングレス、およびシークレットを展開します。

```
kubectl create -f team_hotdrink.yaml -n sg-demo
```

```
kubectl create -f hotdrink-secret.yaml -n sg-demo
```

CPXを展開し、NetScaler ConsoleにCPXを登録する

1. `kubectl create -f rbac.yaml`を実行して、クラスターロールとクラスターバインディングを展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. `kubectl create -f cpx.yaml -n sg-demo`を実行して、CPXを展開します。

展開後、CPXの登録は自動的に行われます。

ライセンス供与のために仮想サーバーの自動選択を有効にする

注

> 十分な仮想サーバーライセンスがあることを確認してください。詳細については、「ライセンス」を参照してください。

NetScaler ConsoleにKubernetesクラスターを追加した後、ライセンス供与のために仮想サーバーを自動選択するようにしてください。サービスグラフにデータを表示するには、CPX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 > NetScaler Console ライセンスと分析設定**に移動します。
2. **仮想サーバーライセンス概要**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トランザクション設定とTCPトランザクション設定を有効にする

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 Transaction Settings**と**TCP Transactions Settings**を**All**に変更します。

1. **Settings > Analytics Settings**に移動します。

   Settingsページが表示されます。
2. 「**Enable Features for Analytics**」をクリックします。
3. 「**Web Transaction Settings**」で、「**All**」を選択します。

4. 「**TCP Transactions Settings**」で、「**All**」を選択します。

5. 「**OK**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

マイクロサービスにトラフィックを送信する

次に、NetScaler Consoleにサービスグラフを表示させるために、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を介してCPXを公開するために、`kubectl get svc -n sg-demo`を実行します。

2. **etc/host**ファイルを編集し、`hotdrink.beverages.com`のドメインIPエントリを作成します。

   これで、`https://hotdrink.beverages.com`を使用してマイクロサービスにアクセスできます。

サービスメッシュトポロジを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展開するための前提条件は、サービスグラフのセットアップで確認できます。

NetScalerエージェントを構成する

KubernetesクラスターとNetScaler Console間の通信を有効にするには、エージェントをインストールして構成する必要があります。エージェントは、ハイパーバイザー、パブリッククラウドサービス（Microsoft Azure、AWSなど）、またはNetScalerインスタンスで利用可能な組み込みエージェント（HA展開に最適）を使用して構成できます。

エージェントを構成するには、手順に従ってください。

注

- 既存のエージェントを使用することもできます。
- エージェントは、デフォルトでNetScaler Consoleの最新ビルドに自動的にアップグレードされます。エージェントの詳細は、**インフラストラクチャ > インスタンス > エージェント**ページで確認できます。エージェントのアップグレードを実行する時間を指定することもできます。詳細については、「エージェントアップグレード設定の構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

エージェントで静的ルートを構成する

Kubernetesクラスター内では、すべてのコンテナ化されたポッドがオーバーレイネットワークを使用します。これらのプライベートIPアドレスを使用して直接通信を確立することはできません。NetScaler ConsoleからKubernetesクラスターへの通信を有効にするには、エージェントで静的ルーティングを構成する必要があります。

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、次のコマンドを実行して、静的ルーティングを行うポッドネットワークを特定します。

```
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。

エージェントを正常に構成した後:

1. SSHクライアントを使用してエージェントにログオンします
2. `shell` と入力し、**Enter**キーを押して `bash` に切り替えます
3. コマンド `route add -net <public IP address range> <Kubernetes IP address>` を使用して静的ルーティングを構成します

   例:

   `route add -net 192.168.0.0/24 101.xx.xx.112`

   `route add -net 192.168.1.0/24 101.xx.xx.111`

   `route add -net 192.168.2.0/24 101.xx.xx.110`
4. `netstat -rn` を使用して構成を確認します

5. 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. エージェントで、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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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`。

必要なパラメータを設定する

Kubernetesマスターで:

1. CPXがイングレスゲートウェイ/サイドカーとして展開されているすべての名前空間で、エージェントの資格情報を使用してシークレットを作成します。

   `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>`

2. `helm repo add citrix https://citrix.github.io/citrix-helm-charts/`
3. NetScaler CPXをイングレスゲートウェイとして展開する

   `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   次の表に、Helmチャートで設定可能なパラメータとそのデフォルト値を示します:

パラメータ	説明	デフォルト	任意/必須 (ヘルム)
citrixCPX	NetScaler CPX	FALSE	NetScaler CPX に必須
xDSAdaptor.image	Citrix xDS アダプターコンテナのイメージ	quay.io/citrix/citrix-istio-adaptor:1.2.1	必須
ADMSettings.ADMIP	NetScaler Console の IP アドレス	なし	NetScaler CPX に必須
ADMSettings.ADMFingerPrint	NetScaler Console のフィンガープリント。**Infrastructure > Instances > Agents** に移動し、	なし	任意

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータ	説明	デフォルト	任意/必須 (ヘルム)
	エージェントを選択して、**View Fingerprint** をクリックします。		
ingressGateway.EULA	エンドユーザーライセンス契約 (EULA) の利用規約。はいの場合、ユーザーは EULA の利用規約に同意します。	いいえ	NetScaler CPX に必須
ingressGateway.image	イングレスゲートウェイ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。

パラメーター	説明	デフォルト値
ADMSettings.ADMIP	NetScaler Console 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) の利用規約。	いいえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター	説明	デフォルト値
	はいの場合、ユーザーはEULAの利用規約に同意します。	
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任意のNamespace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を実行した後、NetScaler CPXがNetScaler Consoleに登録されていることを確認できます。

サンプルアプリケーションを展開する

以下のアプリケーションを展開するとします。

サンプルアプリを展開(/en-us/netscaler-console-service/media/deploy-sample-apps.png)

サンプルアプリケーションを展開するには、以下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`

   注

   > 任意のユーザー名とパスワードを設定できます。

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

ユーザー名とパスワードは任意で指定できます。

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

   NetScaler Consoleのフィンガープリントとエージェントの 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

   NetScaler Consoleのフィンガープリントとエージェントの IPアドレスを指定する必要があります。

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

NetScaler ConsoleでKubernetesクラスターを追加する

Kubernetesクラスターを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Infrastructure > Orchestration > Kubernetes > Cluster** の順に移動します。 クラスターページが表示されます。
3. **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **名前** - 任意の名前を指定します。

b. **APIサーバーURL** - KubernetesマスターノードからAPIサーバーURLの詳細を取得できます。

   i. Kubernetesマスターノードで、コマンド`kubectl cluster-info`を実行します。

   ii. **「Kubernetes master is running at.」**と表示されるURLを入力します。

c. **認証トークン** - 認証トークンを指定します。認証トークンは、KubernetesクラスターとNetScaler Console間の通信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. 以下のYAMLを使用してサービスアカウントを作成します:

   ```
   apiVersion: v1

   kind: ServiceAccount

   metadata:

     name: <name>

     namespace: <namespace>
   ```

   ii. `kubectl create -f <yaml file>`を実行します。

   サービスアカウントが作成されます。

   iii. クラスターロールをサービスアカウントにバインドするには、`kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>`を実行します。

   サービスアカウントは、クラスター全体のアクセス権を持つようになります。

   サービスアカウントの作成中にトークンが自動的に生成されます。

   iv. トークンを表示するには、`kubectl describe sa <name>`を実行します。

   v. シークレット文字列を取得するには、`kubectl describe secret <token-name>`を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. リストからエージェントを選択します。

注

CPX YAMLに追加したエージェントと同じエージェントを選択していることを確認してください。

e. **作成**をクリックします。

クラスターの追加(/en-us/netscaler-console-service/media/add-cluster.png)

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

仮想サーバーのライセンスが十分にあることを確認してください。詳細については、「ライセンス」を参照してください。

NetScaler ConsoleにKubernetesクラスターを追加したら、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。Service Graphにデータを表示するには、仮想サーバーがライセンスされている必要があります。仮想サーバーを自動選択するには：

1. **設定 > NetScaler Console Licensing & Analytics Config**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。

仮想サーバーの自動選択(/en-us/netscaler-console-service/media/auto-select-vservers.png)

Webトランザクション設定とTCPトランザクション設定を有効にする

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。

「**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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**TCPトランザクション設定**」で、「**すべて**」を選択します。

5. 「**OK**」をクリックします。

マイクロサービスにトラフィックを送信する

次に、NetScaler Consoleにサービスグラフを表示させるために、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. Ingress 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。

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、さまざまなサービスの詳細を分析できます。詳細については、サービスグラフを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シングルティアまたは統合イングレストポロジを設定するための詳細な手順

シングルティアまたは統合イングレストポロジを展開するための前提条件は、サービスグラフの設定で確認できます。

NetScaler ConsoleでVPX、SDX、MPX、またはBLXインスタンスを追加する

サービスグラフでティア1 NetScalerインスタンスの分析を取得するには、NetScaler ConsoleにVPX/SDX/MPX/BLXインスタンスを追加し、**Web Insight**を有効にする必要があります。NetScaler ConsoleがVPX/SDX/MPX/BLXインスタンスからのWebトランザクションの詳細を表示するには、**Web Insight**を有効にする必要があります。

1. **Infrastructure > Instances > NetScaler**に移動します
2. インスタンスを追加するには、**Add**オプションをクリックします。詳細については、NetScaler Consoleで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**を有効にしてWebトランザクションの詳細を表示します。詳細については、ライセンスの管理と仮想サーバーでの分析の有効化を参照してください。

NetScaler ConsoleでKubernetesクラスターを追加する

Kubernetesクラスターを追加するには：

1. 管理者資格情報を使用してNetScaler Consoleにログオンします。
2. **Infrastructure > Orchestration > Kubernetes > Cluster**に移動します。 クラスターページが表示されます。
3. **Add**をクリックします。
4. **Add Cluster**ページで、次のパラメーターを指定します。
   a. **Name** - 任意の名前を指定します。
   b. **API Server URL** - KubernetesマスターノードからAPIサーバーURLの詳細を取得できます。
      i. Kubernetesマスターノードで、コマンド`kubectl cluster-info`を実行します。
      ii. **「Kubernetes master is running at.」**と表示されるURLを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **認証トークン** - 認証トークンを指定します。認証トークンは、Kubernetesクラスターと NetScaler Console間の通信アクセスを検証するために必要です。認証トークンを生成するには、次の手順を実行します。

   Kubernetesマスターノードで:

   i. YAMLを使用してサービスアカウントを作成します。

      `kubectl create -f adm_svc_account.yaml`

      サービスアカウントが作成されます。

   ii. クラスターロールをサービスアカウントにバインドするには、`kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa`を実行します。

      サービスアカウント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。

   iii. トークンを表示するには、`kubectl describe sa citrixadm-sa`を実行します。

   iv. シークレット文字列を取得するには、`kubectl describe secret <token-name>`を実行します。

d. リストからエージェントを選択します。

   注記

   > CPX YAML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。

NetScaler® テレメトリプログラムのデータガバナンス

既存のすべてのNetScaler Consoleのお客様は、必要なテレメトリデータをアップロードすることにより、NetScalerテレメトリプログラムに準拠する必要があります。NetScalerテレメトリプログラムは、**14.1-28.x** ビルド以降で有効になり、テレメトリデータは自動的にアップロードされます。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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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。NetScaler Consoleの設定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。

注:

- テレメトリのアップロードは24時間ごとに自動的に行われます。
- 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するために、2024年6月18日にリリースされたNetScalerテレメトリプログラムの一部として、以下の構成がNetScaler Consoleを介してNetScalerインスタンスにプッシュされました。

```
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
```

- `/nsconfig/.telemetry.conf` ファイルは、Gatewayテレメトリのために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、このコマンドがない場合は追加します。このコマンドは、VPN仮想サーバー構成を持つNetScalerインスタンスにのみプッシュされます。

```
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。

次の表に、NetScalerテレメトリプログラムの一部として収集される必要なパラメータの詳細を示します。

カテゴリ	説明	用途?
ライセンス、NetScalerの展開と使用状況のテレメトリ	ライセンスの権利、使用状況、高レベルのNetScaler展開データ、およびNetScalerの機能使用状況に関する情報。	ライセンスコンプライアンス、およびサービスの管理、測定、改善のため。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カテゴリ	説明	用途?
NetScaler Consoleの展開と機能使用状況のテレメトリ	Consoleの展開と機能の使用状況に関する情報。	サービスの管理、測定、改善のため。

必須のテレメトリデータ

NetScalerテレメトリプログラムの一部として収集されたデータは、 Telemetry data governanceドキュメントに記載されています。

*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。

NetScaler MPXおよびVPXのrootパスワードを変更する方法

セキュリティ上の理由またはパスワードローテーションポリシーの遵守のため、NetScalerアプライアンスのrootパスワードを定期的に変更する必要があります。

このドキュメントでは、NetScaler Consoleクラウドを介して管理されるNetScaler MPXおよびVPXアプライアンスのrootパスワードを変更するために必要な手順について説明します。

NetScalerのパスワードを変更した場合、そのNetScalerに関連付けられているNetScaler Consoleの管理者プロファイルを変更する必要があります。NetScaler Consoleの管理者プロファイルは、REST API、SSH、SCP、またはSNMPベースのNetScalerアプライアンスとの通信のためのNetScaler資格情報を保持します。管理者プロファイルを介して、NetScaler ConsoleはNetScaler MPXおよびVPXアプライアンスを管理します。

個々のアプライアンスでNetScaler `nsroot` パスワードを変更する方法の詳細については、記事 CTX224027 を参照してください。

構成ジョブ機能を使用してパスワードを変更する

NetScaler Consoleの構成ジョブ機能を使用すると、繰り返しのパスワード変更プロセスを簡素化し、個々のインスタンスにアクセスすることなく、NetScalerアプライアンスに変更を適用できます。

パスワードを変更するには、次の手順に従います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステップ1. 構成テンプレートを作成します。 ステップ2. 構成ジョブを作成します。 ステップ3. 管理者プロファイルを作成し、変更します。

注：NetScalerアプライアンスが他のツールによっても管理されている場合は、それらのツールでも資格情報を変更する必要があります。

ステップ1. 構成テンプレートを作成する

1. NetScaler Console GUIから、**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. **追加**を選択します。SSHコマンド `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$` を入力して、構成テンプレートを作成します。

3. `$ROOT_USER_NAME$` 変数を選択し、**タイプとしてテキストフィールド**を選択します。
4. オプションで、rootユーザー名のデフォルト値を指定します。**Done**を選択して、変数設定を保存します。

5. `$ROOT_USER_PASSWORD$` 変数を選択し、**Password Field as Type**を選択します。**Done**を選択して、変数設定を保存します。
6. **OK**を選択して、構成テンプレートを保存します。
7. 新しい構成テンプレートが**Configuration Templates**の下に表示されます。

構成ジョブを作成する

1. NetScaler Console GUIから、**Infrastructure > Configuration Jobs**に移動します。
2. **Create Job**を選択し、新しい構成テンプレートの「+」アイコンをクリックします。**Next**を選択します。

3. パスワードを変更する必要があるNetScalerインスタンスを選択します。

4. **Select Instances**ペインで、インスタンスを選択し、**Next**をクリックします。
5. **Specify Variable Values**ペインで、ユーザー名とパスワードの値を入力し、**Next**をクリックします。
6. **Job Preview**で、NetScaler ConsoleがNetScalerインスタンスで実行する実際のCLIコマンドを確認します。プレビューが問題なければ、**Next**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 「**実行**」ペインでは、ジョブをすぐに実行するか、後でスケジュールするかを選択できます。また、選択したすべてのインスタンスでジョブを並行して実行するか、順次実行するかを選択することもできます。実行の詳細を指定したら、「**完了**」を選択します。
8. 「**ジョブ**」ページには、実行が成功したか失敗したかが表示されます。
9. 「**ジョブ**」を選択し、「**詳細**」をクリックします。実行の詳細には、個々のインスタンスレベルでのステータスが表示されます。

管理者プロファイルの変更

NetScalerのパスワードを変更したら、インスタンスの管理者プロファイルを追加および変更する必要があります。以下の手順に従ってください。

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. 「**アクションの選択 > プロファイル**」をクリックして、すべての管理者プロファイルを表示します。
3. 「**追加**」を選択して管理者プロファイルを作成し、新しいNetScalerの資格情報を指定します。

   管理者プロファイルの変更(/en-us/netscaler-console-service/media/change-adc-root-password-15.png)
4. 新しく作成されたプロファイルは、「**管理者プロファイル**」の下に表示されます。
5. 「**ネットワーク > インスタンス > NetScaler**」に移動します。パスワードが変更されたNetScalerインスタンスを選択し、「**編集**」を選択します。
6. 新しく作成されたプロファイル名を選択し、「**OK**」をクリックします。

   新しいプロファイルの選択(/en-us/netscaler-console-service/media/change-adc-root-password-16.png)
7. インスタンスを再度選択し、右クリックして「**再検出**」を選択します。

   インスタンスの再検出(/en-us/netscaler-console-service/media/change-adc-root-password-16a.png)

これらの手順により、NetScaler Console でのパスワードリセットプロセスが完了します。

以前のリリース

このトピックは、NetScaler Application Delivery Management (NetScaler Console) の以前のリリースの一覧です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 13, 2023

インフラストラクチャ

NetScaler® ADMサービスのブランド変更

NetScaler Application Delivery Management service (ADM Service) は、NetScaler Console service にブランド変更されました。

ブランド変更されたその他の用語は次のとおりです。

- ADM agent は NetScaler agent にブランド変更されました。
- ADM Service Connect は Console Advisory Connect にブランド変更されました。

注:

NetScaler Console service の製品UIとドキュメントは現在、これらの変更を反映するために更新中です。この期間中、以前の名称とブランド変更後の名称が混在して参照される場合があります。この移行期間中のご理解に感謝いたします。

ライセンス

NetScaler Flexed ライセンス

NetScaler Flexed ライセンスは、ライセンス管理プロセスを簡素化することを目的とした新しいライセンスフレームワークです。Flexed ライセンスには、ソフトウェアインスタンスライセンス (VPX/CPX/BLX、SDX、MPX、および VPX FIPS) と帯域幅容量ライセンスが含まれます。Flexed ライセンスは、NetScaler Console service または NetScaler ADM on-prem に適用する必要があります。また、MPX Z-Cap および SDX Z-Cap ライセンスは、それぞれ NetScaler MPX ハードウェアおよび NetScaler SDX ハードウェアに適用する必要があります。その後、クラウドまたはオンプレミスに展開されているすべてのNetScalerフォームファクターにそれらを割り当てることができます。

注記:

NetScalerエージェントがバージョン16.x以降を実行していることを確認してください。

詳細については、Flexed licenseを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アナリティクス

Flexed license - NetScaler Consoleに追加された新しいNetScalerインスタンスでは、メトリクスコレクターがデフォルトで無効

Flexed licenseを使用している場合、NetScaler Consoleに追加された新しいNetScalerインスタンスでは、メトリクスコレクターがデフォルトで無効になっています。NetScalerのメトリクスとカウンターデータをConsoleにプッシュするには、このオプションを手動で有効にする必要があります。既存の管理対象インスタンスのメトリクスコレクター設定は変更されません。

注記:

そのインスタンス上のすべてのライセンスされた仮想サーバーについて、アプリケーションダッシュボードおよびパフォーマンス、SSL、主要メトリクスなどの関連タブにデータが表示されるようにするには、メトリクスコレクターを有効にする必要があります。

詳細については、Configure Intelligent App Analyticsを参照してください。

ビデオおよびTCPインサイト機能の廃止

最新リリースでは、NetScaler Consoleで**Video Insight**および**TCP Insight**のレポートデータが視覚化のために利用できなくなりました。

インフラストラクチャ

バッチ構成ジョブのファイルをダウンロード

構成ジョブで、NetScaler ADM GUI を使用して、NetScaler インスタンス上のディレクトリからローカルマシンのディレクトリにファイルをダウンロードできるようになりました。

この機能を使用するには、**Infrastructure > Configuration > Configuration Jobs** に移動し、ジョブを選択して **Download Result Files** をクリックします。

Download Result Files ボタンは、次の条件が満たされている場合にのみ使用できます。

- 作成される構成ジョブがバッチ構成ジョブであること。バッチ構成ジョブを作成するには、**Create Job > Select Configuration** に移動し、**Configuration Editor** で **Configuration Source > Batch Configuration** を選択します。
- `scp get` コマンドが **Configuration Editor** で使用されていること。

複数の NetScaler インスタンスの場合、ダウンロードされた結果ファイルは個別のフォルダーに保存され、それぞれが個々のインスタンスに対応します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バッチ構成ジョブ(/en-us/netscaler-console-service/media/batch-config-job.png)

スケジュールされたアップグレードジョブの一時停止と再開

NetScaler ADM で、スケジュールされたアップグレードジョブを一時停止するオプションが提供されるようになりました。この機能を使用するには、**Infrastructure > Upgrade Jobs** に移動し、既存のスケジュールされたアップグレードジョブを選択して、**Stop** をクリックしてジョブを一時停止します。スケジュールされたアップグレードジョブを再開するには、**Resume** をクリックします。

注:

アップグレードジョブを再開することを決定した後、スケジュールされた時間が過ぎていた場合は、アップグレードジョブを再度作成する必要があります。

詳細については、「Upgrade Jobs」を参照してください。

修正された問題

Build December 13, 2023で対処された問題。

分析

- **Applications > Dashboard** で、トランザクションログデータが表形式またはCSV形式にエクスポートされてもデータが表示されません。この問題は、NetScaler ADMがUTC以外のタイムゾーンで構成されている場合に発生します。

- **Security > Security Violations > Violation Details** で、検索フィルターが「Client-IP !=」クエリを認識しません。

- **Security > Security Violations > Export Reports > Schedule Export** からエクスポートされたスケジュール済みスナップショットレポートで、ファイル形式としてJPEGが選択されている場合、次のエラーが表示されます。

  「レポートコンテキストまたはcsv_export_arrでクエリパラメータを指定してください。」

インフラストラクチャ

- 一部のユーザーは、**Infrastructure > Instances** ページのマップに「開発目的のみ」の透かしが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理と監視

- NetScaler ADMエージェントが「netScalerLoginFailure」SNMPトラップを生成します。この問題は、ADMエージェントがNetScalerにログインするために使用する資格情報が、改行文字のために切り捨てられるために発生します。

セキュリティ

- 統合セキュリティダッシュボード (**Security > Security Dashboard > Manage Application**) で保護を設定した後、コンテンツスイッチング仮想サーバーに保護が展開されません。

November 29, 2023

インフラストラクチャ

タグを使用してユーザーグループのインスタンスを承認する

管理者として、関連付けられたタグに基づいて、特定のインスタンスへのユーザーを承認できるようになりました。ユーザーグループを作成するときは、**Settings > Users & Roles > Add > Authorization Settings > Select Tags** に移動し、タグによってインスタンスへのユーザーを承認します。

詳細については、ロールベースのアクセス制御の構成を参照してください。

修正された問題

Build November 29, 2023で対処された問題。

- **Infrastructure > Instances > NetScaler > SDX > Select Action > Provision VPX** でSDXにVPXインスタンスをプロビジョニングすると、**Manage through network** オプションが表示されません。

November 09, 2023

アナリティクス

Gatewayセッションタイムアウトの設定

> > で、Gateway Insight のタイムアウトセッションを設定できるようになりました。デフォルトでは、値は30分です。この設定により、NetScaler ADM が設定された期間内にセッション終了レコードを受信しない場合、セッションは終了として記録されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScalerのバックアッププロセスとファイアウォールアクセスにおける更新

NetScalerインスタンスのバックアップは、NetScalerエージェントからNetScaler ADM Serviceに直接アップロードされ、その後Amazon S3にアップロードされるようになりました。そのため、NetScalerバックアップサービスのためにファイアウォールでS3 URLへのアクセスを許可する必要はなくなりました。

統合セキュリティダッシュボード

NetScaler ADMでは、単一ペインのダッシュボードを使用して、保護を設定し、分析を有効にし、それらをアプリケーションに展開できるようになりました。 **>** に移動し、 をクリックして、次の操作を行います。

- 保護されたアプリケーションと保護されていないアプリケーションをすべて表示します。
- 保護されていないアプリケーションを選択し、さまざまなテンプレートオプションから保護を設定し、保護の分析を有効にし、それらをアプリケーションに展開してアプリケーションを保護します。

以前は、すべての保護をNetScalerインスタンスで設定する必要があり、NetScaler ADMでは設定された保護の分析のみを表示できました。管理者として、この単一ペインのダッシュボードを使用すると、単一のワークフローでアプリケーションの保護を設定できます。

詳細については、「Unified Security dashboard」を参照してください。

修正された問題

Build Nov 09, 2023 で対処された問題。

インフラストラクチャ

- インスタンスを管理するためにNetScaler組み込みエージェントをセットアップすると、登録は成功し、エージェントは**Instance Dashboard**ページで表示できるにもかかわらず、構成が**Add Instances**ページで停止します。

StyleBook

- パラメータに特殊文字を含む構成パックが更新または削除された場合、NetScalerでの更新または削除操作が不完全であっても、NetScaler ADMは成功メッセージを表示します。この修正により、NetScaler ADMは、構成パック定義内の特殊文字が原因で発生する不完全な構成に対するエラーを正確に表示するようになりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

October 25, 2023

分析

インスタンスの主要なメトリックの詳細を表示するためのカスタムダッシュボードを作成する

統合ダッシュボード（**Overview > Dashboard**）と同様に、カスタムダッシュボードを作成することで、選択に基づいてインスタンスのメトリック詳細を表示できるようになりました。たとえば、アプリケーションとアプリケーションセキュリティの主要なメトリックを監視したい場合は、それら2つのカテゴリのみを選択してカスタムダッシュボードを作成できます。各ダッシュボードに一意の名前を使用して、最大20個のダッシュボードを作成できます。管理者として、この機能強化により、複数のダッシュボードを作成し、必要なインスタンスのインサイトのみを監視できます。

開始するには、**Overview > Custom Dashboard**に移動します。

詳細については、「インスタンスの主要なメトリックの詳細を表示するためのカスタムダッシュボードを作成する」を参照してください。

実行可能なタスクと推奨事項

以下の機能強化が**タスク**機能に追加されました。

- 新しい**タスク**タブが導入され、即座に対応が必要な実行可能なタスクを表示できます。これらのタスクは、現在の利用状況に基づいて表示されます。管理者として、これらの実行可能なタスクを完了することで、NetScalerの展開が安全で、準拠しており、効率的であることが保証されます。これらの実行可能なタスクは、問題の重大度（クリティカルおよびミディアム）に基づいて表示することもできます。
- **To Do**タブは**推奨事項**に名称変更されました。**推奨事項**では、既存のタスクを確認し、**ガイドミー**をクリックしてタスクを完了できます。
- **アーカイブ**タブは利用できなくなりました。代わりに、リストから推奨事項を**却下**することを選択できます。

詳細については、「実行可能なタスクと推奨事項」を参照してください。

インフラストラクチャ

証明書ストアを使用してSSL証明書を更新する

インフラストラクチャ > SSLダッシュボード > 更新でSSL証明書を更新する際、証明書ストアから証明書を選択できるようになりました。以前は、SSL証明書を更新するために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した。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SNMPトラップの更新されたリスト

SNMPトラップのリストが、新しいトラップと以前欠落していたいくつかのトラップで更新されました。完全なリストを表示するには、**インフラストラクチャ > イベント > イベント設定 > NetScaler**に移動します。

修正された問題

Build Oct 25, 2023で対処された問題。

- **インフラストラクチャ > インスタンス > NetScaler > SDX > アクションの選択 > VPXのプロビジョニング**でSDXにVPXインスタンスをプロビジョニングする際、**ネットワーク経由で管理**オプションが表示されません。

October 10, 2023

管理と監視

CVE-2023-4966およびCVE-2023-4967の特定と修復のサポート

NetScaler Console Security Advisoryは、CVE-2023-4966およびCVE-2023-4967の特定と修復をサポートするようになりました。

- 特定には、バージョンと構成のスキャンを組み合わせる必要があります。
- 修復には、脆弱なNetScalerインスタンスを修正を含む推奨ビルドにアップグレードする必要があります。

注：

Security Advisoryは、サポート終了（EOL）に達したNetScalerビルドをサポートしていません。NetScalerがサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

NetScaler 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。

詳細については、「セキュリティ速報」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 26, 2023

分析

選択したインスタンスからのみSplunkおよびNew Relicにデータをエクスポート

SplunkとNew Relicにデータをエクスポートするためのサブスクリプションを作成する際、NetScalerインスタンスを選択できるようになりました。特定のインスタンスでサブスクリプションを作成すると、選択したNetScalerインスタンスからのみデータがSplunkとNew Relicにエクスポートされます。

詳細については、Splunkとの統合およびNew Relicとの統合を参照してください。

インフラストラクチャ

Cloud Connectorを使用してADMサービスに接続されたADMオンプレミスインスタンス

設定で、**ADM On-Prem**という新しいオプションが表示されるようになりました。このページでは、ADM On-Prem Cloud Connectorを介してADMサービステナントに接続されているADMオンプレミスインスタンスの詳細を表示できます。

詳細については、Cloud Connectorを使用してADMサービスに接続されたADMオンプレミスインスタンスを参照してください。

修正された問題

Build Sep 26, 2023 で対処された問題。

分析

- App Dashboardデータの定期的な削除が期待どおりに機能しませんでした。その結果、NetScaler Consoleはより多くのディスク領域を消費しました。

September 13, 2023

インフラストラクチャ

テクニカルサポートバンドルをアップロードするための認証トークン

NetScalerで生成されたテクニカルサポートバンドルをCitrixテクニカルサポートサーバーにアップロードするには、認証トークンが必要になりました。以前は、Citrixのユーザー名とパスワードを

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用してテクニカルサポートバンドルをアップロードしていました。詳細については、NetScaler インスタンスのテクニカルサポートバンドルを生成する方法を参照してください。

修正された問題

Build Sep 13, 2023 で対処された問題。

分析

- NetScaler Consoleが仮想サーバーライセンスを失うと、それらのライセンスを使用している仮想サーバーの分析ステータスは無効になると予想されます。このシナリオは、VPN仮想サーバーでは期待どおりに機能していませんでした。

インフラストラクチャ

- **Gateway > HDX™ Insight** および **Gateway > Gateway Insight** では、グラフのX軸に時刻ではなく日付が表示されます。

管理と監視

- **Infrastructure > Network Reporting > Export** からエクスポートされたレポートが切り詰められたり、不完全になったりします。

- 多数のAzureグループに属するAzure Active Directory (AD) ユーザーは、ADグループがADMグループにマッピングされていても、NetScaler Consoleにアクセスできません。

August 31, 2023

インフラストラクチャ

SSLダッシュボードで「Certificate Store」ページを表示する

Infrastructure > SSL Dashboard > Certificate Store に移動して、**Certificate Store** ページを表示できるようになりました。

エージェントのSNMP機能のサポート

Infrastructure > Agents > Actions > Manage SNMP で、エージェントのSNMPマネージャー、SNMPユーザー、SNMPビューを作成できるようになりました。

SNMPマネージャーとユーザーの詳細については、「NetScaler ADMエージェントのSNMPマネージャーとユーザーを作成する」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

データストレージ管理ダッシュボードのユーザーエクスペリエンスと機能の改善

ユーザーエクスペリエンスを向上させ、データストレージ管理をより効率的にするために、**データストレージ管理**ダッシュボードで以下の改善が利用可能になりました。

- ダッシュボードの新しいUIデザイン:
  - **Data Ingestion**、**Storage Consumption**、**Data Pruning**、および **Actions** のタイルを追加
  - **Actions** タイルには、ストレージの追加、データ保持ポリシーの確認、データプルーニングの実行、システム通知の確認を行うオプションがあります。
- **ストレージ消費傾向**セクションの検索機能:

  ストレージの傾向を表示するだけでなく、特定の機能や傾向を検索できるようになりました。
- データプルーニングの実行:
  - 1つ以上の機能を選択し、そのデータをプルーニングしてストレージを解放できるようになりました。
  - 毎月10回のデータプルーニングが可能です。

データストレージ管理ダッシュボードの詳細については、「データストレージ管理」を参照してください。

セキュリティ

API GatewayがAPI Securityに名称変更

API Gatewayは**API Security**に名称変更されました。変更は以下のページで確認できます。

- **セキュリティ > APIセキュリティ**
- **セキュリティ > APIセキュリティ > APIアナリティクス > ヘルプを表示 > APIセキュリティドキュメント**
- **設定 > ユーザーと役割 > グループ > 承認設定 > APIセキュリティ**
- **設定 > ユーザーと役割 > アクセスポリシー > 権限 > セキュリティ > APIセキュリティ**

修正された問題

Build August 31, 2023で対処された問題。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理と監視

- **Infrastructure > Network Reporting** で、ネットワークレポートダッシュボードに仮想サーバーレポートの履歴データが表示されません。この問題は、ダッシュボードの作成時に **Select Entities** でNetScaler HAペアを選択した場合に発生します。

August 11, 2023

管理と監視

セキュリティアドバイザリ - ファイル整合性監視

NetScaler Consoleのセキュリティアドバイザリにより、NetScalerビルドファイルをスキャンし、元のNetScalerビルドファイルへの変更や追加の結果を表示できるようになりました。

セキュリティアドバイザリ (**Infrastructure > Instance Advisory > Security Advisory**) で、**Scan Now** オプションを使用すると、**Scan CVEs**、**Scan Files**、または **Scan Both** を選択できます。**Scan Files** または **Scan Both** を選択すると、NetScaler Consoleは管理対象のNetScalerビルドファイルのバイナリハッシュを元のバイナリハッシュ値と比較し、**File Integrity Monitoring** タブの下にファイルの変更またはファイルの追加がある場合に強調表示します。

スキャン結果には、元のファイルに潜在的な変更がある、またはその他のファイルが追加されているNetScalerインスタンスが表示されます。スキャン結果に関する詳細な調査については、組織のデジタルフォレンジックにご連絡ください。

詳細については、「Security Advisory」を参照してください。

August 09, 2023

インフラストラクチャ

NetScaler VPX™ の仮想化プラットフォームの詳細を表示

Infrastructure > Instances > NetScaler > VPX で、**Settings > Cloud Platform** を選択することで、NetScaler VPX がホストされているプラットフォームを表示できるようになりました。

失敗したアップグレードジョブを再試行する

Infrastructure > Upgrade Jobs で、失敗したアップグレードジョブを選択し、次のいずれかのアクションを実行できるようになりました。

- 失敗したアップグレードジョブの横にある **Retry** をクリックします

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Select Action > Retry Upgrade Job** に移動します

詳細については、「失敗したアップグレードジョブを再試行する」を参照してください。

セキュリティ

既存のAPI定義を更新する

Security > API Gateway > API Discovery で、選択したAPIリソースを使用して既存のAPI定義を更新できるようになりました。

詳細については、「検出されたAPIエンドポイントで既存のAPI定義を更新する」を参照してください。

修正された問題

Build August 09, 2023 で対処された問題。

プロビジョニング

- VMware vCenter (**Infrastructure > Instance > Citrix ADC > VPX > Provision**) でのNetScaler VPXプロビジョニングが、以前に削除されたVPXインスタンスで使用されていたものと同じ名前が原因で失敗します。

StyleBook

- **Applications > Configuration > Config Packs > Migrate ADC > Get Started > Specify Configuration** で、ADC構成をソースADCインスタンスからターゲットインスタンスに移行しようとして **Next** をクリックすると、次のエラーメッセージが断続的に表示されます。

  ジョブが見つかりません。

- 認証仮想サーバーと組み込みキャッシュポリシーバインディングを持つStyleBook定義からconfigpackを作成し、そのconfigpackを削除すると、削除は成功します。ただし、同じパラメータでconfigpackを再度作成しようとすると、次のエラーメッセージが表示されます。

  リソースは既に存在します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 26, 2023

分析

StyleBookを介したNetScalerからPrometheusへのメトリクスエクスポート設定のサポート

NetScalerからPrometheusにメトリクスをエクスポートするには、NetScalerで分析プロファイルを作成し、スキーマファイルを指定する必要があります。詳細については、Prometheusを使用したNetScaler Console、アプリケーション、およびアプリケーションセキュリティの監視を参照してください。

「**Applications > Configuration > Stylebooks > Default Stylebook**」で、**Prometheus TimeSeries Analytics Configuration** StyleBook を使用して、すべての管理対象インスタンスに構成を実行できるようになりました。

詳細については、「Prometheus analytics StyleBook」を参照してください。

NetScaler Consoleから管理対象のNetScalerインスタンスにネットプロファイルを割り当てる

NetScaler Consoleで仮想サーバーの分析を有効にすると、NetScalerからのAppFlowデータは、NetScalerサブネットIPアドレス（SNIP）を介してNetScaler Consoleにエクスポートされます。シナリオによっては、ネットワーク内のファイアウォールによってSNIPがブロックされる場合があります。そのようなシナリオでは、SNIPとは異なるIPアドレスを使用する必要がある場合があります。ネットプロファイルの詳細については、「Use a specified source IP for back-end communication」を参照してください。

NetScaler Consoleを介してNetScalerインスタンスにネットプロファイルを割り当てることができるようになりました。「**Infrastructure > Instances > Citrix ADC**」に移動し、インスタンスを選択し、「**Select Action**」リストから「**Configure Net Profiles**」をクリックして、インスタンスにネットプロファイルを割り当てます。

「

注:

」:

インスタンスにネットプロファイルを割り当てる前に、すべての仮想サーバーで分析を無効にしていることを確認してください。

この機能強化により、NetScalerからNetScaler ConsoleへのAppFlowデータのエクスポートにネットプロファイルを割り当てることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

インフラストラクチャ

CLIを使用してNetScalerエージェントをプロキシとして構成する際のユーザーエクスペリエンスの向上

NetScalerエージェントをNetScaler Consoleサービスに登録しようとすると、CLIはプロキシの使用に関する（y/n）の質問を促すようになりました。

必要に応じて、同じスクリプトでプロキシを構成するオプションもあります。

NetScalerエージェント登録時にエンドポイントURLを表示するためのCLIサポート

NetScalerエージェントをNetScaler Consoleサービスに登録する際に、CLIでサービスURLを入力すると、アクセスを許可する必要があるすべてのエンドポイントURLのリストを表示できます。

StyleBooks

StyleBooksアナリティクスにおける追加属性のサポート

StyleBooksアナリティクスセクションは、以下のように強化されました。

- トランスポートモードを設定するためのパラメータを受け入れる (`transport-mode`)
- さまざまな種類のトラフィックに対してHDX Insightを設定する(`enable-hdxinsight-for`)
  - HTTP X-Forwarded-Forオプションを有効にする (`http-x-forwarded-for`)
  - クライアント側測定を有効にする (`client-side-measurements`)

詳細については、「StyleBooks Analytics」を参照してください。

July 18, 2023

管理と監視

CVE-2023-3519、CVE-2023-3466、およびCVE-2023-3467の特定と修正のサポート

NetScaler Console Security Advisory は、CVE-2023-3519、CVE-2023-3466、および CVE-2023-3467 の特定と修復をサポートするようになりました。

特定:

- CVE-2023-3519 には、バージョンと構成スキャンの組み合わせが必要です。
- CVE-2023-3466 および CVE-2023-3467 には、バージョン スキャンが必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2023-3519、CVE-2023-3466、および CVE-2023-3467 の修復には、脆弱な NetScaler インスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

注:

Security Advisory は、サポート終了 (EOL) に達した NetScaler ビルドをサポートしていません。NetScaler がサポートするビルドまたはバージョンにアップグレードすることをお勧めします。

NetScaler Console を使用して NetScaler インスタンスをアップグレードする方法の詳細については、「ジョブを使用して NetScaler インスタンスをアップグレードする」を参照してください。

CVE-2023-3519、CVE-2023-3466、および CVE-2023-3467 を修復する方法の詳細については、「セキュリティ速報」を参照してください。

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールに CVE-2023-3519、CVE-2023-3466、および CVE-2023-3467 の影響が反映されるまでに数時間かかる場合があります。影響をより早く確認するには、 をクリックしてオンデマンドスキャンを開始できます。

July 12, 2023

修正された問題

Build July 12, 2023 で対処された問題。

- NetScalerインスタンスをバックアップまたは復元する際、`/var/metrics_conf`ディレクトリはバックアップされません。

- StyleBookの定義に`operations`セクションが含まれている場合、設定パックの展開が失敗する可能性があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 03, 2023

分析

構成ジョブ - NetScalerからPrometheusへのメトリクスエクスポートを構成するジョブの作成をサポート

NetScalerからPrometheusにメトリクスをエクスポートするには、NetScalerで分析プロファイルを作成し、スキーマファイルを指定する必要があります。詳細については、Prometheusを使用したNetScaler、アプリケーション、およびアプリケーションセキュリティの監視を参照してください。

構成ジョブで、**組み込みテンプレート**から`NSConfigurePrometheusAnalyticsProfile`テンプレートを使用してジョブを作成し、必要なパラメータを指定して、すべての管理対象インスタンスに対してジョブを実行できるようになりました。

詳細については、NetScalerからPrometheusへのメトリクスエクスポートを構成するジョブのスケジュールを参照してください。

インフラストラクチャ

NetScalerエージェントがNetScalerイメージをキャッシュする

NetScalerイメージがダウンロード後にNetScalerエージェントにキャッシュされるため、NetScalerのアップグレードにかかる時間が大幅に短縮されました。したがって、その後のアップグレードジョブではイメージをダウンロードする必要がありません。

注:

これは、NetScalerエージェントを使用して追加されたNetScalerにのみ適用されます。

詳細については、「ADCアップグレードジョブの作成」(/ja-jp/netscaler-console-service/networks/configuration-jobs/how-to-upgrade-adc-instances.html#create-an-adc-upgrade-job)を参照してください。

修正された問題

- Web Insightで、詳細を表示するために任意のメトリックをドリルダウンし、さらに別のメトリックをドリルダウンすると、グラフは以前のビューのままですが、他のすべての詳細は期待どおりに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

その結果、これにより、さらなるドリルダウンが期待どおりに機能していないという仮定が生じます。

- **Applications > Configuration > Config Packs > Migrate ADC > Get Started > Specify Configuration**で、ソースADCインスタンスからターゲットインスタンスにADC構成を移行しようとして**Next**をクリックすると、次のエラーメッセージが断続的に表示されます。

  「ジョブが見つかりません」。

- **App dashboard**でアプリケーションを選択し、**SSL**タブに移動して証明書をバインドしようとすると、「**データベースに証明書が見つかりません**」というエラーメッセージが表示されます。

June 14, 2023

セキュリティ

エンドポイントを選択せずにAPI定義を作成するサポート

「**Security > API Gateway > API Discovery** > **Vserver**」ページで、エンドポイントを選択せずにAPI定義を作成できるようになりました。「**Create API Definition**」をクリックすると、検出されたすべてのエンドポイントに対してAPI定義を作成するかどうかを確認するポップアップウィンドウが表示されます。すべてのエンドポイントでAPI定義を作成するには「**Yes**」をクリックし、そうでない場合は「**No**」をクリックします。

詳細については、「APIエンドポイントの検出」を参照してください。

StyleBook

replace() 関数における追加の引数タイプのサポート

`replace()` 組み込み関数は、以下の組み込み型のリストも受け入れることができます。

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- `boolean`

詳細については、「replace()」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修正された問題

Build June 14, 2023 で対処された問題。

- Upgrade Jobs (**Infrastructure > Upgrade Jobs**) で、アップグレード前の検証に失敗したインスタンスを選択して **Revalidate** をクリックすると、エラーメッセージが表示されます。
- **Infrastructure > Citrix ADC Inventory > Citrix ADC (MPX/VPX/CPX/BLX)** ページからMPXインスタンスがありません。
- **Infrastructure > SSL Dashboard > SSL Certificates > Export Reports** から週次、30日、または90日間のSSL有効期限レポートをエクスポートし、**Tabular** を選択すると、結果のレポートにドメイン列が空で表示されます。
- **Infrastructure > SSL Dashboard > SSL Certificates** で、NetScalerの高可用性ペアがプライマリデバイスとセカンダリデバイスの「P」と「S」の上付き文字を表示しません。
- NetScalerリリース13.1以降では、NetScalerのアップグレード中にISSUコマンドが実行されません。
- クラスター内の複数のクラスターIPアドレス (CLIP) の場合、**Infrastructure > Instances > Citrix ADC > Add** で括弧内にCLIPを追加すると、構成が失敗し、CLIPがNetScaler Consoleに追加されません。

May 31, 2023

アナリティクス

タスク機能におけるプールライセンスの推奨事項

「**Tasks**」で、プールされたライセンスエンタイトルメントの推奨事項とガイドミーワークフローを表示できるようになりました。管理者として、これらのプールされたライセンスの推奨事項により、NetScaler Consoleのすべての機能を活用できます。

詳細については、「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」を参照してください。

SSLインサイトデータをSplunkおよびNew Relicにエクスポートする

Citrix ADMとSplunkおよびNew Relicの統合のために、**Settings > Ecosystem Integration**で新しいサブスクリプションを作成する際に、**SSL Certificate Insights**オプションを選択できるように

© 1997–2026 Citrix Systems, Inc. All rights reserved.

なりました。**SSL Certificate Insights**オプションでサブスクリプションを設定すると、SplunkおよびNew Relicダッシュボードで SSLデータ（SSL仮想サーバーおよびSSL証明書関連データ）を表示できます。

詳細については、「Splunkとの統合」および「New Relicとの統合」を参照してください。

修正された問題

Build May 31, 2023 で対処された問題。

- **Gateway > HDX Insight > Instances**でインスタンスを選択してデータをエクスポートすると、デスクトップユーザーのユーザー名情報が利用できませんでした。この修正により、ユーザー名情報もレポートで利用できるようになりました。

- **Infrastructure > Instances > Citrix ADC > SDX**でSDXインスタンスの**Configure SNMP**を選択すると、エラーメッセージが表示されます。この問題は、SDXプロファイルがSNMP v3とセキュリティレベルとして**NoAuthNoPriv**で構成されている場合に発生します。

- **Infrastructure > Configuration > Configuration Jobs > Create Job > Select Configuration** で、パスワード変数（$password$）を入力し、**Type**を**Password Field**ではなく**Text Field**のままにして**Next**をクリックすると、ページがロードされません。

- Web Insight で、スナップショットオプションを使用してデータをエクスポートすると、レポートのグラフが空白で表示されます。

- HDX Insight でアナリティクスが表示されません。Citrix ADM を再起動しても、アナリティクスは短時間しか表示されず、その後表示されなくなります。

- **Infrastructure > Instances > Citrix ADC > SDX > Dasboard** の SDX インスタンスで、リソースの使用済み値と空き値がゼロの場合、**System Resource Utilization** チャートに空白のスペースと空白の値フィールドが表示されます。

  この修正により、使用済み値と空き値がゼロの場合、リソース名の横に数値ゼロが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 18, 2023

アナリティクス

Web Insight の各ウィジェットからのエクスポートのサポート

Web Insight では、すべてのウィジェットにエクスポートオプションが導入され、データを表形式でエクスポートできるようになりました。この機能強化により、次のことが可能になります。

- 任意のウィジェットから必要なデータを個別にエクスポートします。
- 任意のメトリックをドリルダウンし、任意のウィジェットから必要なデータもエクスポートします。

以前は、エクスポートデータは統合レポートのみを提供していました。

注

> 統合レポートを生成するために、既存の「エクスポート」オプションを引き続き使用することもできます。

インフラストラクチャ

完全な証明書チェーンを表示する

ルートCA証明書までのすべての中間証明書を含む、証明書の完全なリンクチェーンを表示できるようになりました。

証明書チェーンを表示するには、**Infrastructure > SSL Dashboard** に移動し、SSL証明書を選択して **Details** をクリックします。

イベントの経過時間に関わらずイベントをログに記録するサポート

NetScaler Consoleでは、イベントルールで設定したイベントの経過時間に関わらず、すべてのイベントを記録できるようになりました。

このオプションを設定するには、**Infrastructure > Rules > Add > Configure Event Age** に移動し、**Log events instantly irrespective of event age duration** チェックボックスを選択します。

修正された問題

Build May 18, 2023 で対処された問題。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Infrastructure > Upgrade Jobs > Add > Schedule Task** で、**Perform two stage upgrade for nodes in HA** を選択し、2つの **Start Time** フィールドで同じ時間を選択すると、続行時に次のエラーメッセージが表示されます。

  「common.date_diff_error:アップグレード時間の間には少なくとも1時間の差が必要です」

  フィールドで開始時刻を変更しても、**ジョブの作成**タブには空のページが表示されます。

- **インフラストラクチャ > インスタンスアドバイザリ > アップグレードアドバイザリ**で、リリース13.0のメンテナンス終了 (EOM) およびサポート終了 (EOL) の詳細が正しくありません。

- イベントのメールアラートで地域が誤って表示されていました。この修正により、イベントのメールアラートに地域は表示されなくなります。

May 09, 2023

管理と監視

CVE-2023-24488およびCVE-2023-24487の特定と修正のサポート

NetScaler Console Security Advisoryは、CVE-2023-24488およびCVE-2023-24487の特定と修正をサポートするようになりました。

特定対象:

- CVE-2023-24488には、バージョンと構成スキャンの組み合わせが必要です。
- CVE-2023-24487には、バージョンスキャンが必要です。

CVE-2023-24487およびCVE-2023-24488の修正には、脆弱なADCインスタンスを修正を含むリリースおよびビルドにアップグレードする必要があります。

CVE-2023-24487およびCVE-2023-24488の修正済みビルドバージョンの詳細については、セキュリティ速報を参照してください。

注:

ADCビルド13.1–45.63は、ビルド13.1–45.61に置き換わります。

NetScaler Consoleを使用してADC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、ADCアップグレードジョブの作成を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

セキュリティアドバイザリシステムのスキャンが完了し、セキュリティアドバイザリモジュールにCVE-2023-24488およびCVE-2023-24487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。

April 25, 2023

Build April 25, 2023 で利用可能な機能強化と変更点。

分析

Web Insight - グラフでnil値を表示するサポート

Web Insightで、アプリケーション、クライアント、URL、またはインスタンスの下にある任意のメトリックをドリルダウンすると、分析ビューで、選択した期間のグラフにnil値（例：0ミリ秒、0リクエスト）が表示されるようになりました。

以前は、選択した期間にトラフィックやトランザクションが受信されなかった場合、Web Insightはこれらのnil値をスキップしてグラフを表示していました。管理者として、これらのnil値を含む完全なグラフを表示できるようになりました。

StyleBook

構成パックへのユーザーグループアクセスを指定する

管理者として、ユーザーグループが他のユーザーグループによって作成された設定パックにアクセスするのを制限できるようになりました。このオプションを選択するには、**Settings > Users & Roles > Groups > Authorization Settings > Config Packs > All Configurations created by the user group** に移動します。

修正された問題

Build April 25, 2023で対処された問題。

- **Applications > Configuration > Config Packs** で、**Properties > Display Key** の検索条件を使用して検索クエリを入力すると、検索結果は表示されますが、検索バーには結果のインデックス番号が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

この修正により、検索バーには数値ではなくテキストで検索クエリが表示されるようになります。

分析

- **HDX Insight** および **Gateway Insight** の帯域幅データが、bits per second ではなく bytes per second で誤って表示されます。

April 13, 2023

Build April 13, 2023で利用可能な機能強化と変更点。

分析

Web Insight の統合キャッシュ通知

NetScalerインスタンスでIntegrated Cacheを有効にすると、対象となるリクエストはオリジンサーバーへのラウンドトリップを必要とせずに処理されます。**Web Insight** では、これらのIntegrated Cacheリクエストは現在、実際のサーバーIPアドレスではなく、仮想サーバーIPアドレスを持つ **Servers** の下に表示されます。

これらの統合キャッシュリクエストの可視性を向上させるため、**サーバー**の下にあるADC仮想サーバーのIPアドレスの横にIC通知を表示できるようになりました。

統合キャッシュで処理されないリクエストの場合、実際のオリジンサーバーのIPアドレスが表示されます。

管理者として、この通知により、ADCインスタンスが統合キャッシュリクエストを処理したことを迅速に特定できます。

Web Insightにおける統合キャッシュのヒットとミスのグラフ

Web Insightでサーバーをドリルダウンすると、**サーバーメトリクス**に**統合キャッシュヒット**と**統合キャッシュミス**のタブが表示されるようになりました。

管理者として、グラフビューでは次のことが可能です。

- **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Insight - グラフで平均値と最大値の両方を表示

13.1 45.47以降のバージョンでは、NetScaler Consoleの**Web Insight**は、**サーバー**と**クライアント**の下で最大遅延値の可視性をサポートしています。

このサポートに加えて、サーバーまたはクライアントをドリルダウンすると、サマリーパネルで平均値と最大値の両方を表示できるようになりました。また、**サーバーネットワーク遅延**、**サーバー応答時間**、**クライアントネットワーク遅延**の時系列分析グラフにマウスポインターを合わせることでも表示できます。

管理者として、この機能強化により、選択した期間の最大遅延をグラフで視覚化できます。

インフラストラクチャ

NetScaler Console GUI でデータストレージの傾向を表示する

設定 > データストレージで、現在のデプロイメントにおけるさまざまな機能全体のデータストレージ情報を表示できるようになりました。**データストレージ管理**ダッシュボードは、データがどのように保存されているか、および機能がストレージエンタイトルメント内で動作しているかどうかを視覚化するのに役立ちます。

注

データストレージポリシーは、今後のリリースで変更される予定です。これらの変更により、ストレージ制限を超過した履歴データを保存できなくなります。

詳細については、「データストレージの管理」を参照してください。

修正された問題

April 12, 2023 ビルドで対処された問題。

インフラストラクチャ

- 高可用性デプロイメントでは、ビルドイメージファイルをセカンダリノードにのみアップロードするオプションがありません。

  この修正の一環として、**インフラストラクチャ > アップグレードジョブ > ジョブの作成**タブ > **セカンダリノードにのみアップロード**から、ビルドイメージファイルをセカンダリノードにアップロードできるようになりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **インフラストラクチャ > インスタンス > NetScaler**からエクスポートされたレポートには、セカンダリノードのシリアル番号が表示されません。

  レポートには、NetScalerインスタンスのプライマリノードとセカンダリノードの両方のシリアル番号が表示されるようになりました。レポートは**インフラストラクチャ > NetScalerインベントリ**からも表示できます。

April 05, 2023

Build April 05, 2023で利用可能な機能強化と変更点。

セキュリティ

NetScaler Console GUIで検出されたAPIエンドポイントからAPI定義を作成

これで、**Security > API Gateway > API Discovery** で検出されたAPIエンドポイントからAPI定義を作成できるようになりました。

統合ダッシュボード - API分析の主要メトリックを表示

統合ダッシュボード (**Overview > Dashboard**) で、NetScaler Consoleを介して構成されたAPIエンドポイントの主要メトリックを表示できるようになりました。

詳細については、「インスタンスの主要メトリックの詳細を表示する統合ダッシュボード」を参照してください。

修正された問題

Build April 05, 2023で対処された問題。

- **Certificate File** および **Key File** フィールドの **Choose Appliance** オプションが、以下のページに表示されます。

  - **インフラストラクチャ > SSLダッシュボード > 証明書ストアの管理 > 追加**
  - **インフラストラクチャ > SSLダッシュボード > SSL証明書 > 更新**

  修正として、「**アプライアンスの選択**」オプションは削除されました。

- NetScalerがオンプレミスのNetScaler Consoleをライセンスサーバーとして持ち、「**インフラストラクチャ > インスタンス > エージェント**」でエージェントが変更された場合、次の問題が発生します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`The IP address of the license server on NetScaler changes from the IP address of the on-premises NetScaler Console to the IP address of one of the NetScaler agents`。

- SNMPv3で構成されたSDX管理者プロファイルのパスワードを「**インフラストラクチャ > インスタンス > NetScaler > SDXタブ > プロファイル**」から編集すると、次のエラーメッセージが表示されます。

  `Please provide valid authentication protocol. The possible values are MD5, SHA`。

March 14, 2023

修正された問題

次の問題は、Build March 14, 2023で対処されています。

「**インフラストラクチャ > SSLダッシュボード > 証明書のインストール**」で、既存の証明書チェーンと同じルート証明書を持つ証明書チェーンをアップロードすると、証明書のインストールが失敗します。「**インフラストラクチャ > SSLダッシュボード > SSL監査ログ > デバイスログ > コマンドログ**」に次のテキストが表示されます。

`Resource Already Exists`

電子メール配布リストを** > > **から削除すると、次のエラーが表示されます。

`Error: Bad Gateway`

この問題は、電子メール配布リストの名前に空白が含まれているために発生します。

修正の一環として、NetScaler Consoleでは、空白を含む電子メール配布リストを削除できるようになりました。

March 02, 2023

アナリティクス

Web Insightの改善

Web Insightでは、****の下で次の機能強化を表示できるようになりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 新しい****タブが導入され、応答時間、要求、帯域幅などのアプリケーションパフォーマンスの概要を視覚化できます。管理者として、これにより選択した期間のアプリケーションパフォーマンスに関する洞察を得ることができます。トグルオプションを使用して表示をカスタマイズできます。
- ****タブでは、既存の合計要求に加えて、合計要求に基づいて上位5つのクライアントからの要求も表示できます。管理者として、これにより選択した期間に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洞察を得ることができます。
- ****タブでは、合計帯域幅消費量に基づいて上位5つのサーバーからの帯域幅消費量を表示できます。管理者として、これにより選択した期間に帯域幅を多く消費しているサーバーに関する洞察を得ることができます。
- ****タブでは、クライアントネットワーク遅延、サーバーネットワーク遅延、およびサーバー処理時間を同じグラフで表示することもできます。管理者として、これにより選択した期間にクライアント、サーバー、およびアプリケーションから発生する遅延に関する洞察を得ることができます。トグルオプションを使用して表示をカスタマイズできます。

インフラストラクチャ

非アクティブなNetScaler Console Expressアカウントの削除

NetScaler Console Expressアカウントが45日間非アクティブのままである場合、そのアカウントは削除されます。Citrixは30日間の非アクティブ状態の後、リマインダーを送信します。

管理と監視

NetScaler高可用性アップグレードの実行サマリーの変更

NetScaler Console GUIの**Infrastructure > Upgrade Jobs > Execution Summary**にある実行サマリーには、高可用性同期関連のコマンドが表示されなくなりました。

これは、NetScaler高可用性アップグレード中に、NetScalerプライマリノードとセカンダリノードのバージョンが異なる場合、NetScalerがノード間の高可用性同期を無効にするためです。NetScaler Consoleはこの操作を実行しません。

ネットワークレポートの個々のエンティティのしきい値を設定する

Infrastructure > Network Reporting > Thresholdsで、しきい値を設定する際に特定のエンティティのしきい値を設定できるようになりました。

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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

個別エージェントアップグレードのスケジューリングのサポート

Infrastructure > Instances > Agents > Settingsで、各NetScalerエージェントのアップグレードをスケジュールできるようになりました。エージェントを次のビルドに自動的にアップグレードするか、アップグレードをスケジュールする日時とタイムゾーンを指定するかを選択できます。

詳細については、「エージェントアップグレード設定」を参照してください。

NetScalerインスタンスのアップグレードにおける改善点

以下の変更が**アップグレード前検証**タブで利用可能になりました。

- **アップグレードがブロックされたインスタンス**セクション - この新しいセクションには、アップグレード前検証エラーのためにアップグレードがブロックされたインスタンスが一覧表示されます。
- **クイッククリーンアップ**ボタン - このボタンは**ディスク容量の詳細**ペインで利用でき、複数のフォルダーからディスク容量をすばやく解放できます。

詳細については、「ADCインスタンスをアップグレードする方法」を参照してください。

NetScaler BLXイメージがイメージライブラリで利用可能に

Infrastructure > Upgrade jobs > Upgrade NetScaler BLX > Select ImageからNetScaler BLXをアップグレードする際に、イメージライブラリから**NetScaler BLXイメージ**を選択できるようになりました。

セキュリティ

NetScalerインスタンスのNetScaler Web App Firewallおよびボットシグネチャのバージョンを表示

NetScalerインスタンスのNetScaler Web App Firewallおよびボットシグネチャのバージョンを表示できるようになりました。最新のシグネチャバージョンは、CVEからインスタンスを保護します。詳細については、「Signature Alert Articles」および「Bot signature alert articles」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリケーションパフォーマンス分析

Web Insight の改善

Web Insight では、**サーバー**と**クライアント**の両方で最大ネットワーク遅延値を表示できるようになりました。管理者として、この機能強化により、最大の遅延で動作している正確なサーバーまたはクライアントを特定できます。

以前は、Web Insight はすべてのサーバーとクライアントの平均遅延値に基づいてのみ最大値を提供していました。

その他

統合ダッシュボードでフィルターを作成して適用する

統合ダッシュボード（**概要 > ダッシュボード**）で、以下のフィルターを作成して適用できるようになりました。

- アプリケーション
- ADC インフラストラクチャ
- アプリケーションセキュリティ

管理者として、選択したインスタンスまたはアプリケーションに対してのみフィルターを適用し、インサイトを表示できます。

詳細については、「インスタンスの主要メトリックの詳細を表示する統合ダッシュボード」を参照してください。

修正された問題

Build Mar 02, 2023 で対処された問題。

- 「**Infrastructure > Upgrade Jobs**」で、特殊文字を含むアップグレード前またはアップグレード後スクリプトファイル名を持つ完了したジョブを選択し、「**Select Action**」リストから出力スクリプトをダウンロードすると、「**File not found**」エラーメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 07, 2023

分析

セキュリティ違反にOWASPタグが表示される

NetScaler Console GUIで、セキュリティ違反にOWASPタグが表示されるようになりました。OWASP 2017およびOWASP 2021リストをサポートしています。これらのタグは、違反がOWASPトップ10リストに属するかどうかを判断するのに役立ちます。

違反を選択すると、詳細が表示されます。詳細には、OWASP 2017およびOWASP 2021の列が含まれるようになりました。これらの列にはOWASPコードが表示され、これらを使用してOWASPウェブサイトから違反について詳しく知ることができます。

管理と監視

現在のパスワードなしでエージェントパスワードを変更するサポート

スーパー管理者として、現在のパスワードなしでエージェントパスワードを変更できるようになりました。

Settings > **Global Settings** > **System Configurations** > **Agent and Time Zone > Agent** に移動し、「**Remove current password prerequisite for agent password change**」チェックボックスを選択します。「**Change Agent Password**」ページには、「**Current password**」フィールドが表示されなくなります。

「**Current password**」フィールドを再度表示するには、「**Remove current password prerequisite for agent password change**」チェックボックスをオフにします。

NetScaler Console Expressアカウントの時系列データ視覚化間隔が改訂されました

Expressアカウントで管理されている仮想サーバーの場合、分析グラフおよびネットワークレポートグラフにおける**過去1時間**の期間の時系列データ可視化が改訂されました。

機能	既存のデータ可視化間隔	新しいデータ可視化間隔
アプリケーションダッシュボード	1分	5分
ネットワークレポート	5分	10分
Web Insight、HDX Insight、Gateway Insight、Security	1分	5分

© 1997–2026 Citrix Systems, Inc. All rights reserved.

機能	既存のデータ可視化間隔	新しいデータ可視化間隔
Insights、BOT Insights、詳細なトランザクション		

修正された問題

以下の問題は、Build February 07, 2023で対処されています。

ADCインスタンスのsyslog設定を有効または無効にしても、ADMはADCインスタンスに設定を保存しません。その結果、設定変更イベントはNetScaler Consoleに保存されません。

Infrastructure > Instances > Agent で、パスワードで暗号化されたキーを持つSSL証明書をインストールした後、ポート443上のエージェントへの接続が失敗します。

January 24, 2023

修正された問題

以下の問題は、Build January 24, 2023で対処されています。

NetScaler Console GUIから、**Infrastructure > Instances > NetScaler > SDX > Select Action > Configure SNMP** に移動してNetScaler SDXインスタンスでSNMP v3を有効にすると、エラーメッセージが表示されます。

January 10, 2023

管理と監視

ガイドミーワークフローを使用して、推奨事項を表示し、ADCとアプリを実用的なタスクとして効率的に管理する

NetScaler Console GUIに新しい **タスク** オプションが導入され、サブスクリプションと現在の利用状況に基づいて推奨事項を表示できるようになりました。管理者として、次のことができます。

- ライセンス、分析、イベント、SSL証明書などに関する実用的な推奨事項として、**To-Do** タスクを表示する
- タスクを正常に完了できるよう、ガイダンスツールチップを提供する**ガイドミー**オプションを使用してタスクを完了します。
- タスクを承認し、アーカイブに移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **アーカイブ済みタスク**に移動し、定期的なニーズのためにガイド付きツールチップを使用します。

これらの推奨事項により、NetScaler Console のすべての機能を活用し、製品の発見と、展開の効率的な管理のために製品が推奨する機能が有効になります。

詳細については、「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」を参照してください。

StyleBooks

StyleBook 設定 GUI でネットマスク長を有効または無効にする

`type: ipnetwork` 属性を持つ StyleBooks から構成パックを作成すると、StyleBook 設定 GUI に**IP アドレス**フィールドの横に**ネットマスク長**ボタンが表示されるようになりました。

次のいずれかのアクションを実行できます。

- ネットマスク長の入力を有効にする
- ネットマスク IP アドレスの入力を無効にする

© 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.